Business Resilience Standards

Helping Businesses Address COVID-19 Related Economic Challenges

PTB

SEE South East Europe Regional Consultancy Fund Quality Infrastructure (QI)

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Table of Contents

About this Publication

Chapter 1: Risk Management (Driton S. Bejtullahu)

Chapter 2: Business Continuity Management (Violeta Haxhillazi)

Chapter 3: Information Security Management Systems (Osman-Jablan Bulić)

Chapter 4: Supply Chain Security Management Systems (Violeta Haxhillazi)

Chapter 5: Occupational Health and Safety Management (Suzana Temelkoska)

Chapter 6: Innovation Management (Liridona Cani)

Chapter 7: Developing Modern Leadership Skills (Antigona Limani)

About this Publication

Introduction

The COVID-19 crisis caused significant challenges to economies and industries. While the richer industrialized countries try to limit the economic damage with considerable financial resources, other countries' industries are experiencing such possibilities to a much lesser extent. Unstable markets, partly closed boarders, lack of transport possibilities are just some of the problems economies and industries were faced with during the pandemic. It can be assumed that the current Corona pandemic will hardly be the last wave of global infections, e.g. due to an increasing world population and even better traveling opportunities. Climate change might cause other questions, we must find answers for soon.

Sustainability and resilience are the terms that are often used when discussing the lessons learned and the consequences resulting from the current pandemic. A resilient company has the ability to successfully implement planned measures to cope with immediate crises or unexpected events. One could state that resilience is one of the prerequisites for sustainability.

A resilient organization is prepared to overcome obstacles and to meet evolving challenges of any kind. In times of economic and political uncertainty, it's more important than ever that organizations have the tools to estimate and to treat their risks in a systematic way, to ensure their value chains are safe, to strive for safe workplaces and to secure systematically their information technology. Further, in a globally competitive market, innovation management is a fundamental precondition to survive.

The international standard organization ISO together with the national standard institutes provide standards, helping to develop the respective tools. Standards provide universally accepted tools and practices to achieve a given objective. The preconditions and ways are mostly defined in form of requirements which can be used as a basis for certification. Certification under accreditation provides the organizations, their stakeholders, clients and shareholders with the assurance, that the standards are being effectively implemented.

Implementation of all these standards and tools require the involvement of highly engaged staff. It is therefore important that organizational development and leadership is not just a buzzword. Knowledge of leadership and modern management concepts are a prerequisite for making organizations more resilient and implementation of standards effective and efficient.

In the frame of the South East Europe Regional Consultancy Fund PTB organized a training for future trainers in standards, which are essential when improving business resilience and in leadership. The trainings were held by well reputed and experienced experts. As part of the training these experts provided an article as a contribution to this handbook. Its aim is not to summarize the content of the standards, but much more to focus on important elements of the standards to consider when improving business resilience and sustainability. At the same time, each chapter provides tools and possibilities on how to implement the respective requirements e.g. to prepare for future certification. Reading this hand booklet is therefore a must for consultants, trainers, and executives looking to improve business resilience.

The undersigned thank all the experts for the excellent cooperation during this project. Especially we would like to give thanks PTB and Mr. Stefan Wallerath for making this project possible and the German Federal Ministry for Economic Cooperation and Development (BMZ) for financing this project.

Suzana Lange, Sophie Salimkhani & Hanspeter Ischi

About the Authors

Driton S. Bejtullahu

An MBA Graduate in Strategic Management/Change Management in Danube University Krems (DUK), Driton has 19+ years of experience in different industries with local and international organization for public and private sector. During the years, his approach was to serve as a bridge between Technology and Management by helping organization improve their business process through integrations of advanced technology and management frameworks. As a certified trainer and implementer, his experience helped him apply integrated ISO management system in different organization during the years. Now he is engaged as a Management Consultant in EBRD projects for empowering local business in Kosovo to increase their level of services and products and support them in the export process toward international markets. In meantime he is a member of Technical Committee for ICT in Kosovo Standardization Agency.

Violeta Haxhillazi

Violeta has 20 years of experience in business consultancy and project management in local and international companies. Her advisory experience is extensive in several areas: strategic planning and transformations, operational efficiency and excellence, and IT governance. One of her areas of expertise is Supply Chain Management, in which she supports businesses to achieve their goals of ensuring that products are delivered on time, in the right quantity and in a cost-effective manner, by looking at current processes and identifying methods for improvement, focusing on risk management as well as personnel supervision. She is a Certified Management Consultant (CMC©), Certified Sales Executive (CSE©) and Certified Digital Transformation Expert (CDTE©).

Osman-Jablan Bulić

Consultant with close to 20 years of practical experience working on numerous projects related to the implementation of various management systems, governance frameworks, risk management systems, and security controls. His hands-on experience in variety of different organizations (small and large, private and governmental, spreading across various industries) gives him a great perspective on the issues and challenges that these organizations face. Beside consulting, he is an approved training instructor for a wide range of training courses though the PECB certification organization, having trained over 100 successfully certified candidates. Osman holds Lead Implementer and Auditor status for variety of ISO standards and works as an external certification auditor for TÜV Nord.

Suzana Temelkoska

Suzana Temelkoska is a Chemical Engineer and the founder and CEO of Euromak-Kontrol, the first consulting company in Macedonia certified in accordance with the requirements of the standards ISO 9001: 2015, ISO 14001: 2015 and ISO 45001:2018. Euromak-Kontrol has an accredited laboratory in accordance with ISO 17025 and an accredited inspection body in accordance with ISO 17020, both accredited by the Institute for Accreditation of the Republic of North Macedonia for quality and quantity control of goods. Suzana has forty years of experience as a consultant, auditor and trainer of management systems. Suzana is also the president of Technical Committee TK9 in the Institute for Standardization of the Republic of North Macedonia for the standards ISO 9001, ISO 14001, ISO 45001, ISO 50001 and ISO 26000. She is also a member of the Macedonian Consulting Association and Association for Occupational Safety – run by the Economic Chamber of North Macedonia, She is the lead auditor for ISO 9001, ISO 14001, ISO 45001, ISO 50001, ISO 17025 and ISO 17025. Suzana has been an occupational safety and health expert since 2010 and actively works on issues in the field of safety and health in more than 50 organizations with different activities.

Liridona Cani

Liridona Cani currently in the role of Information Security Officer and Data Protection in a Software Development Company. She has a long experience in Management, consultancy, Lecturing, Training and Project management. Her experience started as a Lecturer at University of Tirana and also at a language course Center in Tirana. As a professional and quite competent in her skills, she has started to work in a Software and Engineering Company where she is focused on implementation of ISO Standards practically ISO 27001, ISO 9001 and ISO 560001 and Data Protection. Liridona Cani is certified as ISO 27001 Lead Implementer, ISO 27001 Lead Implementer Trainer, as a Project manager certified with PRINCE2 Certification.

Antigona Limani

Antigona Limani is a Strategic Marketing, Management and Sustainability Consultant with more than 15 years of experience in different industries and companies in Kosovo. She currently holds the role of Head of Marketing and PR department and responsible for Sustainability Management in the Bank, she is also co-founder of consultancy company Be Consulted in Kosovo, and Board member in CSR network. Her experience in many companies and experience in change management in big and smaller companies in Kosovo are appropriate for sharing the experience for managing change as well as the role of leadership and the importance of being resilient.

Chapter 1

Risk Management

Based on ISO 31000/ISO 31004/ISO 31010

By Driton S. Bejtullahu

1. Introduction

Imagine you are a hiker and you have to climb on the top of a mountain. Your equipments are not 100% secure but you still need to pass this peak in order to survive. Considering that the market does not offer you a suitable rope that is 100% secured in all conditions, you still need to take an action. Your every action will be like a Risk Management Process.

2. Complexity – a Reason for Increased Risks in Industry and Trading

Risk can stem from a wide variety of sources. Based on the Economic and Human Impact of Natural Disaster data, risks associated with natural disaster (i.e. floods, earthquakes, volcanic eruptions, hurricanes) from 2005 until 2014 there were:

- $ 1.4 trillion of total financial damage
- $ 1.7 billion people were affected
- $ 0.7 million people were killed

Even though we cannot stop natural disasters from occurring, we can, however, assess, manage, and treat risks associated with such phenomena and therefore better manage their impact and lessen the financial burden.

2.1. Damage Incurred Countries

- According to the United Nations Office for Disaster Risk Reduction (UNISDR), during the period 2005 until 2014, China has faced the greatest number of disasters – 286 of them, totalling to over $256 billion in damages.
- The United States has had fewer disasters during the same period but incurred the largest financial damage – $443 billion.
- Japan, on the other hand, although having far fewer disasters, its economic loss was almost as big as that of China's – $239 billion

The Evolving Risk Landscape 2016-2020 – Top five global risk in terms of likelihood (Source: World Economic Forum. The Global Risk Report, 2020)

	2016	2017	2018	2019	2020
1st	Involuntary migration	Extreme weather	Extreme weather	Extreme weather	Extreme weather
2nd	Extreme weather	Involuntary migration	Natural disaster	Climate action failure	Climate action failure
3rd	Climate action failure	Natural disaster	Cyberattacks	Natural disaster	Natural disaster
4th	Interstate conflict	Terrorist attracts	Data fraud or theft	Data fraud or theft	Biodiversity loss
5th	Natural catastrophes	Data fraud or theft	Climate action failure	Cyberattacks	Human-made environmental disaster

Economic Environmental Geopolitical Societal Technological

The Evolving Risk Landscape 2016-2020 – Top five global risk in terms of impact (Source: World Economic Forum. The Global Risk Report, 2020)

	2016	2017	2018	2019	2020
1st	Climate action failure	Weapons of mass destructions	Weapons of mass destructions	Weapons of mass destructions	Extreme weather
2nd	Weapons of mass destructions	Extreme weather	Extreme weather	Climate action failure	Weapons of mass destructions
3rd	Water crisis	Water crisis	Natural disaster	Natural disaster	Biodiversity loss
4th	Involuntary migration	Natural disaster	Climate action failure	Water crisis	Extreme weather
5th	Energy price shock	Climate action failure	Water crisis	Natural disaster	Water crisis

Economic Environmental Geopolitical Societal Technological

2.2. Some of the Reasons for Risk Management Failure

- Insufficient capital – 58% of small business loan applicants sought 100,000$ or less
- Failure in communicating the risks to the top management – A manager should spend 90% of his time communicating problems
- Risk ignorance – There is deliberate ignorance which is based on social factors and ignorance as a result of impulse
- Failure to mitigate risk – With the right risk mitigation techniques, SMEs could increase revenues by 26% in 3 years and 42% in 5 years
- No concrete plan – Only 17% of organizations have a business model that investors can trust and rely on

The way we work is changing with the developments in globalization, technology, regulation and demographics; and this will have an impact in the way we work in the future. Risk and risk management remain quintessential features of successful organizational models worldwide. With an increased focus on risk identification and management, organizations are able to act more confidently on future business decisions.

Successful organizations are those that have the ability to identify and manage risks before those risks become destructive actualities that impair the organization's reputation and its ability to operate.

3. Value of ISO 31000/ISO 31004/ISO 31010 and Risk-Oriented Corporate Management Systems

ISO 31000 offers guidance on how organizations can incorporate risk-based decision-making into their governance, planning, management, reporting, policies, values, and culture. It helps organizations in establishing a risk management strategy to detect and mitigate risks in an effective manner, therefore increasing the chance of achieving their objectives.

Besides ISO standards, there are also other national-levels standards that tackle risk management and risk assessment.

NIST SP 800-30: This standard provides guidance for conducting risk assessments in federal information systems and organizations. Such guidance helps organizations determine the appropriate course of action when they face risks.

MoR: The key capabilities of MoR will enable organizations to support business change, manage risks in line with the business needs, optimize costumer experience and improve their processes on a continual basis.

COSO ERM: This standard is published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is an initiative whose mission is to provide guidelines in the fields of internal monitoring, enterprise risk management, and detection and prevention of fraud with an organization. In the context of this standard, Enterprise Risk Management (ERM) is defined as the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with the purpose of managing risks in creating, preserving, and realizing value.

NIST SP 800-30

This standard has been developed by the US National Institute of Science and Technology (NIST).

Management of Risk

The Management of Risk (M_o_R), developed jointly by the UK government and Capita, is a route map for risk management. It can help organizations in identifying, assessing, controlling risks, and putting in place effective frameworks for making informed decisions.

COSO ERM

This standard provides a perspective on current and evolving concepts of enterprise risk management and defines a "framework" which aims to help organizations in strategy-setting and decision-making.

4. Elements of a Successful Risk Management

Understand emerging risk: Gather intelligence on far-of threats

Consider extreme events: Consider unexpectedly large deviations (i.e., "fat tails" or "black swans") that could have a catastrophic impact.

Define and understand risk appetite: Provide key risk indicators in order to ensure that risk remains with the determined thresholds.

Assess and aggregate all risks: Assess correlations and more general interactions within the set of an organization's exposures; implement a "portfolio approach" to the aggregation of risks.

Ensure sound judgement: While data quantifying tools are important, they also have their limitations. Data reflect on past events and in order to predict future events, we must rely on hypothesis and interpretation. Therefore, sound judgement and quantifying tools should be part of risk management.

Foster a risk culture in the organization: Have the upper, middle, and lower management manage operational and tactical risks.

Clarification notes:

Risk appetite: The level of risk that an organization is willing to accept

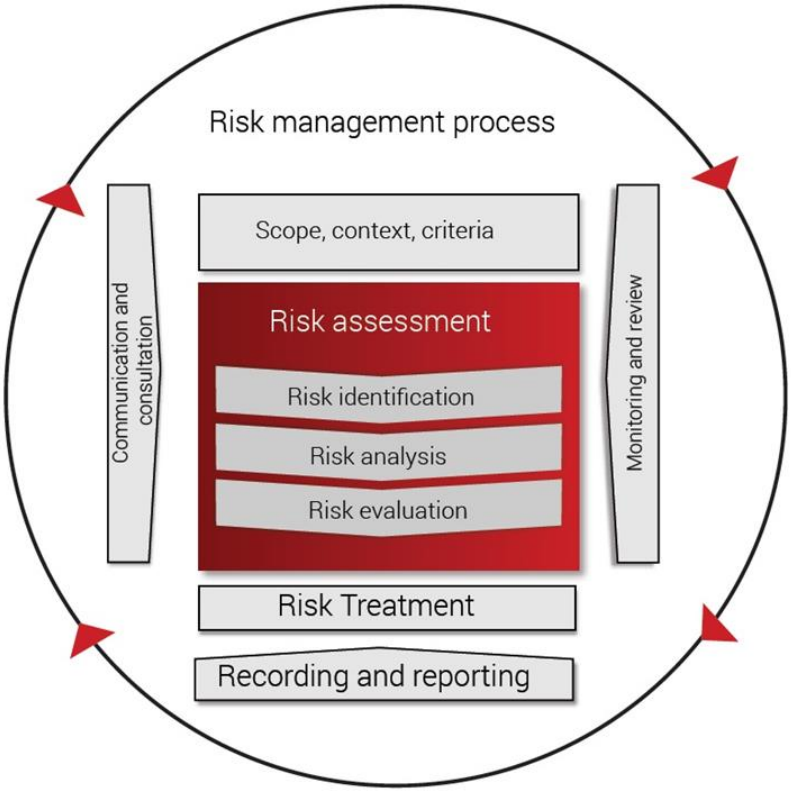
Fat-tailed distribution: The probability distribution that display a large skewness or kurtosis in comparison to a normal or exponential distribution.

Black swan: An event which can have high impacts, but whose probability of occurrence is low.

5. Risk Management Process According to ISO 31000

A risk management process should be iterative for risk assessment and risk treatment activities. If the risk assessment activities have provided sufficient evidence that the determined actions will bring risk exposure to an acceptable level, the next step is to implement risk treatment options. However, if there is insufficient evidence to determine the risk level, and if the risk treatment process appears to be unacceptable, an iteration of risk assessment will be conducted on some or all the items of the application domain. If the risk treatment option is not satisfactory, but the scope, context, criteria and risk assessment are correct, a new iteration of risk treatment will be conducted. Otherwise, a new iteration of scope, context, criteria will also have to be applied.

The effectiveness of risk treatment may depend partially on the accuracy of risk assessment. It is possible that risk treatment may not directly lead to an acceptable level of residual risk. If that is the case, a new iteration of risk assessment should be undertaken. Risk communication to the organization's interested parties is an ongoing activity, as is risk monitoring.



Risk management is a management process that stimulates the cost-effective accomplishment of an organization's objectives; furthermore, the standard also states that the purpose of risk management is the creation and protection of value. This leads us toward the question: How does a risk management process, based on ISO 31000, support organizations in the creation and protection of value, and consequently, in the achievement of organizational objectives? In addition to providing answers to such questions, ISO 31000 also provides a set of principles, a framework and a risk management process that the organizations can follow. The standard proposes 8 principles which organizations should consider when establishing their risk management framework and processes.

Furthermore, the purpose of risk management principles provided by ISO 31000 is to link the framework and practice of risk management to the organization's strategic goals.

6. Risk Categories

Some risk types presented by PECB that can be faced by organizations of any type include:

- Operational Risk
- Financial Risk
- Credit Risk
- Information Technology Risk
- Integration Risk
- Security Risk
- Legal Risk
- Strategic Risk

An organization aiming to implement a risk management process should be aware of all the risk types that have been or can be faced by the organization while they operate. This can be achieved by considering all of the past risk registers and identifying whether any risk from the past has been intertwined or is still present. In case the organization does not have risk registers at all, the top management should provide the risk management team with enough information on what risks have been faced in the past and what were their sources. In case the organization has not faced any risk in the past, they still should identify potential risks, so that the organization does not have to suffer any consequences.

Operational Risk

The loss resulting from inadequate procedures, policies, and systems within the organization is called Operational Risk.

Financial Risk

The process of coping with uncertainties that derive from financial markets. The main sources of financial risk include:

- The organization's exposure to changes in market prices;
- Actions and transactions with other organizations;
- Internal actions and organizational failures.

Credit Risk

The loss that is generated due to the inability of the counterparty to meet its' obligations is called Credit Risk.

Information Technology Risk

The operational, financial, and project failures due to the usage of new technology.

Integration Risk

The negative outcomes triggered by the integration of new processes and technology, and/or lack of communication.

Security Risk

The losses encountered due to the information security incidents or physical incidents.

Legal Risk

The risk that emerges because of the inability to comply with the applicable regulatory obligations

Strategic Risk

The following are few types of strategic risk:

- Completive Risk – The risk that you lose ground to competitors as they improve and innovate
- Change – The risk that change such as new technology will threaten your business model
- Regulatory Risk – The potential for new regulations to disrupt your business
- Political Risk – Political events and conditions can disrupt your business or impact the economics of an industry
- Economic Risk – The potential for economic conditions to affect your strategy

7. Risk Management Process

Risk identification: The identification of risks should be a formal, structured process that includes risk sources, events, their causes and their potential consequences. Simply said, risk identification is about the creation of a comprehensive list of risks (both internal and external) that the organization faces, and can involve input from sources such as historical data, theoretical analysis, expert options, and stakeholders' needs. The risk identification process enables the organization to identify its assets, risk sources, risk events, existing measures and consequences. By identifying such elements, the organization will be ready to begin the risk analysis process.

Risk analysis: The organization should analyse each risk that was identified in the previous step. Based on the level of risk that is determined after the risk analysis, the organization is able to define whether the risk is acceptable or not. As so, if the risk turns out to be unacceptable, the organization can take actions to modify the risk to correspond to the acceptable level of risk. The organization should use a formal technique to consider the consequence and likelihood of each risk. These techniques can be qualitative, semi-quantitative, quantitative, or a combination thereof, based on the circumstances and the intended use.

Risk evaluation: This step offers the organization the opportunity to have a mechanism that helps it rank the relative importance of each risk so that a treatment priority can be established.

Risk treatment: Proper risk management requires rational and informed decisions about risk treatment. Typically, such treatments include: avoidance of the activity from which the risk originates, risk sharing, managing the risk by the application of controls, risk acceptance and taking no further action, or risk taking and risk increasing in order to pursue an opportunity. Remember that organizations do not always find themselves in trouble because of their excessive and reckless behaviour. Sometimes organizations fall behind their competitors as a result of their reluctance to take risks and pursue opportunities.

Communication and consultation: Proper risk management requires structured and ongoing communication and consultation with those affected by the organization's operations. The communication seeks to promote awareness and understanding of risk and the means to respond to it, whereas consultation involves obtaining feedback and information to support decision-making.

Recording and reporting: Another step of the risk management process based on ISO 31000 is the recording and reporting, i.e. the outcomes of the risk management process are to be documented and reported through appropriate mechanisms. Recording and reporting is important for reasons such as communication of the risk management activities and outcomes pertaining to those activities throughout the organization and providing the necessary basis and information for making informed decisions.

Monitor and review: Considering that both the external and internal environment are subject to constant change, the purpose of this step is to help organizations assure and improve the quality and effectiveness of the risk management process. Monitoring includes actions such as examining the progress of treatment plans, monitoring the established controls and their effectiveness, ensuring that activities which are proscribed are being avoided, and checking that the environment has not changed in a way that affects the risks.

8. Who Shall Manage Risks?

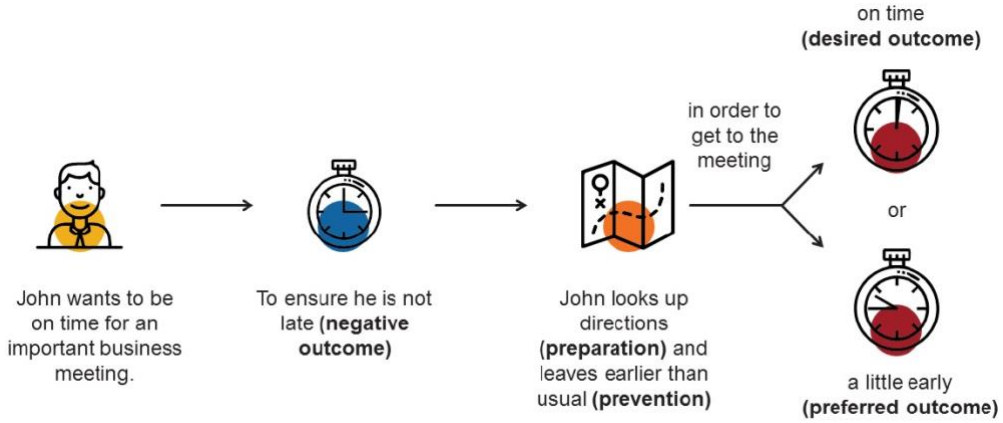
Although risk management is commonly viewed as something that solely belongs to organizations, enterprises, or companies – the opposite is true.

Risk is something people deal with on daily basis on a various front, like health, career, or personal finances. So, everyone has a share in participating in risk management.

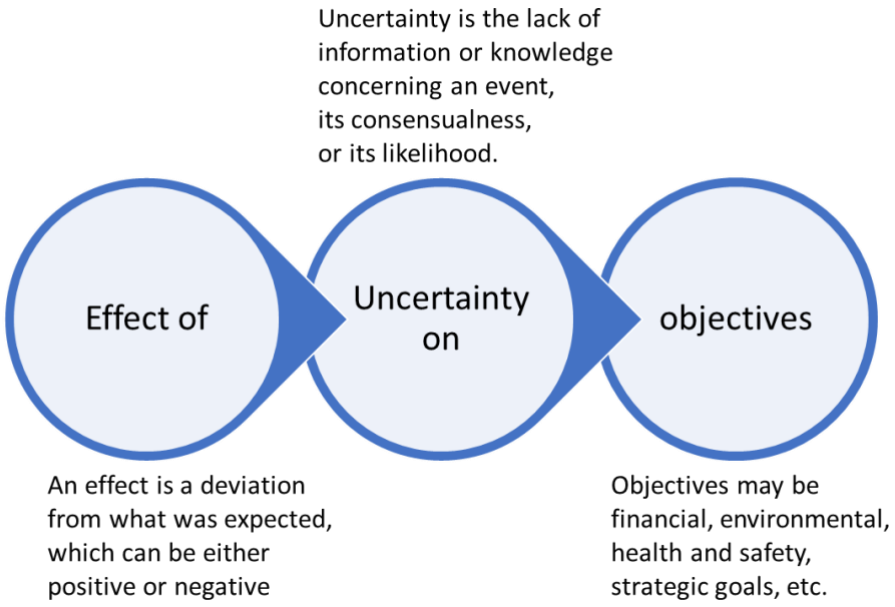
> "In addition to all the current issues specific to risk management, the risk management community must stay on the alert to all the changes the world is going through at all times, and on the watch to anticipate and remain open-minded to bring appropriate answers that the situations may dictated."

– Julia Graham, President of the Federation of European Risk Management Associations (FERMA)

9. Intuitive Risk Management



10. Definition of Risk



11. Management, Risk Management and Managing Risk

Management involves coordinated activities that direct and control an organization in pursuit of its objectives. Risk Management is an integral component of managements it involves coordinated activities concerned with the effect of uncertainty of those objectives. That is why, in order to effective, it is important that risk management is fully integrated into organizations' management system and processes.

In ISO 31000, the expression "Risk Management" generally refers to the architecture that organizations use (principles, framework and process) for managing risk effectively, and "managing risk" refers to applying that architecture to particular decisions, activities and risk.

12. Risk and Objectives

Organization of all kinds face internal and external factors and influences that make it uncertain whether, when and the extent to which, they will achieve or exceed their objectives. The effect that this uncertainty has on the organization's objective is risk

The objectives referred to ISO 31000 and ISO/TR 31004 Technical Report are the outcomes that the organization is seeking. Typically, these are the highest expression of intent and purpose, and they typically reflect its explicit implicit goals, values and imperatives, including consideration of social obligations and legal and regulatory requirements. In general, risk management is facilitated if objectives are expressed in measurable terms. There are often multiple objectives, however, an inconsistency between objectives can be a source of risk.

Risk is created or altered when decisions are made. Because there is almost always some uncertainty associated with decisions and decision making, there is almost always risk. Those responsible for achieving objectives need to appreciate that risk is an unavoidable part of the organization's activities that is typically created or altered when decisions are made. Risk associated with a decision should be understood at the time the decision is made, and risk-taking is therefore international. Using the risk management process described in ISO 31000 makes this possible.

13. Risk Owner – Definition

ISO Guide 73, clause 3.5.1.5 Risk Owner

- Person or entity with the accountability and authority to manage the risk.

PMBOOK 6th edition, 2017

- Risk owner, the person responsible for monitoring the risk and for selecting and implementing an appropriate risk response strategy.

COSO Enterprise Risk Management 2nd edition, 2011

- Risk owner, the person or entity responsible for recognizing and monitoring the status of a specific risk.

13.1. Uncertainty

Uncertainty is a term which embraces many underlying concepts. Type of uncertainty includes:

Examples of uncertainty include:

- Uncertainty as to the truth of assumptions, including presumptions about how people or systems might behave
- Variability in the parameters on which a decision is to be based
- Uncertainty in the validity or accuracy of the models which have been established to make predictions about the future
- Events (Including changes in circumstances or conditions) whose occurrence, character or consequences are uncertain
- Uncertainty associated with disruptive events
- The uncertain outcomes of systematic issues, such as shortages of competent staff, that can have wide ranging impacts which cannot be clearly defined
- Lack of knowledge which arises when uncertainty is recognized but not fully understood
- Unpredictability
- Uncertainty arising from the limitations of the human mind, for example in understanding complex data, predicting situations with long-term consequences or making bias-free judgements.

13.2. Risk Notation

Risk is often associated with the negative consequences it entails, such as the possibility of losses, injuries, or some other negative events. This connotation has lead organizations to consider risk as a barrier to the achievement of their objectives and that they should simply minimize or avoid it altogether. For these organizations, the purpose of risk management becomes to limit their exposure to risk.

However, this perception is incomplete as risk can have both positive and negative consequences. Opportunities for organizations to expand, innovate, and improve are almost always accompanied by some forms of risk. The definition of risk in ISO 31000 recognizes this by implying that risks can expose organizations to either an opportunity, a threat, or both.

Furthermore, as stated in ISO/TR 31004, understanding that risk can have positive and negative consequences is a central and vital concept to be understood by risk managers and managements.

13.3. Opportunity

Definition	• Combination of circumstances expected to be favorable to objectives
Note 1	• An opportunity is a positive situation in which gain is likely an over which on has a fair level of control.
Note 2	• An opportunity to one party may pose a threat to another
Note 3	• Taking or not taking an opportunity are both source of risk.

13.4. Threat

Definition	• Potential source of danger, harm, or other undesirable outcome.
Note 1	• A threat is a negative situation in which loss is likely and over which one has relatively little control.
Note 2	• A threat to one party may pose an opportunity to another

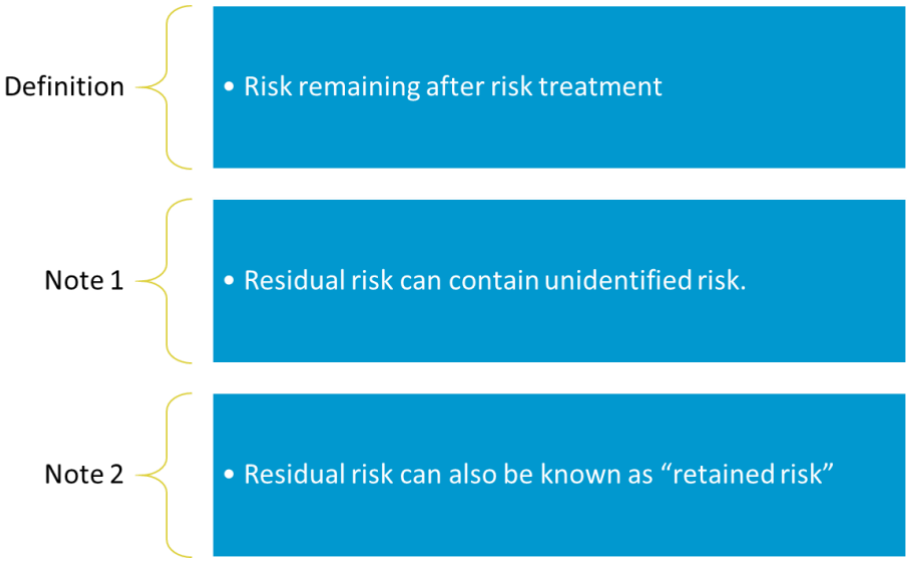
13.5. Event

Definition	• Occurrence or change of a particular set of circumstances
Note 1	• An event can be one or more occurrences, and can have several causes
Note 2	• An event can sometimes be referred to as an “incident” or “accident”.

13.6. Consequences

Definition	• Outcome of an event affecting objectives
Note 1	• An event can lead to a range of consequences.
Note 2	• An consequence can be certain or uncertain and can have positive or negative effects on objectives.
Note 3	• Consequences can be expressed qualitatively or quantitively
Note 4	• Initial consequences can escalate through knock-on effects

13.7. Residual Risk



Examples of events:

- Natural events, e.g. flooding, cold weather
- Accidents, e.g. road accident, chemical spill
- Disease or infection
- Political unrest, e.g. war, terrorism, industrial action
- Crime, e.g. violence, theft, fraud
- Economic events, e.g. recession, trade wars, bankruptcy
- Pollution or habitat destruction

Examples of possible negative consequences of events:

- Minor or major injuries or death
- Health implications
- Loss of or damage of property
- Financial loss
- Loss of livelihood or earning potential
- Inconvenience or loss of time
- Damage to the environment
- Emotional distress

Examples of possible positive consequences of events:

- Going viral on the internet
- Breakthrough in a production method

13.8. Level of Risk

Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood:

	CONSEQUENCE				
LIKELIHOOD	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Rare (1)	Low	Low	Low	Low	Low
Unlikely (2)	Low	Low	Low	Medium	Medium
Possible (3)	Low	Low	Medium	Medium	Medium
Likely (4)	Low	Medium	Medium	High	High
Almost certain (5)	Low	Medium	Medium	High	Extreme

→ Level of Risk 1 is Low

→ Level of Risk 2 is Medium

→ Level of Risk 3 is High

13.9. Risk Types

The risk types that an organization faces depend heavily on the context of that organization, its industry sector, and the environment in which it operates. Therefore, it is difficult to define a universal list of all risk type, perhaps with the expiation of one risk that impacts all organization.

Operational Risk

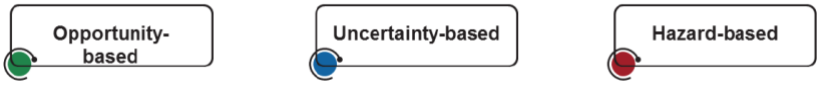
Operational risk involves any event that disrupts the normal operations of the organization. Operational risk can also include employee errors, fraud, or criminal activities. These types of risks happen everywhere, not just in a business environment, for example:

- Injuries sustained from a design weakness in playground equipment
- Engineering flaws resulting in a mass recall of motor cars
- Poor labelling on pharmaceutical packaging leading to the wrong dose being administered
- Swabs or instruments left in a patient after surgery

Attention to safety has a crucial role in mitigating these risks.

What we can take as an example to use a different approach to define risk types as Australian government practices.

The following is a classification of risk types by the Australian government:



Opportunity-Based Risk

An organization faces opportunity-based risks when it takes one opportunity over another, and by doing so, the organization has the risk of:

- Receiving results, it did not expect
- Missing out on better opportunities
- Examples of opportunity-based risks include relocation, introduction of a new product line, purchase of a new property, etc.

Uncertainty-Based Risk

An organization faces uncertainty-based risks when it deals with an unexpected or unknown event. These events are hard to predict and it can be difficult to control the damage caused by them. Examples include:

- Unpredicted financial loss due to bankruptcy, an economic downturn, or other reasons
- Destruction by natural calamities
- Loss in market share due to new entrants in the market or due to changing customer habits

Organizations can take several measures to reduce the impact of uncertainty-based risks, for example:

- Analyse the business environment to identify customer expectation and trends in the market
- Establish an emergency response plan, a business continuity plan, etc. Check the organization's financial health
- Establish a feedback culture

Hazard-Based Risk

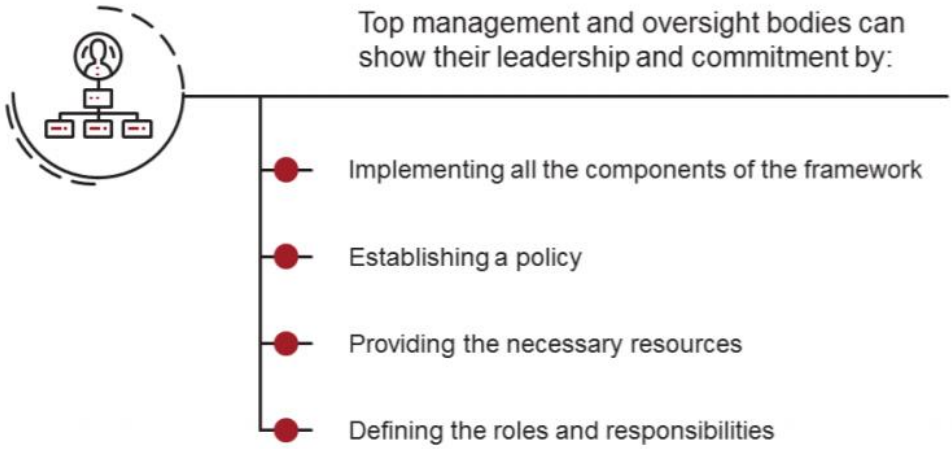
When an organization faces dangerous situations in the workplace, it means that it is prone to hazard-based risks. Example of this type of risk include:

- Physical hazards (e.g. extreme weather)
- Chemical hazards (e.g. toxic chemicals)
- Biological hazards (e.g. bacteria)
- Ergonomic hazards (e.g. poor workplace design)
- Psychological hazards (e.g. stress, discrimination, burnout)

14. Leadership and Commitment

Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organizational activities and should demonstrate leadership and commitment by:

- customizing and implementing all components of the framework
- issuing a statement or policy that establishes a risk management approach, plan or course of action
- ensuring that the necessary resources are allocated to managing risk
- assigning authority, responsibility and accountability at appropriate levels within the organization.



In order for leadership and commitment to be effective, the organization's top management and other relevant bodies need to present the stakeholders with the method of managing risk and documenting and communicating it appropriately. Leadership commonly involves changes in behaviour, culture, policy, processes, and expected performance in managing risks. They will all be reflected in the risk management framework. Leadership and commitment intentions can be best expressed in a short policy statement that should be communicated widely.

The demonstration of leadership and commitment should meet the following criteria:

1. It should be aligned with the organization's strategic plan, objectives, policies, styles of communication, and management systems.
2. It should be compatible with the risk criteria determined by the top management and oversight body.
3. It should, in addition, meet the principles of ISO 31000 to attempt for excellence in risk management.
4. It should be tested for comprehension inside and outside the organization and it should be easy to communicate.
5. It should have reasonable expectations regarding its successful application.
6. It should address the responsibilities of risk owners.

15. Integrating the Risk Management Framework into an Organization

Structures differ depending on the organization's purpose, goals and complexity. Risk is managed in every part of the organization's structure. Everyone in an organization has responsibility for managing risk.

Governance guides the course of the organization, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose. Management structures translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability.

Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.

Understanding organizational structures and context

- Integrating risk management relies on an understanding of organizational structures and context

Defining roles and responsibilities

- Determining risk management accountability and oversight roles within an organization are integral parts of the organization's governance.

Customizing risk management

- Integrating risk management into an organization is a dynamic and iterative process, and should be customized to the organization's needs and culture

16. Defining the Risk Management Framework

Considering the purpose of the framework, which is to assist the organization in integrating risk management into significant activities and functions, the design process should reflect where and how decisions are taken and should take into account any compliance obligations which the organization should respect.

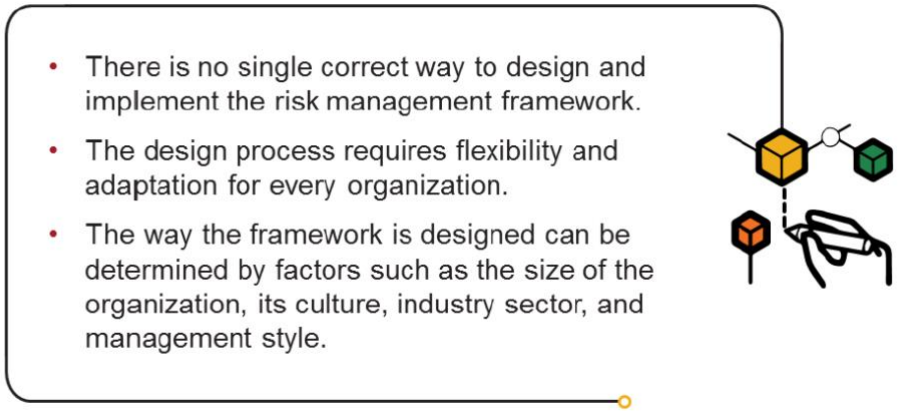
To design the new framework, the following must be specifically evaluated:

- Principles and attributes, as described in ISO 31000
- The initial framework, the evaluation of which should, in particular, compare the current practices with the recommendations of the following sub-clauses of ISO 31000:
- Clause 5.4.2 Articulating risk management commitment
- Clause 5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities

- Clause 5.4.4 Allocating resources
- Clause 5.4.5 Establishing communication and consultation

The procedure, the evaluation of which should compare the factors of the existing processes with those outlined in ISO 31000, clause 6, as well as the principles that drive and provide the rationale for the process with the principles set out in ISO 31000, clause 4 (e.g., whether this process is actually implemented to decision-making at all levels), should:

- Evaluate whether or not the current process provides decision-makers with the information (about risk) they need to make better decisions and meet or exceed objectives
- Evaluate whether the existing techniques for managing risk sufficiently address interrelated risks and risks that occur in multiple locations



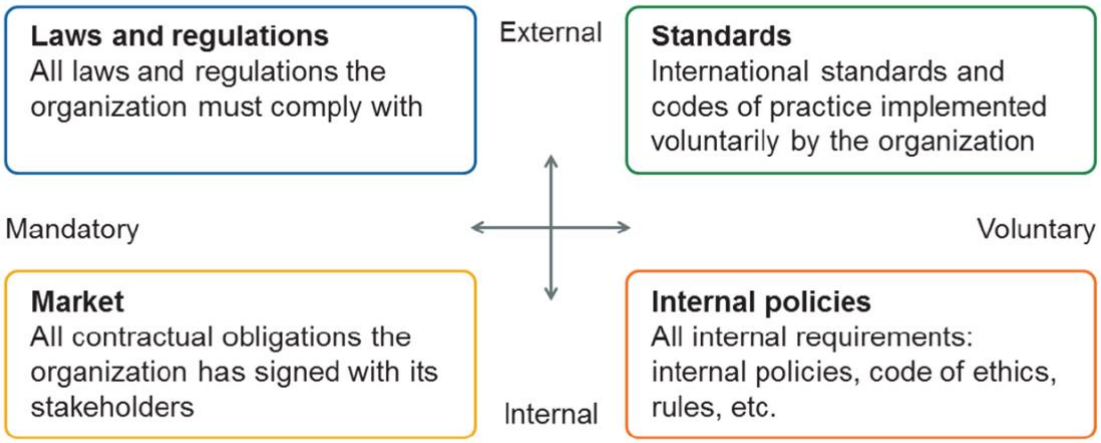
17. Identifying and Analysing the Stakeholders

First, the risk management team should identify all stakeholders and their requirements and expectations regarding risk management. Second, the risk management team should analyse the stakeholders' risk management issues and confirm whether the organization responds to their concerns. This activity can be done by sending a questionnaire, conducting interviews, or by facilitating focus groups. One should also be aware of the service agreements concluded and analyse the requirements (explicit or implicit) that they contain. Lastly, the risk management team should define what is expected from different stakeholders within the project, including their roles, responsibilities, and the required levels of participation. It should, thereby, come to a consensus on their involvement with the stakeholders during the planning stage.

The organization must dedicate a considerable amount of time in the project in order to support the stakeholders in their assigned tasks (answering questions, consolidating reports, presenting project progress, etc.).

Note: Many ISO standards use the term "interested party" instead of "stakeholder." These terms, as acknowledged by ISO, are synonymous and can be used interchangeably.

18. Identifying and Analysing the Requirements Related to Risk Management



Laws and regulations: The organization must comply with the applicable laws and regulations. In most countries, the implementation of an ISO standard is a voluntary decision, not a legal requirement. In all cases, laws take precedence over standards.

Standards: Organizations must comply with a set of international standards and codes of practice related to their industry sector. Although the implementation of regulatory frameworks is a voluntary choice, from the risk management point of view, they become obligations to comply with (e.g., the risk of losing a certification in case of serious failure to comply with standard requirements).

Market: Market requirements include all contractual obligations that the organization has signed with its stakeholders. A breach of contractual obligations may result in penalties (when stated in the contracts) or civil suits for damages. Market requirements are all implicit rules that an organization should fulfil in order to conduct business. For example, although the organization has no contractual obligation to deliver its products as planned, it goes without saying that this is a commercial policy basis to meet the scheduled delivery times and failing to do so will lead to a loss of market share, customer trust, profit, etc.

Internal policies: Internal policies are principles, rules, and guidelines that include all the requirements defined within the organization: internal policies (human resources, supply chain, etc.) ethical codes, work rules, etc. It is worth noting that not complying with internal policies does not necessarily involve any legal implications.

19. Articulating Risk Management Commitment

The commitment should include, but not be limited to:

- *the organization's purpose for managing risk and links to its objectives and other policies;*
- *reinforcing the need to integrate risk management into the overall culture of the organization;*
- *leading the integration of risk management into core business activities and decision-making;*
- *authorities, responsibilities and accountabilities;*
- *making the necessary resources available;*
- *the way in which conflicting objectives are dealt with;*
- *measurement and reporting within the organization's performance indicators*
- *review and improvement.*

Top management and oversight bodies, where applicable, should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an organization's objectives and commitment to risk management.

The risk management commitment should be communicated within an organization and to stakeholders, as appropriate.

20. Risk Management Policy and Risk Management Manual

Risk management policy

- Is typically a short document (2 pages)
- Is an informative organizational document intended for the organization's internal and external stakeholders.
- Describes briefly its purpose and the objectives of the organization toward risk management.

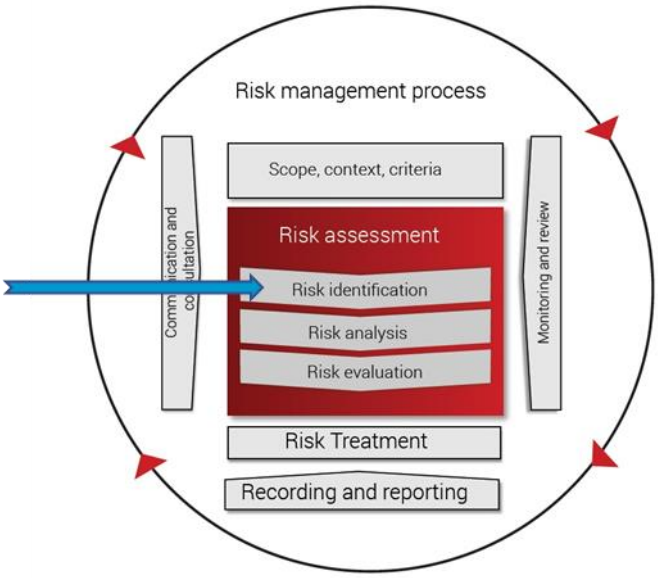
Risk Management Manual

- Is more extensive (10-15 pages) than a risk management policy
- Provides information on the organization's scope, purpose, policy statement, objectives, and roles and responsibilities.
- Describes in detail the risk management process on how to identify, assess, and treat risk.
- Can contain appendixes, annexes, and other supporting documents.

21. Techniques of Risk Management

21.1. Risk Identification

Relevant, appropriate and up-to-date information is important in identifying risks. The organization should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.



Techniques for identifying risks usually make use of the knowledge and experience of a variety of stakeholders.

They include considering:

- what uncertainty exists and what its effects might be
- what circumstances or issues (either tangible or intangible) have the potential for future consequences
- what sources of risk are present or might develop
- what controls are in place and whether they are effective
- what, how, when, where, and why events and consequences might occur
- what has happened in the past and how this might reasonably relate to the future
- which human aspects and organizational factors might apply

Physical surveys can also be useful in identifying sources of risk or early warning signs of potential consequences. The output from risk identification can be recorded as a list of risks with events, causes and consequences specified, or using other suitable formats.

Whatever techniques are used, risk identification should be approached methodically and iteratively so that it is thorough and efficient. Risk should be identified early enough to allow actions to be taken whenever possible. However, there are occasions when some risks cannot be identified during a risk assessment. A mechanism should therefore be put in place for capturing emerging risks and recognizing early warning signs of potential success or failure.

21.1.1. Identification of Assets

An asset is an item, thing or entity that has potential or actual value to an organization. The value will vary between different organizations and their stakeholders, and can be tangible or intangible, financial or non-financial.

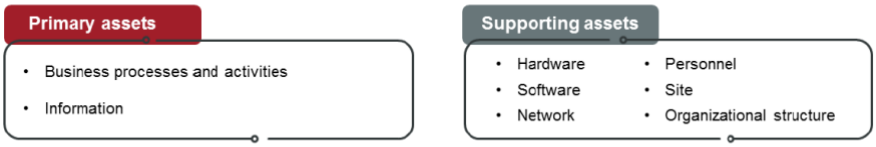
The period from the creation of an asset to the end of its life is the asset life. An asset's life does not necessarily coincide with the period over which any one organization holds responsibility for it; instead, an asset can provide potential or actual value to one or more organizations over its asset life, and the value of the asset to an organization can change over its asset life.

In order to identify assets, the scope for the risk assessment needs to be considered and the assets within the established scope should be identified. As an output, a list of assets to be risk-managed and a list of business processes related to assets and their relevance will be generated.

The identification of assets must be performed at a level of detail that provides sufficient information for risk evaluation. However, the identification of assets should be limited to those that have the most important value to the organization.

21.1.2. Type of Assets

The level of detail used during asset identification has a vital effect on the amount of information collected during risk assessment. There are two types of assets:



21.1.3. Identification of Supporting Assets

Category	Definition	Examples
Hardware	All physical elements supporting processes	Laptop, computer, personal digital assistant (PDA)
Software	All Programs contributing to the operation of a data processing set	Database management software, groupware, web server software
Network	All telecommunication devices used to interconnect several physical remote computers or elements of an information system	Public Switching Telephone Network, Ethernet, Wi-Fi, FireWire
Personnel	All groups of people involved in the information systems	Top Management, project leader, risk manager, system administrator
Sites	Physical places where the operation take place	Urban area, buildings, utilities
Organization Structure	Organizational framework, consisting of all functional and professional or technical discipline structures assigned to a task and the procedures controlling these structure	Head office, IT management, purchasing management, business unit management

21.1.4. Asset Valuation

Organizations value their assets in order to assess the significance of processes and other operational activities that involve such assets. Organizations can have different assets, including monetary and non-monetary assets.

Monetary assets should be valued by using a currency that best suits the organization's needs and operations. Examples of monetary assets are cash, investments, accounts receivable, and notes receivable.

A value range should be assigned for each asset, be it qualitative or quantitative. The type of scale used to value assets should be chosen carefully because it affects the asset's performance. Both scale types can be used for the same asset, if necessary.

Organizations should establish relevant criteria to value their assets. This is often considered the most difficult part of the asset evaluation because different people within the organization can value assets differently and establish different criteria based on their perceptions. A possible type of criteria that can be used to determine the value of an asset is the original cost of the asset or the replacement or re-creation cost. Sometimes, the value of an asset can be abstract, such as the value of the organization's reputation or international recognition.

The organization must identify the value of its assets by developing a scale of values.

The scales of the value of assets must:

- Integrate the difference properties that could affect the confidentiality, integrity and availability of significant assets.
- Consider asset dependencies Asset Valuation – Tangible assets valuation

According to the Oxford Dictionary of Economics, tangible assets are assets that can be physically touched (such as equipment, plant, property). When calculating the values of tangible assets, organizations need to:

- Identify the tangible and intangible assets in their balance sheet
- Deduct the value of the intangible assets from the total asset value
- Deduct the value of the liabilities

The resulting number is the net tangible assets or asset valuation

For example:

- Total asset value: $8 million
- Intangible assets value: $2.5 million
- Total liabilities: $2 million
- **Tangible assets valuation: $3.5 million**

Assets can be categorized into two broad categories: tangible and intangible. Tangible assets are those assets that are physical, such as machinery. These types of assets can be categorized as current assets (assets which are expected to be converted into cash within a year, like inventory) and fixed assets (assets which are considered for long-term use and unlikely to be converted into cash quickly, like land, buildings, vehicles, etc.). In the example shown above, the intangible assets value ($2.5 million) is deducted from the total asset value ($8 million), leaving the organization with $5.5 million. The amount of total liabilities ($2 million) is, then, deducted from the $5.5 million. The end result gives the tangible assets valuation, which is $3.5 million.

21.1.5. Asset Valuation – Intangible Assets Valuation

To estimate the monetary value of intangible assets, **Direct Intellectual Capital (DIC)** methods enable the identification of the various components of intangible assets and their evaluation either as an aggregated coefficient or individually.

Scorecards (SCs) report the identified components of intangible assets, indicators, and indices generated in scorecards or as graphs. Despite being quite similar to DIC methods, SCs make no estimates of the monetary value of intangible assets. On the other hand, **Market Capitalization (MC)** computes the value of intangible assets as the difference between an organization's market capitalization and its stockholders' equity.

Lastly, the **Return on Assets (ROA**) is generated by dividing the average pre-tax earnings to the average total of tangible assets. This value is then compared with the industry average and the difference is multiplied by the organization's average total of tangible assets to compute the average annual earnings from intangible assets. The value estimation of intangible assets is derived by dividing the above-average earnings to an interest rate or the organization's average cost of capita

Assets that have no physical form are classified as intangible assets (e.g., trademarks, patents, logos, franchises). Some of the measuring approaches for intangible assets are:

- Direct Intellectual Capital (DIC) methods
- Scorecards (SCs)
- Market Capitalization (MC)
- Return on Assets (ROA)

21.1.6. Scale of Asset Values

After establishing the criteria, the organization should agree on scale to be used on an organization-wide level. The first step is to decide on the number of levels to be used. There are no rules with regard to the most appropriate number of levels.

Example:

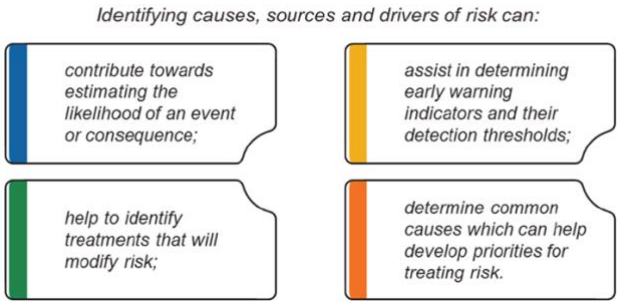
Scale	Asset Value
Low	0-3
Medium	4-6
High	7-10

21.1.7. Determination of Sources, Causes and Drivers of Risk

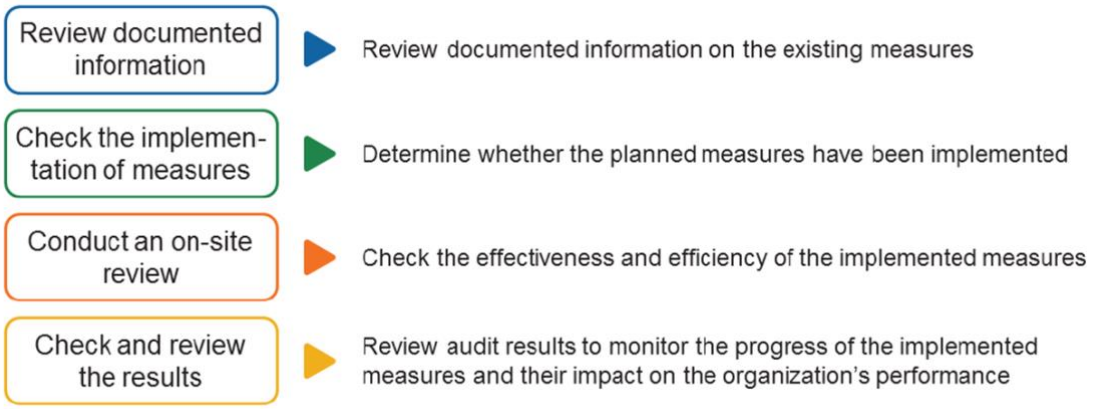
All sources of risk, areas of impacts, events, causes, and potential consequences should be identified by the organization in order to have a comprehensive list of risks based on those events that may prevent or delay the achievement of objectives.

Sources of risk can include events, decisions, actions and processes, both favourable and unfavourable, as well as situations that are known to exist but where outcomes are uncertain.

Events and consequences can have multiple causes or causal chains. Risk can often only be controlled by modifying risk drivers. They influence the status and development of risk exposures, and often affect more than one risk. As a result, risk drivers often need more and closer attention than sources of individual risks.



21.1.8. Investigation of the Effectiveness of Existing Controls

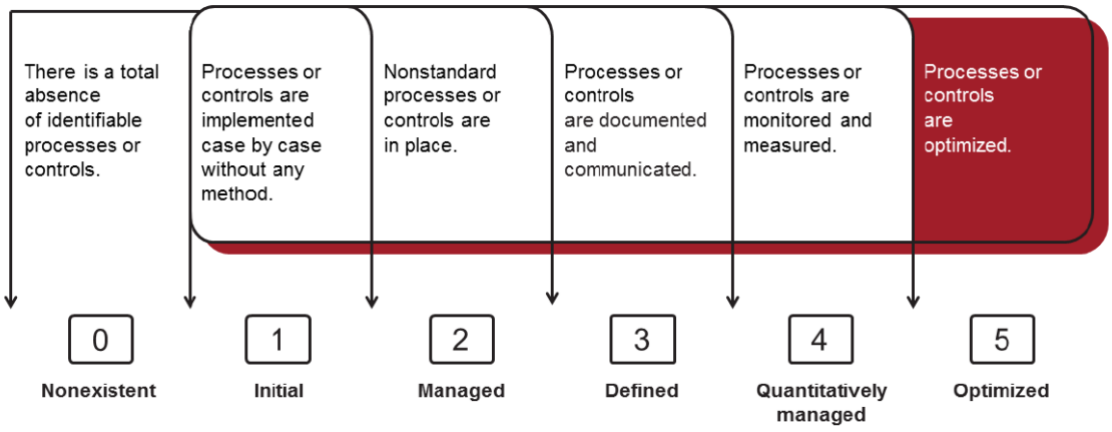


How can an organization conduct the above-mentioned activities?

- Review documented information: Review the risk treatment implementation plans
- Check the implementation of measures: Check, with the Lead Risk Manager and other personnel, which measures are implemented to ensure the effectiveness of the risk management process (e.g., an organization outsourcing its marketing activities to a third-world country can implement a data protection policy that prohibits the unauthorized access to the personal data of the organization's customers.)
- Conduct an on-site review: Review whether the measures in place are effective and efficient. The organization can compare the likelihood of risk occurrence before and after the implementation of the policy.
- Check and review the results: Use a checklist to determine if all ISO 31000 recommendations have been followed; take the respective corrective actions if the ISO 31000 recommendations have not been followed accordingly.

21.1.9. Identification of the Level of Maturity

Existing Processes or controls can be evaluated based on maturity levels:



0. Nonexistent: The organization is not aware that there is a total absence of the identifiable process or control.

1. Initial: The organization has some processes or controls that are implemented but there is no standardized procedure to do this.

2. Managed: The organization has some processes or controls that are implemented using the same procedure, but there are no training and communication sessions performed with regard to these procedures. People implementing these processes or controls rely on personal knowledge, where the probability of error is high.

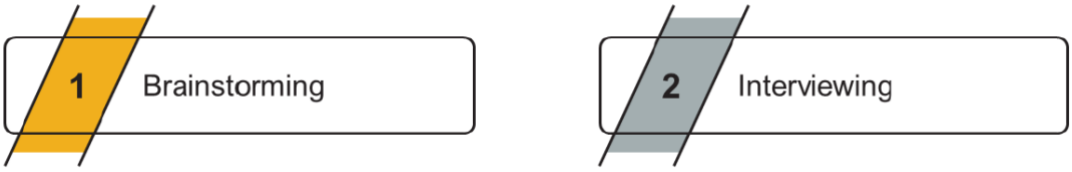
3. Defined: The organization has standardized, documented, and communicated the procedure in the training sessions. However, there is still a margin for error since these procedures are used only on individual initiatives.

4. Quantitatively managed: The organization is able to monitor and measure whether these processes or controls are implemented as required and take action when procedures are not fully functional. The organization constantly improves these processes or controls but there is limited or partial use of automation and tools.

5. Optimized: The organization's processes or controls have reached a top-quality level following continual improvement and compliance with best practices. Computers are being used to automate integrated workflow in order to improve quality and efficiency and allow the organization to adapt quickly to new situations.

21.1.10. Risk Identification Techniques

Two of the most well-known information gathering techniques are:



21.1.11. Brainstorming

Brainstorming is a process used to stimulate and encourage a group of people to develop ideas related to one of more topics of any nature. The term "brainstorming" is often used very loosely to mean any type of group discussion, but effective brainstorming requires a conscious effort to ensure that the thoughts of others in the group are used as tools to stimulate the creativity of each participant. Any analysis or critique of the ideas is carried out separately from the brainstorming.

This technique gives the best results when an expert facilitator is available who can provide necessary stimulation but does not limit thinking. The facilitator stimulates the group to cover all relevant areas and makes sure that ideas from the process are captured for subsequent analysis.

Brainstorming can be structured or unstructured. For structured brainstorming the facilitator breaks down the issue to be discussed into sections and uses prepared prompts to generate ideas on a new topic when one is exhausted.

It has been demonstrated that, in practice, groups generate fewer ideas than the same people working individually. For example:

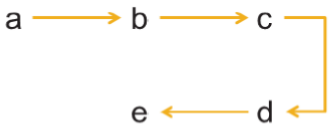
- in a group, people's ideas tend to converge rather than diversify
- the delay in waiting for a turn to speak tends to block ideas
- people tend to work less hard mentally when in a group

21.1.12. Structured or Semi-Structured Interviews

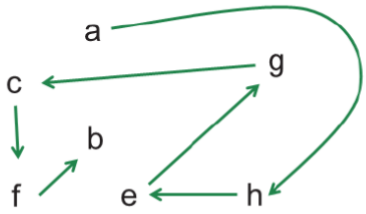
In structured interviews, the interviewer asks a set of predetermined questions in a standardized order, which does not allow space for the interviewee to deviate from the schedule or the interviewee’s questions. Structured interviews are not flexible. Thus, the interviewer cannot ask impromptu questions and has to follow the given interview guide.

In semi-structured interviews, the interviewer asks a few fixed questions. There is, however, flexibility to pose other questions and have a free-flowing conversation with the interviewee. These interviews allow more space for the interviewee to answer on their own terms, as well as offer the opportunity to identify new ways of seeing and understanding the topic at hand.

In a structured interview, individual interviewees are asked a set of prepared questions.



A semi-structured interview is similar, but allows more freedom for a conversation to explore issues which arise.



In structured interviews, the interviewer asks a set of predetermined questions in a standardized order, which does not allow space for the interviewee to deviate from the schedule or the interviewee's questions. Structured interviews are not flexible. Thus, the interviewer cannot ask impromptu questions and has to follow the given interview guide.

In semi-structured interviews, the interviewer asks a few fixed questions. There is, however, flexibility to pose other questions and have a free-flowing conversation with the interviewee. These interviews allow more space for the interviewee to answer on their own terms, as well as offer the opportunity to identify new ways of seeing and understanding the topic at hand.

21.1.13. Individual and Group Interviews

Although there are doubts cast on the value of detailed questions addressed to people that have no professional experience on matters of risk, research shows that it is important to get the opinion of interested parties, whether they are experts or not, regarding the activities they do or tasks they perform. Individuals responsible for business processes will provide a much more business-oriented view on risks, e.g., the public relations officer will indicate concerns about the reputational risk to which the organization is exposed.

Individual interviews

The most significant advantage of individual interviews is that interviewing only one person at a time allows the interviewer to obtain more detailed information about risk. In this way, the interviewer will be able to get a more comprehensive understanding of the organization and the risks it is exposed to. The interviewer is able to read the body language of the interviewee and can probe for explanations of responses. However, the interview length can be time-consuming if there are a lot of people to be interviewed.

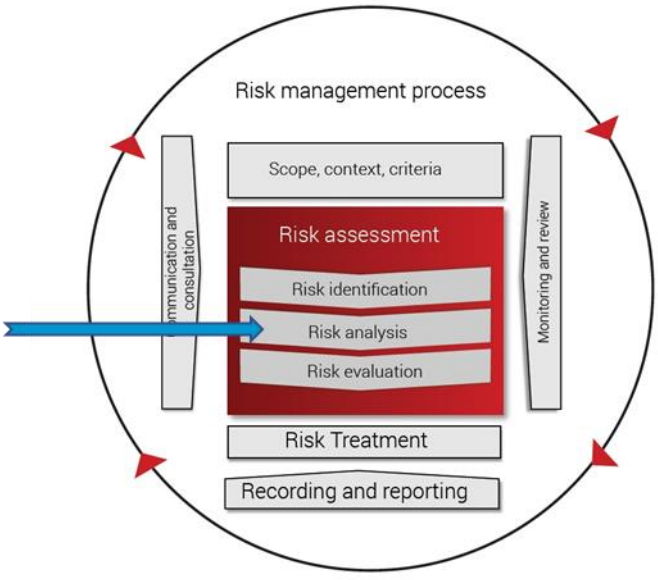
Group interviews

Group interviews are helpful when there is little time to conduct individual interviews or when the interviewer wants to examine the interaction between the group members. However, group interviews can produce unnatural responses, since a dominant member of the group may influence the response of others, known otherwise as the “bandwagon effect.”

21.2. Risk Analysis

Risk analysis should consider factors such as:

- The likelihood of events and consequences
- The nature and magnitude of consequences
- Complexity and connectivity
- Time-related factors and volatility
- The effectiveness of existing controls
- Sensitivity and confidence levels



Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

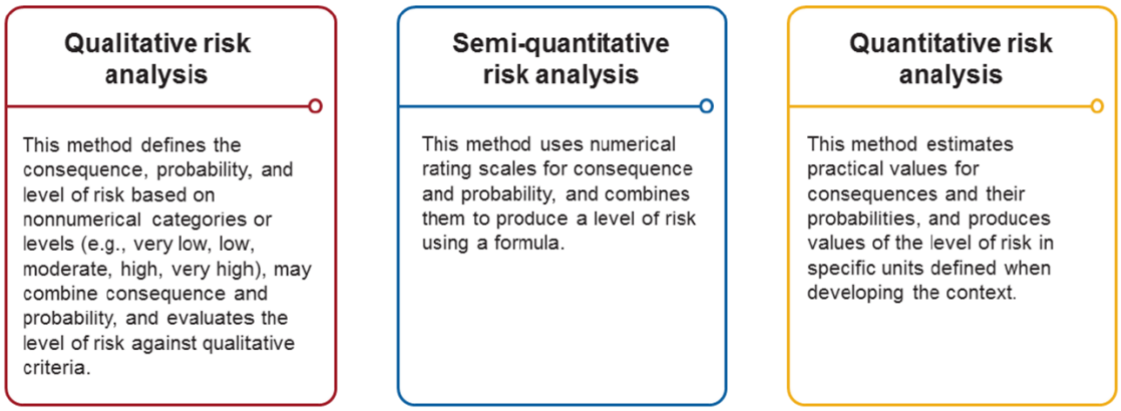
Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made and the options involve different types and levels of risk.

21.2.1. Selecting a Risk Analysis Approach

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information and the resources available.

Analysis techniques can be qualitative, quantitative or a combination of these depending on the circumstances and intended use.

21.2.2. Qualitative, Semi-Quantitative and Quantitative Risk Analysis



Qualitative analysis

This type of analysis supports the communication of risk results to decision-makers. When using a qualitative approach to risk analysis, a clear explanation of all the terms employed and the basis for all criteria should be recorded because, unless each value is clearly defined or characterized by meaningful examples, different experts relying on their individual experiences could produce significantly different results. To counter this and to increase the chances for repeatability and reproducibility, explanatory notes for the assessed values can be written (e.g. explaining that X value is high because of Y or Z reasons) by using properly defined functions to combine qualitative values.

Semi-Quantitative analysis

Scales may be linear, logarithmic, or have some other relationship; the formulas used can also vary. This type of analysis can provide the benefits of both quantitative and qualitative risk analyses.

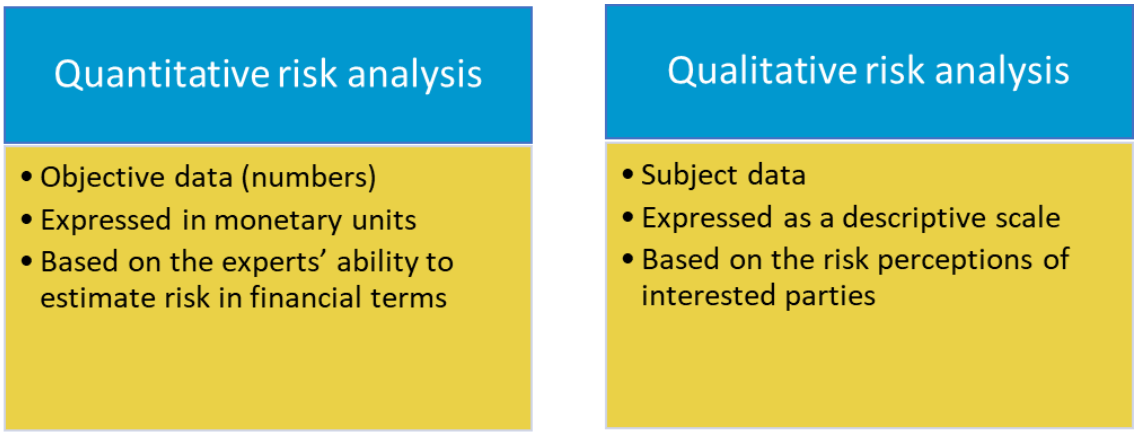
Quantitative analysis

A purely quantitative risk analysis may not always be possible or advisable. Some of the reasons for this include insufficient information about the system or the activity being analysed, lack of data, biases, assumptions, or beliefs of those involved. Another reason can be the fact that the costs can outweigh the benefits of such an analysis. Furthermore, the outcome of the quantitative results may not always be clear and may require interpretation and explanation, particularly to explain the assumptions and constraints on using the results. Under such circumstances, a comparative semi-quantitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

Where full quantification has been carried out, it needs to be acknowledged that the calculated levels of risk are estimated. One should be careful to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

21.2.3. Qualitative and Quantitative Risk Analysis

As already shown, risk assessment can be performed in several ways, including qualitatively, semi-quantitatively and quantitatively.



Each of the approaches presented on the slide has its advantages and disadvantages. The degree of detail, rigor, repeatability and reproducibility required depends on the circumstances, the availability of reliable data, and the decision-making needs of the organization. The appropriate approach can be selected based on the organization's (internal and external) context and risk exposure.

21.2.4. Biases in Risk Analysis

As in most human activities, biases can become present during risk analysis. Risk managers can overestimate some risks, while underestimating other more consequential risks. Therefore, the

question becomes not whether biases exist, but rather how well the risk manager can effectively counteract those biases.

In the following slides, we take into consideration three groups of biases:

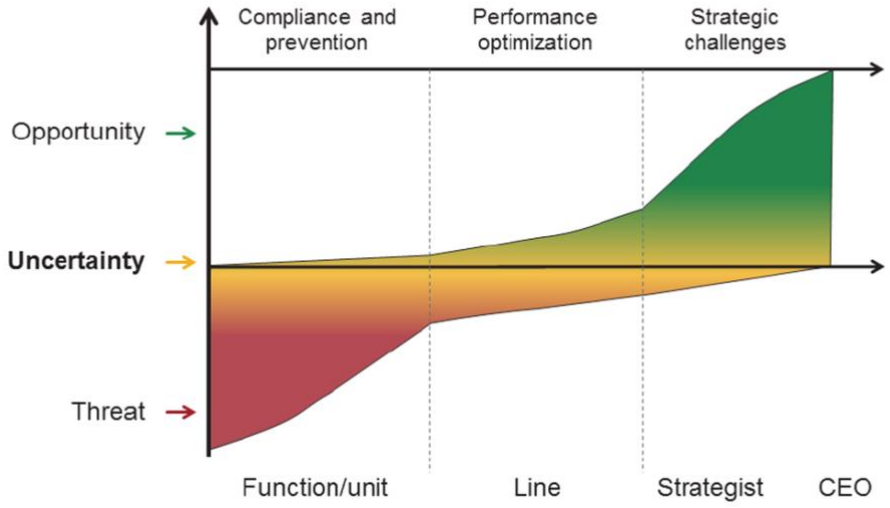
- Motivation biases
- Cognitive biases
- Group-specific biases

Risk managers should be aware of the most significant motivational, cognitive, and group-specific biases. Having an understanding of these biases and how they can affect the risk analysis process, risk managers can take appropriate actions to mitigate their negative effects, thus enhancing the decision-making process.

This list of biases is not exhaustive; there may be other biases which can influence risk analysis. Risk managers are strongly encouraged to further explore the topic of biases

21.2.5. Risk Perception in the Organization

The way risk is perceived varies within the organization and its levels (board level, executive level, operational level, etc.) depending on the perspective of the evaluator. Furthermore, how risk-averse employees are or their attitude toward risk depends on their responsibilities and tasks. Typically, the board is more of a “risk taker” as opposed to the middle management who tends to be more risk-averse. This is because the board level acts strategically; they are more focused on seizing opportunities (upside risks). The operational level, on the other hand, is more focused on protecting the organization from negative events and preventing them from occurring (downside risks).



21.2.6. Identifying Consequences

Based on the information collected from the risk identification stage, the organization proceeds with the identification of the consequences based on risk scenarios. A risk scenario is the description of a risk exploiting a weakness or set of weaknesses that creates or may create negative consequences.

The consequences of the occurrence of a risk scenario may be evaluated differently, depending on the stakeholders' involvement in risk assessment. The significant impacts on the organization should be documented accordingly.

The consequences of a risk scenario are determined by using the impact criteria defined during the context establishment phase. An impact may derive from one or more aspects. Consequences can be calculated on the basis of financial securities or qualitative scales. These effects may be temporary or permanent, as is the case with the destruction of an asset.

21.2.7. Risk and Consequences

Risk	Consequence
Theft of equipment	Monetary losses
Social unrest	Market uncertainty, financial losses
Unethical behavior from personnel	Lawsuits, reputational damage
Hacker	Information theft
Bad weather	Bad corps

The following is a list of several potential consequences that may affect the organization:

- Financial losses
- Loss of an asset or its value
- Loss of customers or suppliers
- Prosecution and penalties
- Loss of competitive advantage
- Loss of effectiveness or efficiency
- Service interruption
- Inability to provide a service
- Loss of brand image, reputation, or credibility
- Disruption of operations
- Disruption of operations of external stakeholders (suppliers, customers, etc.)
- Violation of laws or regulations or inability to fulfil legal obligations
- Inability to meet contractual obligations

21.2.8. Criteria for Identifying Consequences

Organizations should identify the operational consequences of incident scenarios in terms of:

- The time lost (working time)
- The time needed to investigate the incident and repair the damage

- The financial cost to repair the damage
- The lost opportunities
- The health and safety of stakeholders
- The damage to reputation

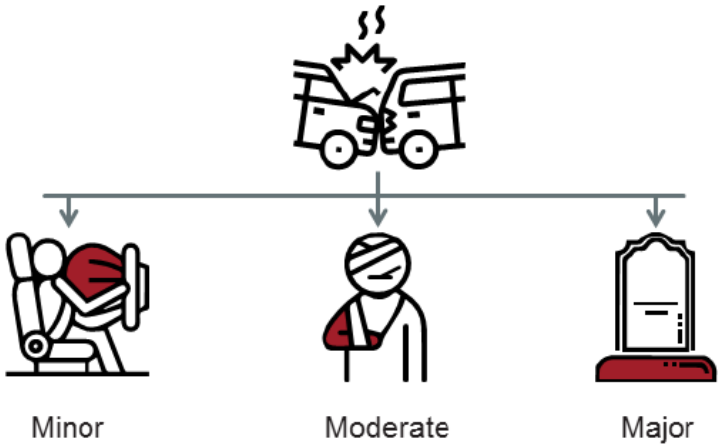
The consequences of an incident may be assessed differently, depending on the stakeholders involved in the risk assessment process. The significant impacts on the organization should be documented. In this way, the different areas that may be impacted and provide the justifications of security needs are shown.

21.2.9. Assessing Consequences

Consequence analysis can vary from a description of outcomes to detailed quantitate modelling or vulnerability analysis. Consequential effects (domino or knock-on effects) where one consequence leads to another should be considered where relevant.

Risk can be associated with a number of different types of consequences, impacting different objectives. The types of consequence to be analysed should have been decided when planning the assessment. The context statement should be checked to ensure that the consequences to be analysed align with the purpose of the assessment and the decisions to be made. This can be revisited during the assessment as more is learned.

21.2.10. Expressing the Magnitude of Consequences



The magnitude of consequences can be expressed quantitatively as a point value or as a distribution. A distribution can be appropriate where:

- The value for the consequence is uncertain
- The consequences vary depending on circumstances
- The parameters that affect consequences vary

Consideration of the full distribution associated with a consequence provides complete information. It is possible to summarize the distribution in the form of a point value such as the expected value (mean), variation (variance) or the percentage in the tail or some other relevant part of the distribution (percentile).

21.2.11. Expressing the Magnitude of Consequences (Negative)

			Consequence				
Scope	**Measure**	**Scenario**	Very high (a)	High (b)	Moderate (c)	Low (d)	Very low (e)
Reputation	Employee commitment	Key personnel turnover	20%	14%	7%	4%	2%
Occupational health and safety	Work safety	Workplace incidents	Casualty	More than one major wound	More than one minor wound	Minor wound	Local physical damage only

21.2.12. Expressing the Magnitude of Consequences (Positive)

			Consequence				
Scope	**Measure**	**Scenario**	Very high (a)	High (b)	Moderate (c)	Low (d)	Very low (e)
Customers	Retail customer growth	New customers and retention of existing customers	+18%	12-18%	6-12%	3-6%	1.5-3%
Reputation	Public relations	New marketing campaign in social media	More than 10M views on social media	More than 5M views on social media	More than 2M views on social media	More than 1M views on social media	Less than 1M views on social media

21.2.13. Analysing the Likelihood

Likelihood can refer to the likelihood of an event or to the likelihood of a specified consequence. The parameter to which a likelihood value applies should be explicitly stated and the event or consequence whose likelihood is being stated should be clearly and precisely defined. It can be necessary to include a statement about exposure and duration to fully define likelihood.

21.2.14. Describing the Likelihood

Likelihood can be described in a variety of ways, including as an expected probability or frequency or in descriptive terms (e.g. “highly likely”).

Where a descriptive term is uses, its meaning should be defined. There can be uncertainty in the likelihood which can be shown as a distribution of values representing the degree of belief that a particular value will occur. Where a percentage is used as a measure of likelihood the nature of the ratio to which the percentage applies should be stated.

21.2.15. Assessing the Likelihood

After identifying the relevant scenarios and estimating their consequences, the probability of the occurrence of each scenario should be estimated. It is necessary to estimate the realistic probability of an event and the impacts associated with the already implemented controls or measures.

Likelihood	Probability	Possible example event
1 – Rare	1-2 times or once in 75-100% of the target time period	Environmental pollution is caused once every ten years.
2 – Few	1-3 times or once in 50-70% of the target time period	Dyeing technology is changed once in five years.
3 – Even	3-5 times or once in 25-50% of the target time period	Mergers and acquisitions are observed with outsourced contractors three times in five years.
4 – Often	5-10 times or once in 5-25% of the target time period	Imitation of company products is observed nine times in five years.
5 – Very often	More than 10 times or once in 0-5% of the target time period	Contract liabilities are violated 12 times in three years.

IEC 31010, clause 6.3.5.2 analysing likelihood

EXAMPLE 1: The statement that the chance of a supplier failing to deliver is 5 % is vague in terms of both time period and population. It is also unclear whether the percentage refers to 5 % of projects or 5 % of suppliers. A more explicit statement would be "the probability of one or more suppliers failing to deliver the required goods or services to a project within the life of a project is 5 % of projects".

To minimize misinterpretations when expressing likelihood, either qualitatively or quantitatively, the time period and population concerned should be explicit and consistent with the scope of the particular assessment.

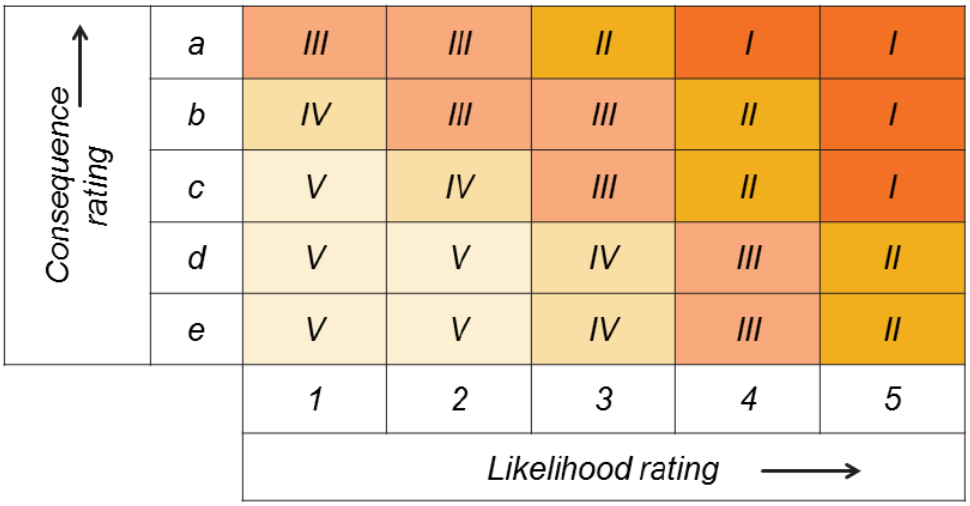
EXAMPLE 2: The probability of one or more suppliers failing to deliver the required goods or services to a project within the next two months is 1 % of projects whereas within a six-month time scale failure can occur in 3 % of projects.

21.2.16. Determining the Level of Risk

Risk Levels	Quantitative Levels	Qualitative Levels
Low	Less than €1m or < 0.15% of the net sales	All below medium
Medium	€1-5m or 0.5-0.75% of the net sales	Limited occurrences with low impact
Medium-high	€5-10m or 0.75-1.5% of the net sales	All between high and medium
High	More than €10m or < 1.5% of the net sales	Frequent occurrences with high or very high impact

The table above was adopted from “Implementing Enterprise Risk Management.” It uses quantitative and qualitative terms to describe the determined levels of risk, starting with the lowest level up to the highest. Each risk level is accompanied with a precise description (determined) of their respective risk.

21.2.17. Consequence/Likelihood Matrix



A consequence/likelihood matrix is used to evaluate and communicate the relative magnitude of risks on the basis of a consequence/likelihood pair that is typically associated with a focal event.

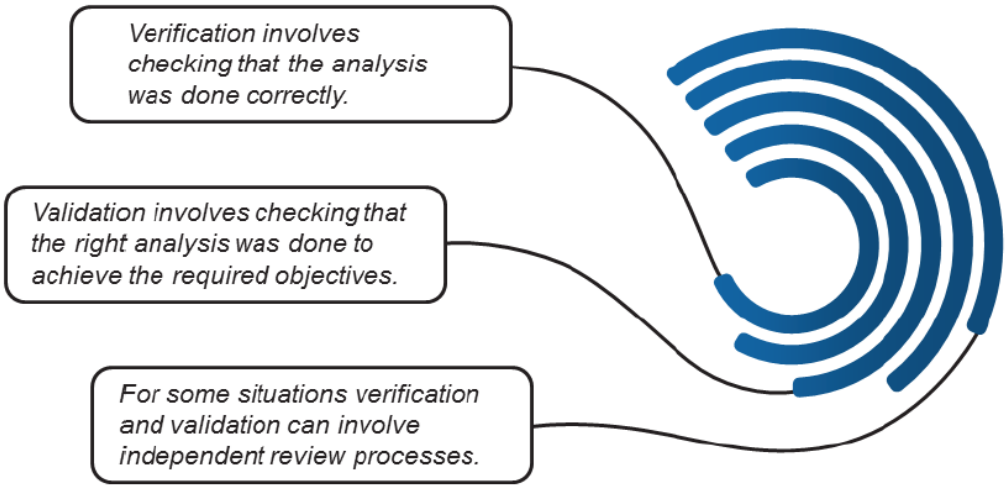
To rate a risk, the user first finds the consequence descriptor that best fits the situation then defines the likelihood with which it is believed that consequence will occur. A point is placed in the box which combines these values, and the level of risk and associated decision rule are read off from the matrix. Risks with potentially high consequences are often of greatest concern to decision makers even when the likelihood is very low, but a frequent but low impact risk can have large cumulative or long-term consequences. It can be necessary to analyse both kinds of risks as the relevant risk treatments can be quite different.

Where a range of different consequence values are possible from one event, the likelihood of any particular consequence will differ from the likelihood of the event that produces that consequence. Generally, the likelihood of the specified consequence is used. The way that likelihood is interpreted and used should be consistent across all risks being compared.

The matrix can be used to compare risks with different types of potential consequence and has applications at any level in an organization. It is commonly used as a screening tool when many risks have been identified, for example to define which risks need to be referred to on a higher level of management. It can also be used to help determine if a given risk is broadly acceptable, or not acceptable according to the zone where it is located on the matrix. It can be used in situations where there is insufficient data for detailed analysis or the situation does not warrant the time and effort for a more detailed or quantitative analysis.

21.2.18. Reviewing the Risk Analysis

Where practicable, results of analysis should be verified and validated.



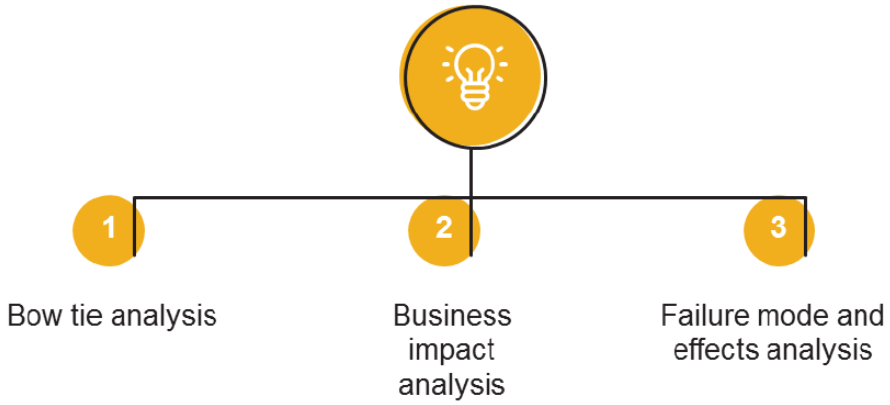
Validation can include:

- Checking that the scope of the analysis is appropriate for the stated goals
- Reviewing all critical assumptions to ensure they are credible in the light of available information
- Checking that appropriate methods, models and data were used
- Using multiple methods, approximations and sensitivity analysis to test and validate conclusions

Verification can include:

- Checking the validity of mathematical manipulations and calculations
- Checking that the results are insensitive to the way data or results are displayed or presented
- Comparing results with past experience where data exists or by comparison with outcomes after they occur
- Establishing whether the results are sensitive to the way data or results are displayed or presented and to identify input parameters that have a significant effect on the results of the assessment
- Comparing results with past or subsequent experience including explicitly obtaining feedback as time progresses.

21.2.19. Risk Analysis Techniques

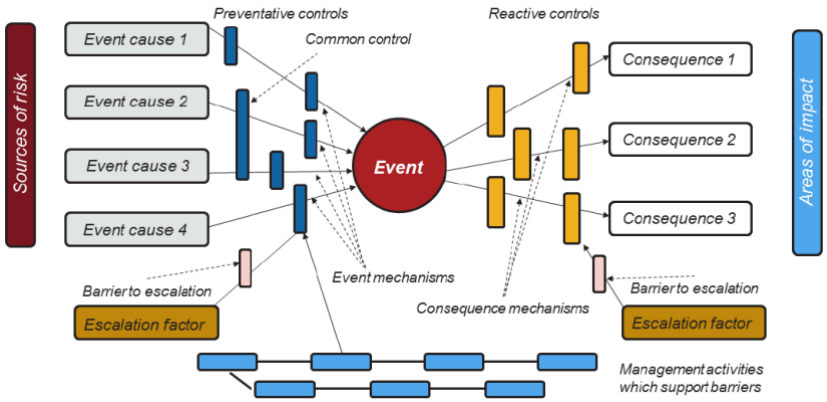


Bow Tie Analysis

A bow tie is a graphical depiction of pathways from the causes of an event to its consequences. It shows the controls that modify the likelihood of the event and those that modify the consequences if the event occurs. It can be considered as a simplified representation of a fault tree or success tree (analysing the cause of an event) and an event tree (analysing the consequences). Bow tie diagrams can be constructed starting from fault and event trees but are more often drawn directly by a team in a workshop scenario.

A bow tie is used when assessing controls to check that each pathway from cause to event and event to consequence has effective controls, and that factors that could cause controls to fail (including management systems failures) are recognized. It can be used as the basis of a means to record information about a risk that does not fit the simple linear representation of a risk register. It can be used proactively to consider potential events and also retrospectively to model events that have already occurred.

The bow tie is used when the situation does not warrant the complexity of a full fault tree analysis and event tree analysis but is more complex than can be represented by a single cause- event-consequence pathway. For some situations cascading bow ties can be developed where the consequences of one event become the cause of the next.



Bow Tie Analysis – Strengths & Weakness

Strengths of bow tie analysis include the following.	Limitations include the following.
• It is simple to understand and gives a clear pictorial representation of an event and its causes and consequences. • It focuses attention on controls which are supposed to be in place and their effectiveness. • It can be used for desirable consequences as well as undesirable ones. • It does not need a high level of expertise to use.	• A bow tie cannot depict a situation where pathways from causes to the event are not independent (i.e. where there would be AND gates in a fault tree). • It can over-simplify complex situations particularly where quantification is attempted.

Business Impact Analysis

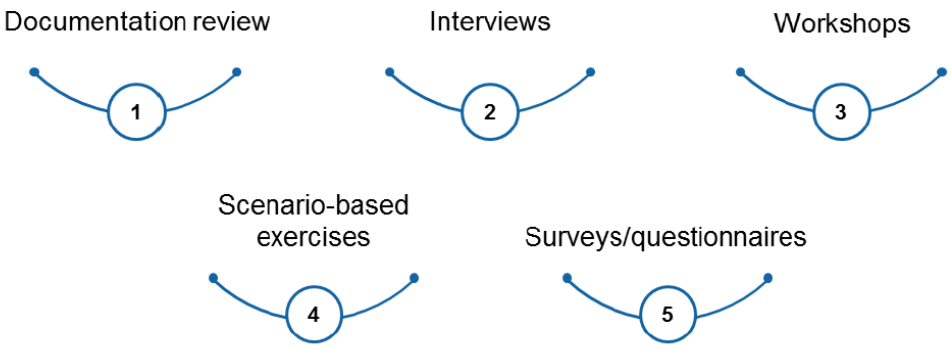
Specifically, a BIA provides an agreed understanding of:

- The criticality of key business processes, functions and associated resources and the key interdependencies that exist for an organization
- How disruptive events will affect the capacity and capability of achieving critical business objectives
- The capacity and capability needed to manage the impact of a disruption and recover to agreed levels of operation.

BIA can be undertaken using questionnaires, interviews, structured workshops or a combination of all three. It can also be used as part of consequence analysis when considering consequences of disruptive events. The BIA provides information that helps the organization determine and select appropriate business continuity strategies to enable effective response and recovery from a disruptive incident.

The methods to ensure information consistency, regardless of information collection method, are the following:

- Provide training for those who are leading or participating
- Identify information requirements
- Provide oversight or quality assurance of outputs
- Perform a trial of information collection method before implementing on a whole scale.



Strength and Limitations of BIA

Strengths of the BIA include that it provides:	Limitations include the following.
• a deep understanding of the critical processes that enable an organization to achieve its objectives and which can indicate areas for business improvement; • information needed to plan an organization's response to a disruptive event; • an understanding of the key resources required in the event of a disruption; • an opportunity to redefine the operational process of an organization to assist in improving the resilience of the organization.	• BIA relies on the knowledge and perceptions of the participants involved in completing questionnaires, or in undertaking interviews or workshops. This can lead to simplistic or over-optimistic expectations of recovery requirements. • Group dynamics can adversely affect the complete analysis of a critical process. • There can be simplistic or over-optimistic expectations of recovery requirements. • It can be difficult to obtain an adequate level of understanding of the organization's operations and activities.

EMEA and FMECA

The difference between these two techniques is that FMEA provides qualitative information, whereas FMECA provides quantitative information. FMEA should be performed before FMECA because FMECA is an extension of FMEA. Therefore, if one applies FMEA, the criticality analysis can be included and as such obtain FMECA results.

Definition:

FMEA (Failure Mode and Effects Analysis)
This technique is used to determine the failures and errors that may exist in the manufacturing, design, or production of products or services.

FMECA (Failure Mode, Effects and Criticality Analysis)
This technique is used to determine the consequences of failure modes. It is more sophisticated than FMEA because it includes the criticality analysis too.

FMEA and FMECA – Background

FMEA was developed in 1949 for military usage and was known as the "Procedure for Performing a Failure Mode, Effects and Criticality Analysis." This technique was used by the military to study problems that brought issues to military systems.

FMEA was used to determine the effect of system and equipment failure. Specifically, failures were determined in accordance with the effect on a mission's success or the safety of personnel and equipment.

This technique was widely used by the automotive industry in the 1970s, and du to their success, its use expended to other industries, as well.

In FMEA, a team subdivides hardware, a system, a process or a procedure into elements. For each element the ways in which it might fail, and the failure causes and effects are considered. FMEA can be followed by a criticality analysis which defines the significance of each failure mode (FMECA).

For each element the following is recorded:

- Its function
- The failure that might occur (failure mode)
- The mechanisms that could produce these modes of failure
- The nature of the consequences if failure did occur
- Whether the failure is harmless or damaging
- How and when the failure can be detected
- The inherent provisions that exist to compensate for the failure.

For FMECA, the study team classifies each of the identified failure modes according to its criticality. Several different methods of criticality can be used. The most frequently used are a qualitative, semi-quantitative or quantitative consequence/likelihood matrix or a risk priority number (RPN). A quantitative measure of criticality can also be derived from actual failure rates and a quantitative measure of consequences where these are known.

NOTE The RPN is an index method that takes the product of ratings for consequence of failure, likelihood of failure and ability to detect the problem (detection). A failure is given a higher priority if it is difficult to detect.

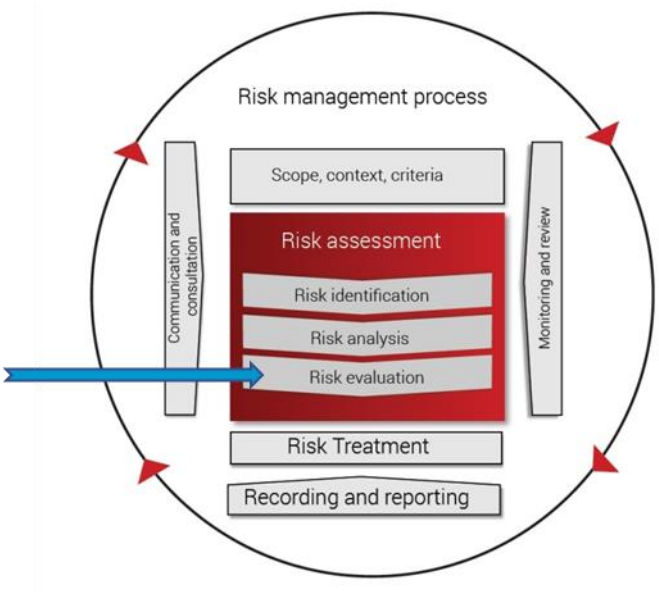
FMEA and FMECA				
Process name	**Process number**		**Date:**	
			Revision:	
Failure mode	**A. Severity** Rate 1-10 10 = Most severe	**B. Probability of occurrence** Rate 1-10 10 = Highest probability of occurrence	**C. Probability of detection** Rate 1-10 10 = Lowest probability of detection	**Risk priority number (RPN)** A x B x C
1. Wrong color seat belt selected	5	4	3	60
2. Seat belt bolt not fully tightened	9	2	8	144
3. Trim cover clip misaligned	2	3	4	24

FMEA/FMECA can be applied during the design, manufacture or operation of a physical system to improve design, select between design alternatives or plan a maintenance programmed. It can also be applied to processes and procedures, such as in medical procedures and manufacturing processes. It can be performed at any level of breakdown of a system from block diagrams to detailed components of a system or steps of a process.

FMEA can be used to provide information for analysis techniques such as fault tree analysis. It can provide a starting point for a root cause analysis.

22. Risk Evaluation

ISO 31000 emphasizes that the top management is ultimately responsible for the integration of the information generated during the risk analysis phase into their decision-making process; however, risk managers often play an important role in advocating such integration.



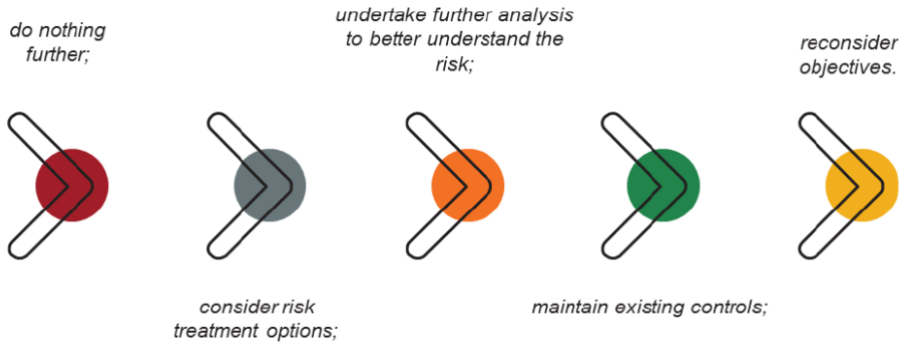
There are cases when the top management, intentionally, prefers incomplete information on certain issues. For example, driven by motivation to reach certain targets, they may prefer incomplete information that does not expose the real extent of the risks that the organization faces.

They can provide justifications, regardless of the result:

- If the result is favourable, such behaviour is attributed to the high quality of the management, expertise, business foresight, etc.
- If the result is unfavourable, the responsibility for the lack of success can be attributed to poor and incomplete risk analysis results.
- If faced with such situations, risk managers should point out to the top management that in order to make better decisions, they need to obtain all the applicable information.

22.1. Evaluating the Levels of Risk Based on Risk Evaluation Criteria

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:



22.2. Applying Results to Support Decisions

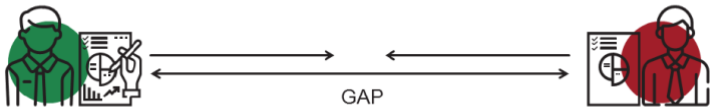
The outcomes from risk analysis provide an input to decisions that need to be made and actions that are taken. The factors to consider when making decision and any specific criteria should have been defined as part of establishing the context for the assessment.

Two type of decisions can be distinguished:

- Decision about the significance of risk and whether and how to treat risk
- Decision that involves comparing options where each has uncertainties (such as which of several opportunities to pursue)

22.3. Closing the Gap between the Risk Analysis Result and Decision-Making Function

In theory, the decision-makers in an organization should compare the results of the risk analysis with the established criteria in order to support the decisions. This is done as part of risk evaluation. In practice, however, in organization (especially in medium and large ones) where decisions are made at the top management level, the results of the risk analysis are often processed at lower hierarchical levels. This means that there exists a gap between the information generated at lower hierarchical levels and the one that decision-makers possess.



ISO 31000 emphasizes that the top management is ultimately responsible for the integration of the information generated during the risk analysis phase into their decision-making process; however, risk managers often play an important role in advocating such integration.

Some risks may be accepted for a finite time (for example, to allow time to actually implement treatments). The assessor should be clear about the mechanisms for temporarily accepting risks and the process to be used for subsequent reconsideration.

22.4. Evaluation the Expected Monetary Value

It is essential that organizations estimate the value of risk, also known as the expected monetary value (EMV). This is done by multiplying the probability of the risk by the cost of the recovery.

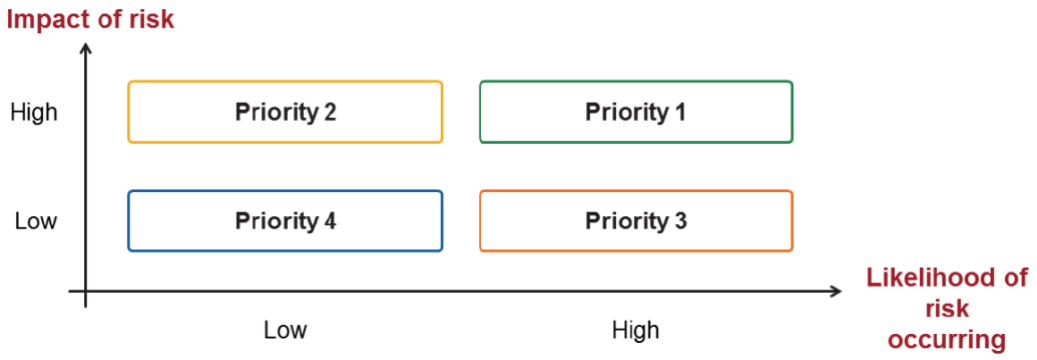
This type of decision is often made using expert judgement based on the understanding from an analysis of the options concerned and the risk associated with each, taking into account:

- trade-offs that may need to be made between competing objectives
- the organization's appetite for risk
- the different attitudes and beliefs of stakeholders

During this process, it is important to take the time necessary to gather enough information in order to accurately estimate the risk probability and the cost associated with its recovery. Organizations are free to use past data as a guide when accurate means of prediction are not available. At this point, asset valuation plays a role, as well, since the cost of risk is dependent on the asset.

22.5. Prioritizing Risk

The organization needs to prioritize risk in order to focus the treatment efforts into risk that have both higher impact and likelihood.



In order to prioritize risks, they should first be identified. In this way, risk is managed more effectively. Factors other than the magnitude of risk that can be taken into account in deciding priorities include:

- Other measures associated with the risk such as the maximum or expected consequences or the effectiveness of controls
- The qualitative characteristics of events or their possible consequences
- The views and perceptions of stakeholders
- The cost and practicability of further treatment compared with the improvement gained
- Interactions between risks including the effects of treatments on other risks.

Risk prioritization is the process of identifying risks that have a significant impact on the organization. Risk prioritization also supports the decision-making process by considering possible responses to various risks. Once the potential incident scenarios have been established, the criteria for the prioritization of risks should be defined.

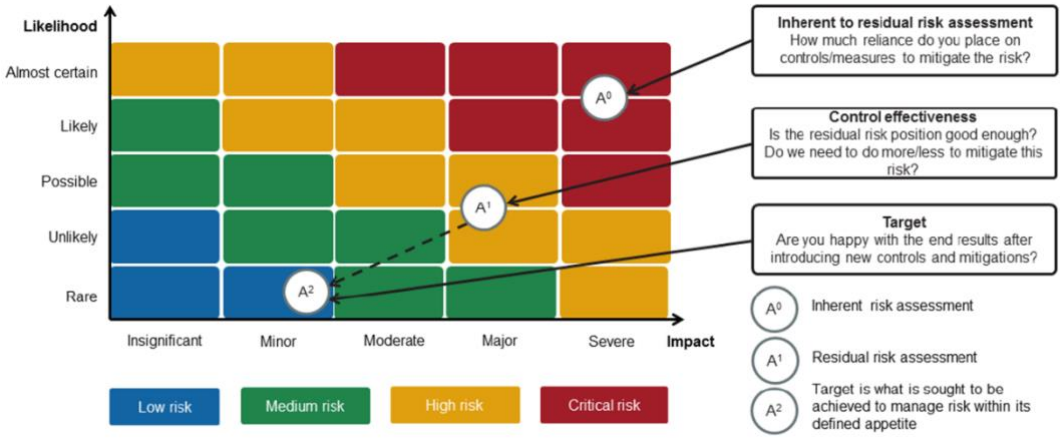
22.5.1. Risk Evaluation – Ratings

In order to conduct a risk evaluation, it is important that organizations identify three types of risk ratings, namely:

The inherent risk: The level of risk before any controls or measures are taken (the untreated risk)

The residual risk: The remaining level of risk after existing controls or measures are taken to mitigate the inherent risk

The target risk: The satisfactory level of risk after new mitigation measures have been introduced



The next step is to evaluate whether the residual risk rating is acceptable or unacceptable. This is based on an assessment of the target risk. For a risk to be considered acceptable, the residual risk needs to be equal to or less than the target risk, where except maintaining existing controls or measures, no further action is required from the organization.

However, this does not mean that the target risk must always be low for the risk to be accepted. When evaluating the target risk, the organization should consider:

- Its overall risk appetite
- Its degree of control over the risk
- The cost, benefits, and opportunities presented by the risk

When the residual risk is considered to be unacceptable, the organization should implement a risk improvement plan to bring the target risk Zto a level that is considered acceptable.

23. References

The United Nations Office for Disaster Risk Reduction. "The Economic and Human Impact of Disasters in the last 10 years." [online] Available at: http://www.ybusdr.org/we/inform/disaster-statistics [Accessed on November 6, 2019]

World Economic Forum. The Global Risk Report, [online] Available at: https://www.weforum.org/reports/the-global-risks-report-2020 [Accessed on 15 January 2020]

Some of the reasons for Risk Management Failure, [online] Available at: https://www.cbinsights.com/research/startup-failure-reasons-top/

International Organization for Standardization. “Risk management ISO 31000.” [online] Available at: iso.org, [Accessed 16 February, 2021]

Jean-Paul Louisot, Christopher H. Ketcham. [Book] ERM: Issues ad Cases. West Sussex, UK: John Whiley & Sons Ltd, 2014.

Risk Management Process According to ISO 31000, [online] Available at: https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines [Accessed 15 March, 2021]

Mardsen, Erik. “The ISO 31000 standard on risk management.” Risk Engineering: Sveiby, Karl-Erik. “Methods for Measuring Intangible Assets.” Sveiby. [online] Available at: https://www.sveiby.com/files/pdf/intangiblemethods.pdf [Accessed 13 March, 2021]

Borghesi, Antonio, and Barbara Gaudenzi. [Book] Risk Management — How to Assess, Transfer and Communicate Critical Risks. Italy: Springer — Verlag Italia, 2013.

Fraser, John R.S., Betty J. Simkins, and Kristina Narvaez. [Book] Implementing Enterprise Risk Management — Case Studies and Best Practices. New Jersey: John Wiley & Sons, Inc., 2015.

New Zealand Government. “ICT Risk Management Guidance.” [online] Available at: https://www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html [Accessed 13 March, 2021]

Chapter 2

Business Continuity Management

ISO 22301/ISO 22313

By Violeta Haxhillazi

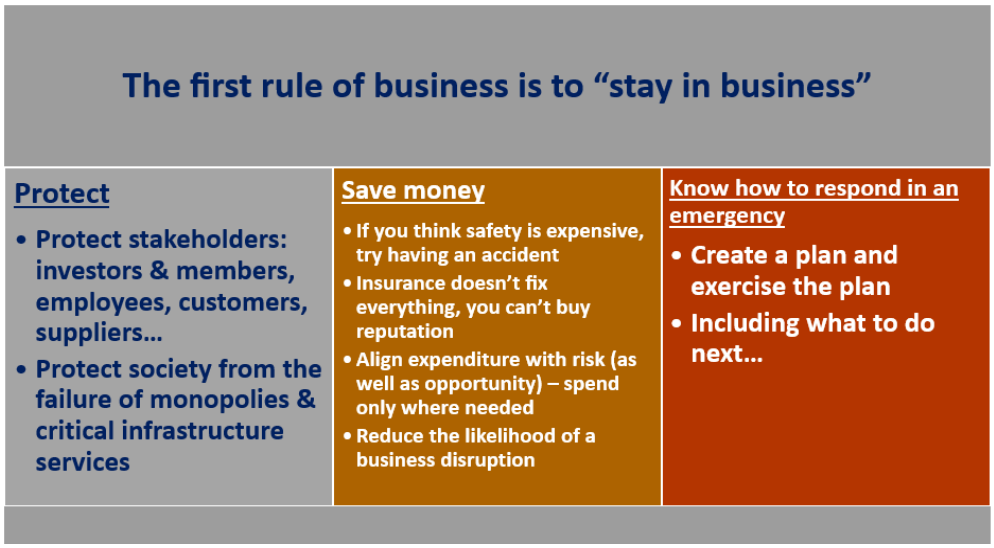
1. Introduction and Definitions of Business Continuity Management

In the current environment, in which businesses of all sizes and types are being tested in unprecedented ways by the coronavirus (COVID-19) pandemic, business continuity and resilience has become a critical discussion in boardrooms and C-suites across the world. The pandemic's widespread impact has forced organizations to revisit business continuity planning (BCP) and how to embed BCP practices in day-to-day operations. As we consider the changing landscape brought on by the pandemic, it's important to remember that other business risks continue to threaten business continuity. Natural and man-made disasters, as well as technology risks, abound.

- How can organisations stay prepared for these events?
- How can they develop a business continuity management (BCM) programme that responds to all crisis types and scenarios?
- Who is the right person in the organisation to own and manage the BCM programme? And,
- What are the critical elements of a business continuity policy? (Protiviti, 2020)

2. Why Discuss Business Continuity?

Business Continuity: is the enterprise-wide proactive business process by which we manage the risks we operate within. It addresses all aspects of the business: People, Processes, Resources and Technology (PPRT. The goal is: preventing or mitigating the risks we can and preparing for recovery from those we cannot, or choose not to prevent.



Business continuity plans: are designed to help organizations protect themselves from the losses to infrastructure and resources caused by natural disasters, pandemics and terrorism.

Preparation is the key: You fight like you train (SIMILAR TERMS: Contingency, Planning, Business Resumption, Planning, Corporate Contingency Planning, Business Interruption Planning, Disaster Preparedness!

3. Business Continuity (BC) and Business Continuity Management (BCM)

One of the more confusing aspects of BCM is its terminology. The confusion is mostly due to differences in how regulators and industry groups use and define terms in the BCM lexicon. Below are a few explanations about BCM:

Business Continuity (BC) is defined by ISO 22301 and ISO 22313 as 'the **capability of the organisation** to continue delivery of products or services at acceptable predefined levels following a disruptive incident'. (Dr David J. Smith, 2019)

Business Continuity Management (BCM) is defined in ISO 22301 as 'an **holistic management process** that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which **provides a framework for building organizational resilience with the capability for an effective (business continuity) response** that safeguards the interests of its key stakeholders, reputation, brand and value creating activities'. Whilst the term stakeholder is used within the definition the phrase 'interested parties' is used throughout the ISO standards and BCMS albeit it means the same thing. The relevance of the needs and requirements of interested parties is emphasised within both ISO standards as being a part of the key building blocks of BCM and BCM System. (Dr David J. Smith, 2019)

A BCM programme

- is defined in ISO 22301 as 'an ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management'

BCM strategy

- is defined as an 'approach by an organisation that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption'

Prioritised Activities

- are defined to which priority must be given following an incident in order to mitigate impacts- terms in common use to describe activities within this group include; critical, essential, vital, urgent and key'

Process

- is defines as a 'set of interrelated or interactive activities which transforms inputs into outputs'.

Risk Appetite

- is defined as the 'amount and type of risk that an organisation is willing to pursue or retain'.

Top Management

- is defined as 'person or group of people who directs and controls an organisation at the highest level'

In contrast to the statement within ISO 22313 that all definitions to be applied within ISO 22313 are to be found within ISO 22301 the following definition of **BCM** is described within ISO 22313 is '**Business Continuity Management (BCM)** is **the process of achieving business continuity** and is about preparing an organisation to deal with disruptive incidents that might otherwise prevent it from achieving its objectives... **placing BCM within the framework and disciplines of a management system creates a Business Continuity Management System (BCMS)** that enables BCM to be controlled, evaluated and continually improved'.

Consequently, a clear understanding of the terms; BC, BCM, BCMS, and BCM programme and other key definitions is not only essential to understanding but critical to providing resilience within an organisation subject to its risk appetite. (Dr David J. Smith, 2019)

4. BCM Role in Threat/Disaster Planning and Response

BCM is the design, development, implementation and maintenance of strategies, teams, plans and actions that provide protection over, or alternative modes of operation for, those activities or business processes which, if they were to be interrupted, might bring about seriously damaging or potentially significant loss to an enterprise. As BCM has evolved, the threat landscape has grown considerably to include both internal and external events, as well as extreme-but-plausible incidents. (Jonna Järveläinen, 2020)

During a threat/ disaster response, BCM should ensure the crisis management function remains engaged, particularly as it relates to following a defined protocol and crisis communications. Following a defined protocol that also can be flexible to the fluidity of any disruptive situation is key to a successful response. Since a pandemic can cause the workforce to be dispersed, which can lead to feelings of isolation and disconnectedness among employees, teams and even third parties, crisis communications can and should include strategies for both internal and external audiences. (Jonna Järveläinen, 2020)

The business continuity programme provides critical information that can be utilized as key inputs to the pandemic response plan. Similar to other plans (e.g., business resumption and IT disaster recovery plans), the contents of a pandemic response plan should be informed by foundational activities such as the business impact analysis (BIA) and continuity risk assessment. Outputs of these efforts should include elements such as the criticality of business processes, expected impact to the business caused by a disruption and maximum tolerable downtime. This information can be used to shape or inform a company's response.

Another important data element that can be useful to threat/disaster response is identification of critical third parties essential for each business process to function. These critical third parties can be identified during the BIA, along with the resulting impact if they are disrupted or unable to provide products and services. This information will serve as a guide to develop subsequent strategies and planning discussions. (Jonna Järveläinen, 2020)

BCM consists of three core disciplines:

Crisis management and communications

- This discipline enables an effective and cohesive response to an event. Crisis management processes focus on stabilising the situation and supporting the business if alternate modes of operation are needed, using effective planning, leadership and communication protocols.
- The communications protocols are important to be planned and exercised internally and externally.

Business resumption planning or business recovery planning

- This discipline focuses on disrupted aspects of business functions and processes that relate to or support the delivery of core products or services to a customer. Business resumption processes focus on the evaluation of people, processes, technology and other resources vital to the organisation's operations. The objective of business resumption planning is to mitigate potential impacts from disruptions, regardless of the cause, by developing plans that guide personnel through operations with diminished capabilities and towards business as usual.

IT disaster recovery (ITDR)

- This discipline addresses restoration of critical IT assets, including systems, applications, databases, and storage and network assets. An ITDR strategy also should encompass all technology service provider relationships (e.g., cloud providers) to ensure that all technical stakeholders remain aligned.

In addition to the traditional BCM disciplines listed above, many organizations manage other closely related programmes as part of their overall BCM programme. These programmes include:

Incident management (or incident response)

- This term commonly refers to identifying, analysing and managing the response to a disruptive event. Regardless of nomenclature, incident management programmes typically include emergency response measures such as evacuation of facilities, first-aid response and first-responder interactions.

Cybersecurity incident response

- This is specific to the planning for, response to and recovery from a cybersecurity incident such as a data breach, a phishing attempt or a distributed denial of service (DDoS) attack.

5. Added Value of Business Continuity and Risk Management

The value of BCM lies in risk mitigation in minimizing the risks associated with any disruption to business as usual. In the wake of recent catastrophic natural disasters and the COVID-19 pandemic, business leaders are more mindful than ever of the need to plan for and respond to business disruptions.

The business environment is fraught with risks that can impact businesses' ability to not only continue operations, but also protect their people and brand, earn revenue, maintain relevance and remain compliant with regulations. Companies need to stay ahead of these risks by understanding priorities, planning for disruptions, employing good business practices, and exercising forethought to increase their ability to course-correct quickly when things go wrong.

Organisations realize value when they proactively design and deploy business continuity solutions to manage a specific risk or multiple risks. For example, understanding and developing contingency plans for the loss of a key supplier can help a business mitigate potential financial, operational and reputational impacts. (Protiviti, 2020)

5.1. Financial risk

This is the most evident and quantitative area of risk. Companies can minimize financial loss and maintain market share by focusing on several factors, including:

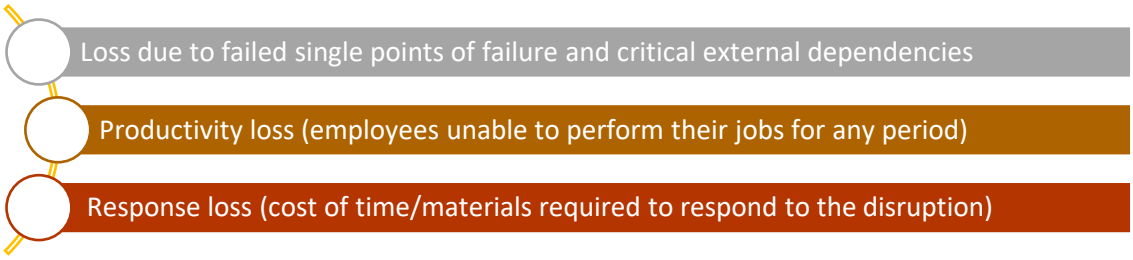
- Responding to customer demands and maintaining a viable supply chain
- Understanding officer liability
- Inventorying potential replacement loss (i.e., the cost of replacing damaged assets)

To protect the supply chain and ensure that supply keeps up with customer demand, a company may hold its suppliers accountable for disruptions to the supply chain that impact its operations. For example, a company can use contract provisions to hold a supplier accountable for timeliness in delivery of products or services, as well as for quality of products or services delivered.

A company can implement BCM solutions to minimize the potential for huge unexpected costs stemming from single points of failure and critical external dependencies. For example, if a company depends on a single critical supplier that suddenly is unable to provide core products or services, a well-designed BCM solution would provide contingencies to mitigate the financial loss. (Protiviti, 2020)

5.2. Operational Risk

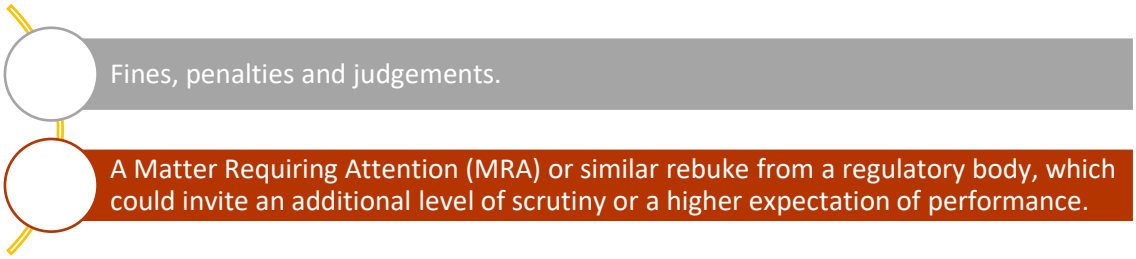
This area of risk stems from the inability of companies to produce core products and services as expected. This can include risks associated with equipment or technology obsolescence, a failure in internal functions, and unexpected changes to a leadership team. Other operational risks directly impacting business as usual include:



A company should implement BCM solutions to minimize operational gaps and ensure that the delivery of products and services continues, even during unusual circumstances. Comprehensive implementation of a BCM programme will lower risks associated with readiness, planning and response, which can decrease overall operational risk. (Protiviti, 2020)

5.3. Regulatory Risk

Regulatory bodies are increasingly holding companies accountable for maintaining validated capabilities, teams and plans, and can issue fines to those that operate without a BCM programme. Depending on the regulator, a repeated and unmitigated issue at a regulated entity could result in a reportable item, which could impact the company's credit worthiness or reputation. Generally, companies that violate regulations or compliance requirements face:



5.4. Reputational Risk

Bad press can cause a decline in revenue, unwanted social media attention, lower market capitalisation and, in the long term, a negative opinion of an organisation in the eyes of the

discerning public. In today's 24-hour news cycle, a measured, empathetic, rapid and relevant response to any event is crucial to maintain a positive reputation. A mature BCM programme drives value by protecting a company's brand and adeptly managing the ever-changing business landscape in the face of growing competition. (Protiviti, 2020)

5.5. Health and Safety Risks

Last but not least, a solid and comprehensive BCM aims the reduction of the incidence of the injuries and of the cases of the work ill related ill- health. A numerous studies has confirmed that a more evidenced based risks management and targeting of control is beneficial as it most the organization away from the one-size-fits-all mindset and approaches about health and safety. It enhances the ability to measure the health and safety performance and demonstrate improvement and benefits of interventions. The establishment of BCM function is providing a better awareness of what good risk control looks like, what's feasible from a health and safety performance perspective, which helps in the prediction and therefore the opportunity to prevent them.

5.6. Conclusion

- BCM is not just a response
  also building **resilience to strengthen an organization**
- BCM is not just about fighting fires
  also developing understanding what **might be at risk and developing strategies if things do go wrong**
- BCM is not just about having plans to recover a business that are over elaborate
  also about **having plans that suit the nature of your business**
- BCM is not an add-on to business
  To be effective, it must be an **embedded management process**, as part of risk management and part of good business management

IT'S A PROACTIVE PROCESS THAT CONCENTRATES ON CRITICAL RESOURCES REQUIRED TO CONTINUE KEY BUSINESS PROCESS DISREGARDS THE EVENT

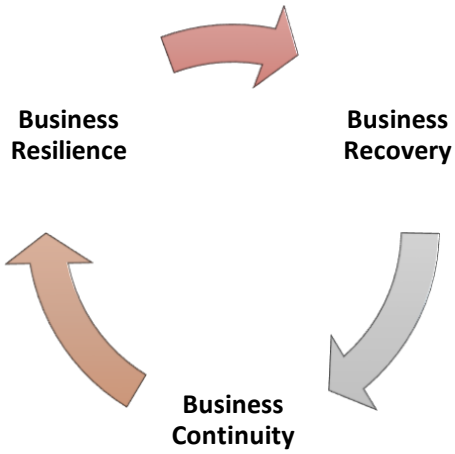
6. BCM and Business Planning

The term 'Business Continuity Management' is used rather than 'business continuity planning'. This approach is deliberate because 'planning' implies there is a start and end to the process and can lead to unwanted planning bureaucracy. However, business continuity planning is still a critical and key component of the BCM process. (Dr David J. Smith, 2019)

In contrast to the earlier narrow and reactive approaches to BCM it is now recognized as a dynamic, proactive, and ongoing business as usual management process. To be effective it

must be aligned with or complete against a standard, appropriate (fit for purpose), practical, realistic, up-to-date, effective and a plausible (proven) capability. (Dr David J. Smith, 2019)

Three definitions important to be highlighted:

<table>
<tr>
<td>Business continuity planning (BCP) – This term is used to denote the planning aspects of business continuity management (BCM). BCM usually refers to the comprehensive programme, while BCP is the predefined set of steps taken to recover a business process in the event of a disruption. This term is often used interchangeably with “business resumption,” “contingency planning” or “business recovery planning.”</td>
<td> 
</td>
</tr>
<tr>
<td>Business recovery planning – The term refers to various steps taken for an individual process or business line as it relates to the planning of inputs/outputs, personnel resources, information technology and physical work locations in the aftermath of a disruption. This term is often used interchangeably with “business resumption,” “contingency planning” or “business continuity planning.”</td>
<td>Business resumption planning – This process focuses on recovery of business functions.

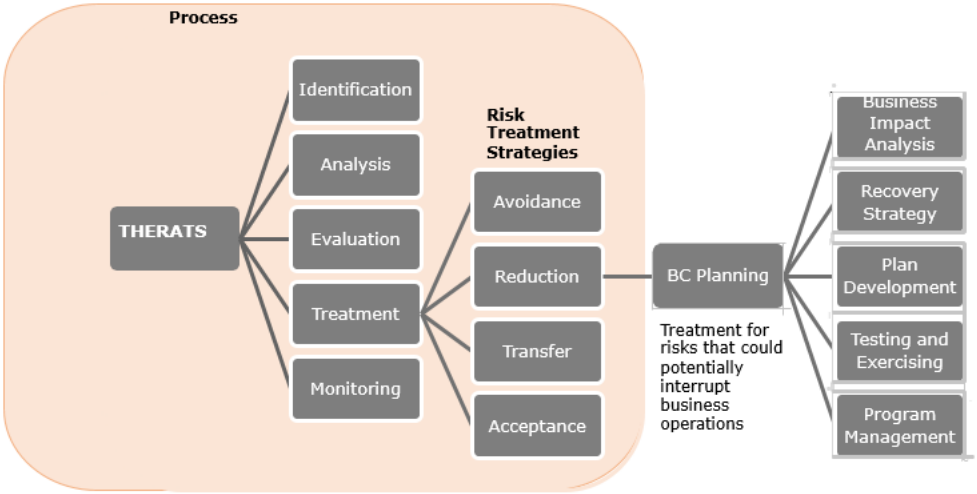
The term is often used interchangeably with “business recovery,” “contingency planning” or “business continuity planning.”</td>
</tr>
</table>

Due to the nature of business continuity, it is common for several functions to be integrated at various phases of business continuity planning. For example, facilities or physical security teams may engage in emergency management activities, and safety and environmental health teams may have input in developing recovery strategies. (Dr David J. Smith, 2019)

Knowing who is responsible for the creation and modification of a business continuity plan checklist is one component. The other is identifying the team responsible for implementation. Governance provides clarity in what can be a chaotic time for all involved. (Dr David J. Smith, 2019)

The scope is also crucial. It defines what business continuity means for the organization.

Is it about keeping applications operational, products and services available, data accessible, or physical locations and people safe? Businesses need to be clear about what is covered by a plan whether it’s revenue-generating components of the company, external facing aspects, or some other subset of the total organization. Roles and responsibilities need to be assigned during this phase as well. These may be roles that are obvious based on job function, or specific, given the type of disruption that may be experienced. In all cases, the policy, governance, scope, and roles need to be broadly communicated and supported. (Dr David J. Smith, 2019)



6.1. Business Continuity Planning and Risk Assessment

Risk comes in many forms. A Business Impact Analysis and a Threat & Risk Assessment should be performed. Threats can include bad actors, internal players, competitors, market conditions, political matters (both domestic and international), and natural occurrences. A key component of the plan is to create a risk assessment that identifies potential threats to the enterprise.

Risk assessment identifies the broad array of risks that could impact the enterprise.

Step 1: Identifying Potential Threats is the First Step and Can Be Far-Reaching.

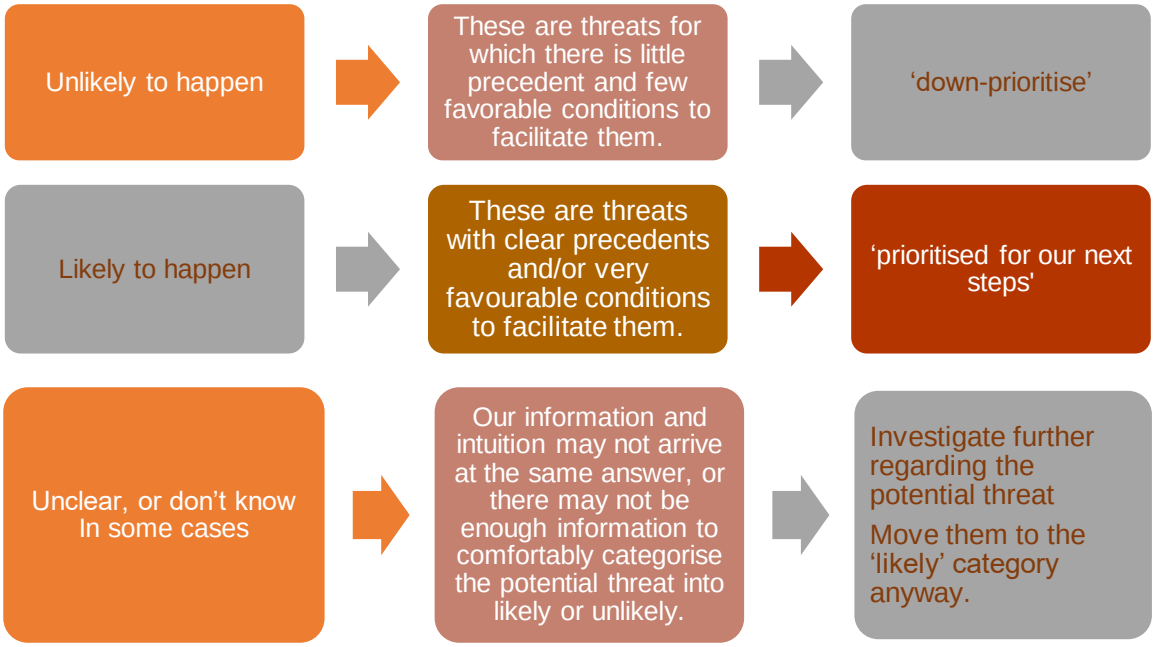
This includes:

- The impact of personnel loss
- Changes in consumer or customer preferences
- Internal agility and ability to respond to security incidents with a plan
- Financial volatility

Step 2: Likelihood and Probability of the Threat

Each risk needs to be articulated and detailed. In the next phase, the organization needs to determine the probability of each risk happening and the potential impact of each one. Likelihood and potential are key measures when it comes to risk assessment.

Once the risks have been identified and ranked, the organization needs to determine what its risk tolerance is for each potentiality. What are the most urgent, critical issues that need to be addressed? At this phase, potential solutions need to be identified, evaluated, and priced. With this new information, which includes probability and cost, the organization needs to prioritize which risks will be addressed.



The ranked risks then need to be evaluated as to which risks will be addressed first. Note that this process is not static. It needs to be regularly discussed to account for new threats that emerge as technologies, geopolitics, and competition evolves. (Refer to Annex 1: Business Continuity Management (Bow-Tie Analysis)

Step 3: Validation and Testing

The risks and their impacts need to be continuously monitored, measured and tested. Once mitigation plans are in place, those also should be assessed to ensure they are working correctly and cohesively.

- Incident Identification: With business continuity, **defining what constitutes an incident is essential**. Events should be clearly described in policy documents, as should who or what can trigger that an incident has occurred. These triggering actions should prompt the deployment of the business continuity plan as it is defined and bring the team into action.
- After an incident, one fundamental task is to debrief and assess the response, and revising plans accordingly.

6.2. Business Impact Assessment (BIA)

A BIA is carried out within the activities of a Business Continuity Management System (BCMS). Its formal definition is: “Process of analyzing the impact over time of a disruption on the organization” (ISO 22301: 2019, 3 Terms and definitions, 3.5).

In a BIA, the organization’s business processes are analyzed to know what impact is produced in the event of an incident that causes the interruption of these processes. The objective is to identify which are the most critical processes for the company.

Business continuity focuses on those processes in which availability is vital, i.e., in the event of being interrupted, the impact caused to the organization may not be acceptable in a short period of time. (ISO 22301: 2019, 3 Terms and definitions, 3.5).

It is necessary to consider different types of impacts that may occur as a consequence of the interruption of a process, some of them may be the following:

- **Operational impact**, that prevents obtaining the product or result of the service to which the process belongs.
- **Economic impact** due to additional costs, loss of income, penalties, etc.
- **Reputation impact,** due to loss of brand image by not being able to provide the service normally to customers.
- **Legal and contractual impact**, by interrupting a specific process, the organization may be failing to comply with any legal or contractual requirement that may have serious consequences.

The impact assessment is a cataloging process to identify the data your company holds, where it’s stored, how it’s collected, and how it’s accessed It determines which of those data are most critical and what the amount of downtime is that’s acceptable should that data or apps be unavailable. While companies aim for 100 percent uptime, that rate is not always possible, even given redundant systems and storage capabilities. This phase is also the time when you need to calculate your recovery time objective, which is the maximum time it would take to restore applications to a functional state in the case of a sudden loss of service. Also, companies should know the recovery point objective, which is the age of data that would be acceptable for customers and your company to resume operations. It can also be thought of as the data loss acceptability factor. (Bojana Dobran, March 2019)

The BIA measures the *potential quantifiable and qualifiable impact* that *could occur* if any business function was unable to operate for a period of time *for any reason*. That measurement becomes the basis on which we prioritize our efforts in building an efficient Business Continuity Plan (BCP).

BIA is *Not* a Threat Analysis

BIA is *Not* a Facility Risk Analysis/Assessment

- Business unit managers aren't the best people to ask about the potential cost of facility loss.
- People who can estimate those costs, and that would probably involve real estate people, engineers, technology resources, records managers

A BIA is *Not* A Risk Analysis

- A Risk Analysis identifies operational risks, defines controls to mitigate those risks, and monitors residual risk that remains after the controls have been put into place.
- The BIA identifies the quantitative (measurable) and qualitative (usually reputational) impact that could occur if a Department or Business Function was unable to function for any reason.

The process of Business Impact Analysis goes in several steps. Each step and the respective analysis is formulated as below.

Step 1: Define Goals

Goal #1

Identify the impact that any individual Department or Business Function could have on the institution if it was unable to function *for any reason*

Goal #2:

Have a final deliverable that will satisfy Goal #1 in clear and understandable language.

Goal #3:

Make the process as easy as possible forthe Departments.

Step 2: Root Cause Analysis

Cause: "Something" that happened to produce a deviation of the actual from the expected or desired:

- Proved reason for existence of problem.
- Often "multiple causes"

Dominant or Root Cause: a major contributor to existence of problem which must be fixed before there is an adequate solution.

Remedy: a change that can successfully eliminate or neutralize the cause of a problem.

Step 3: Define "Critical Impact"

- The definition of critical impact needs to be based upon something measured, proven, and dynamic enough to change as your company changes.
- You won't know the appropriate definition of critical impact until you have implemented a BIA process that can keep up with changes in the company.
- What is considered non-critical today could become critical tomorrow.

Step 4: Define your Deliverables

Report #1

Compared to other Departments or Business Functions in the company, each Department/Function's criticality is this.

Report #2:

Based on when a Department/Function could cause Quantifiable Impact, its Recovery Time Objective (RTO) would be this.

Report #3:

Based on when a Departmental/Function could cause Qualifiable Reputational Impact, its RTO would be this.

Step 5: Identifying Dependencies

You could do your analysis Department, including all of the Business Functions within each Department, and then identify the Dependencies of each Business Function,

System/technology dependencies

Vendor dependencies

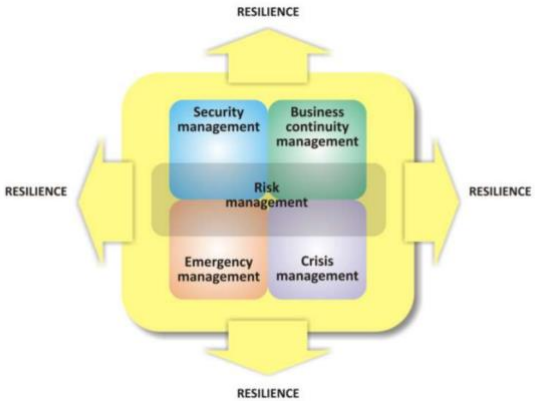
Supporting internal department dependencies

Other dependencies

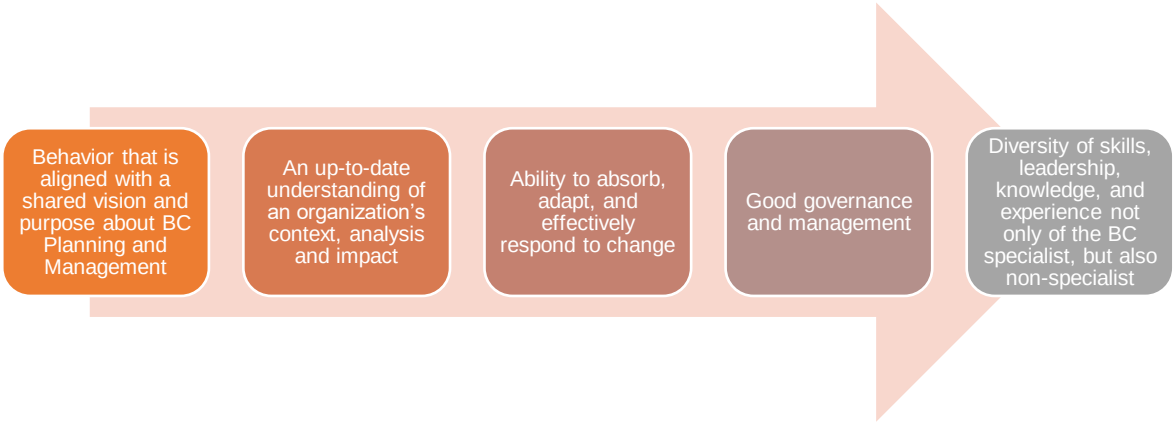
While Dependency identification could be an entirely separate process, incorporating it into your BIA can add significant value to the final deliverables.

7. BCM and Resilience

While Risk Management is process centric, Business Continuity Management is more strategic in nature, being a holistic approach that is influenced by a unique interaction and combination of strategic and operational factors.

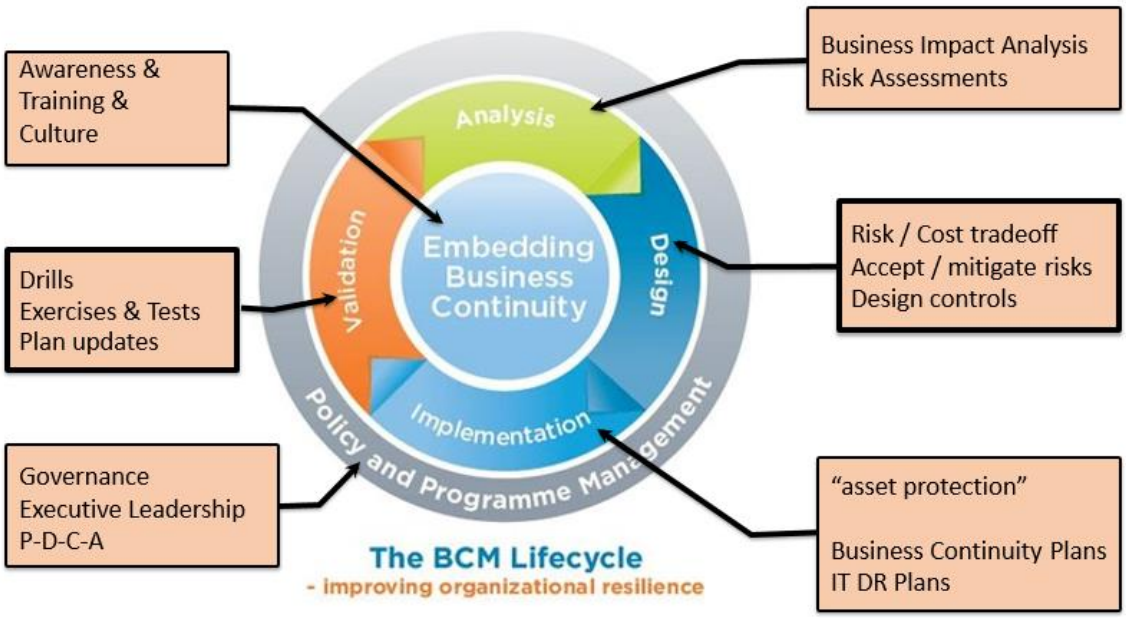


Therefore several aspects are critical in achieving that, which are presented in the diagram below:

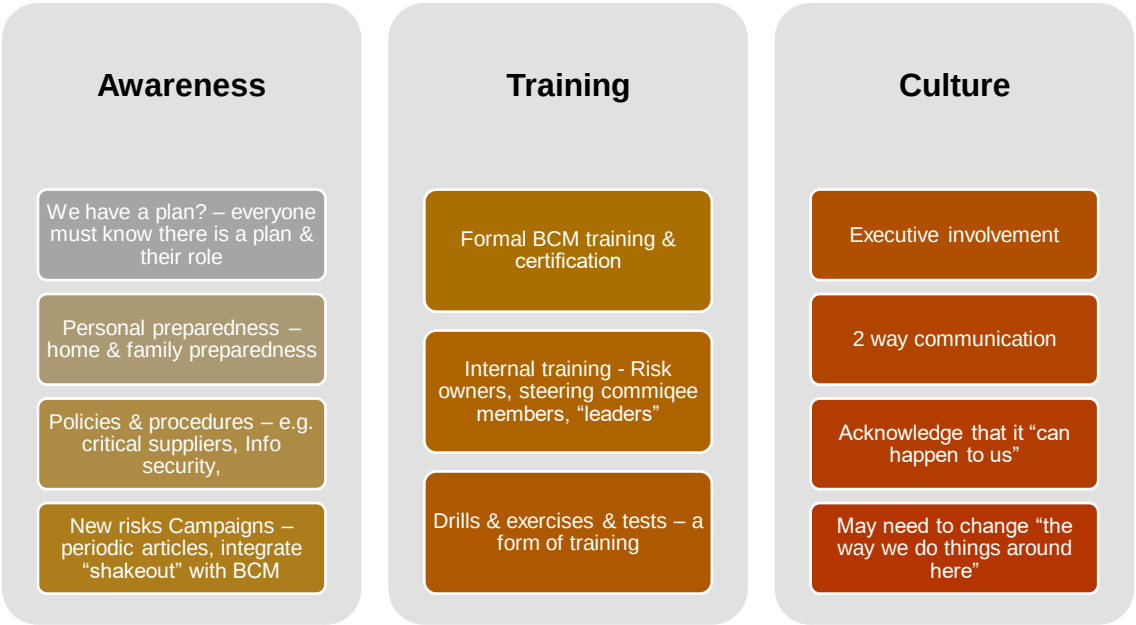


Educating, awareness-raising, training, whatever you like to call it, is a vital and ongoing part of any BCM programme. I believe that 'embedding' is now accurately reflected in the BCM Lifecycle diagram, showing that all we seek to deliver should have a wider impact on the culture of our organizations. By utilizing every opportunity within each component of the Lifecycle to spread the word, you should be able to provide deeper levels of understanding that broad and generic campaigns could never achieve. (Andy Mason, 2010)

While we will always have different depths of knowledge as to what business continuity means to each individual and business unit, and support for the BCM programme, 'embedding into the culture' is truly where the BCM programme meets with the people who make up your business, this is where the rubber hits the road! Awareness equals understanding, and understanding leads to a greater chance of success in what you are trying to achieve. (Andy Mason, 2010)



Tools for dealing with the enhancement of BCM concepts in the organization culture (Ihab Hanna S. Sawalha, John R. Anchor & Julia Meaton , Dec.2015)



BCM can be embedded in the organization's culture through:

- regular testing, training and awareness and
- the maintenance and updating of the continuity plan.

Embedding BCM- Continuity Testing

Testing helps to examine the comprehensiveness and applicability of the BC plan and its ability to cope with various disaster and crisis scenarios.

It ensures that the BC plan can be executed and that all the required resources are deployed as part of the overall BCM strategy.

Full plan testing in a real atmosphere (also known as exercising the plan) enables continuity teams to find possible weaknesses in their plans and to strengthen them.

Testing also builds confidence amongst people and reduces panic at the time of emergency

Most importantly, it is significant to note that testing should not be limited to internal employees. Engaging customers, business partners, and other agencies that support business operations is also significant.

Embedding BCM-Continuity Training and Awareness

Enhancing awareness levels and motivating change.

It helps to reduce resistance by providing participants with the opportunity to think critically, work in groups, and learn.

Organizations that are better at learning are more capable of coping with emerging threats.

They are also better in creating new knowledge and in adapting to changing environmental conditions more quickly and efficiently

Overall, training should be made in order to enhance preparedness for future incidents

Embedding BCM-Continuity Maintenance and Updating

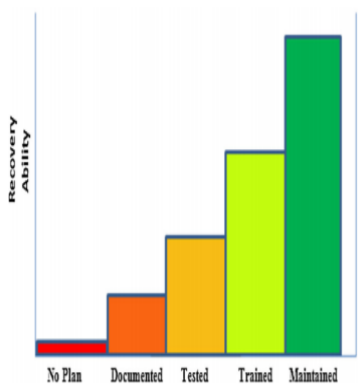
The purpose of maintenance is:

- To ensure that the BC plan is capable of responding to the changing nature of the business environment
- Fit for use and is quality assured that subsequently helps to ensure that the organization's BCM competence and capability remain effective.
- Regular maintenance protects the organization from having to develop continuity procedures again (helps to keep plans relevant) thereby ensuring the existence of workable business continuity plans at all times. (*Civil Contingencies Act Enhancement Programme, March 2012*)

Embedding BCM-Indicators

The testing, training and awareness and maintenance and updating activities are indicators of the maturity level of the business continuity plan and have been described as the ability of an organization to recover following major incidents. (Ihab Hanna S. Sawalha, John R. Anchor & Julia Meaton , Dec.2015)

This ability is classified into five levels in terms of the business continuity plan:

Level 1 = no plan Level 2 = documented BC plan Level 3 = tested BC plan Level 4 = trained BC plan Level 5 = maintained and updated BC plan	Fig. 1 Ability to recover versus BC plan maturity. *Source* adapted from Strohl Systems (2007) 

The higher the level is, the more the organization will be able to recover following major disruptions and return to normal. (Ihab Hanna S. Sawalha, John R. Anchor & Julia Meaton , Dec.2015)

8. References

Andy Mason, 2010, The Business Continuity Journal, Embedding BCM in the organization's culture

Bojana Dobran, March 2019, PHOENIXNAP, What is Business Continuity Management (BCM)? Framework & Key Strategies

Civil Contingencies Act Enhancement Programme, March 2012, Emergency Preparedness | Business Continuity Management

Dr David J. Smith, 2019, Organisation Resilience: Business Continuity, Incident and Corporate Crisis Management

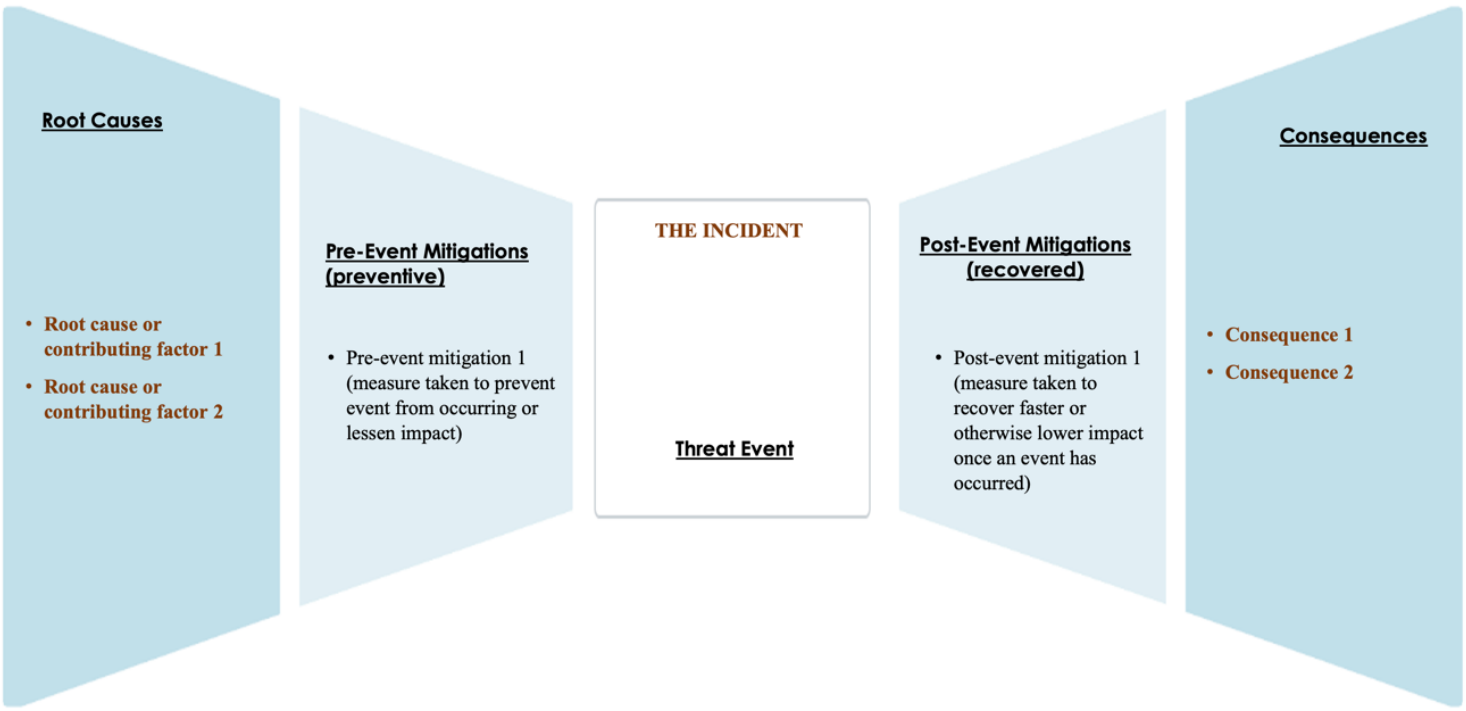
Ihab Hanna S. Sawalha,, John R. Anchor & Julia Meaton , Dec.2015, Continuity Culture: A Key Factor for Building Resilience and Sound Recovery Capabilities

ISO 22301: 2019, 3 Terms and definitions

Jonna Järveläinen, January 2020, Understanding the Stakeholder Roles in Business Continuity Management Practices – A Study in Public Sector

Protiviti, July 2020, A Guide to Business Continuity Management

Annex 1: Business Continuity Management (Bow-Tie Analysis)



Chapter 3

Information Security Management Systems (ISMS)

By Osman-Jablan Bulić

1. Information Security Management Systems (ISMS) – Why are These Important in Today's Industries?

Information Security Management System (ISMS) is, in its essence, a set of policies, procedures, organizational roles, governance mechanisms, and security controls, which are wholistically implemented to proactively address security risks and to provide the management with a tool that enables them to manage security aspects in a systematic manner.

In today's rapidly evolving environments the risk landscape is swiftly changing as well. Today's organizations are faced with kinds of risks that were not even considered just a while ago. As a consequence, the previously commonly used ad-hock approach to information security is no longer adequate and sufficient.

What organizations need is a system that is principally based on the risks management and preventive engagement (primarily through the implementation of security controls with the objective to put risks under control). This is what ISMS offers to the organizations: protection of critical business processes from the effects of information security incidents, disasters, and major failures of information systems.

Furthermore, ISMS (when implemented based on ISO/IEC 27001 standard requirements) does not only address IT security and protection of electronic information or IT systems. Information security, as ISO/IEC 27001 approaches it, deals with the protection of confidentiality, integrity and availability of information in any shape, form, or state and includes electronic-based information as well as non-electronic information.

2. Establishment of an Adaptable Information Security Policy and IT Security Policy

Information security policy is a top-level document which defines the management's approach to security, expressed through a set of rules, lower-level policies, and procedures defined to ensure protection of confidentiality, integrity, and availability of information assets. Information security policy gives an organization a set of governing rules that presents a foundation for the development of topic-specific policies and procedures which prescribe practical activities that aim to achieve security objectives.

As we said earlier, information security includes the protection of information in any shape, form, or state and includes electronic-based information as well as non-electronic information. As such, INFORMATION SECURITY POLICY is encompassing all aspects of a business and most, if not all, of its processes. On the other hand, IT SECURITY POLICY presents a subset policy that focuses on the definition of information security as related to the IT systems and information that is "flowing" through these systems. It also includes other critical information assets such are software and hardware that comprise these systems, services required to operate, as well as people that are using it, administering it, or in other ways influencing the IT systems.

It is critical for organizations to adopt information security policy based on their personal requirements, needs, and expectations, considering expectations of all other interested parties as well. This policy will set the tone for the organization's whole approach to the information security - including the scoping of the future ISMS.

In today's world of ever-changing threats and emerging vulnerabilities the information security policy must be constantly reviewed to assure its continuous suitability, adequacy, and effectiveness. Some of the elements what must be taken in consideration when defining the information security policy will include requirements and expectation of interested parties (explicit and implicit), scope of the ISMS, the perceived risks and implemented controls, as well as information security objectives. As the risks landscape changes or as the organization's own business change the top management of an organization must review and modify the policy and adjust the implemented ISMS to adequately respond to the changing needs.

3. ISMS Aspects with View to BCM

One of the many functions of an implemented ISMS is to ensure continuity of information security as a part of overall business continuity management. A number of security controls directly or indirectly address risks that are based on risk scenarios that result in a temporary or permanent loss of information availability.

Specific security controls identified in Annex A of the ISO/IEC 27001 standard address issues such are backup, redundancies, records protection, as well as planning, implementation, and testing of information security continuity. These controls add an additional layer of security and information protection to the existing or planned arrangement for business continuity management within an organization.

4. The Standards in the Field of ISMS

Information security management is defined through a number of ISO standards which we often address as ISO 27000 family of standards (with more than seventy standards, about fifty of which have been published so far). The standards in the series range from ISO 27000, which gives an overview and introduction to the series, all the way to the very comprehensive industry-specific or topic-specific standards such as ISO 27799 - ISMS implementation guidance for the health sector, or ISO 27043 – incident investigation (and eForensics).

Following are some of the most important or most used ISO 27k standards:

- ISO/IEC 27000:2018 - overview of the ISO 27k family of standards and dictionary of specific terms used throughout the series. (ISO/IEC refers to the issuing organization. In this case standards are issued by ISO (International Standardization Organization) and IEC (International Electrotechnical Commission); ":2018" indicates the last published version of the standard.)
- ISO/IEC 27001:2013: gives requirements for the implementation of Information Security Management System. This is the only certifiable standard in the series (provides common requirements for any organization which serves as basis for a certification audit)
- ISO/IEC 27002:2013: commonly known as Code of practice serves as reference for determining and implementing controls for information security risk treatment in an ISMS based on ISO 27001. (Please note that new version of ISO 27002 standard is currently in the final stages of review and approval, and new version of this standard is poised to be published by the end of 2021 or during 2022. New version of this standard will contain 93 controls divided into 4 categories and will take in consideration new technologies, threats and lessons learned.)
- ISO/IEC 27003:2017: provides guidance on how to implement ISO 27001
- ISO/IEC 27004:2016: covers information security management measurements.
- ISO/IEC 27005:2018: covers information security risk management process.

5. The Implementation of an ISMS

The implementation of an ISMS is a risks-based process that follows the PDCA cycle (Plan, Do, Check, Act). Fundamentally, one can follow the requirements of the ISO/IEC 27001 standard (sections 4. to 10.) and as a result expect to have a functioning Information Security Management System. In reality, of course, the implementation is substantially more complex, but all the required steps are identified within standard itself – making it somewhat of a "cookbook" for the implementation of ISMS.

Some of the critical activities in the implementation process are:

1. Defining the context of the organization for the future ISMS in terms of identifying its interested parties as well as their explicit and implicit expectations. Furthermore, at this stage it is very important to properly size up the future ISMS by defining the Scope of the ISMS, based on the analysis of the organization's processes and information flow and risk management. Scope of the ISMS is used to delineate the reaches of the direct control over information security (what's "in-house") vs. all those interconnected systems and information assets that are not under our direct control but need to be taken in consideration (as they may pose information security risks).

2. Identifying key roles and responsibilities related to the implementation of the ISMS, as well as obtaining leadership support from top management of the organization.
3. It is very important to note the need for the top management involvement in all phases of the implementation project as well as other non-IT parts of the business (business owners, finance, legal, HR etc.). Only by engaging all levels of the organization full benefits of the ISMS implementation can be expected.
4. After the initial setup of the framework for the future ISMS, one of the critical activities in ISMS implementation will be to define the Risk Management approach. Risk management is composed in two major components: a) risk assessment, and b) risk treatment.
   a. In the Risk assessment, the organization tries to understand all the risks that the processes, information, and information assets are exposed to, by identifying threats and vulnerabilities (risk scenarios) and assessing likelihood of the scenario happening and impact on the organization if the scenario materializes.
   b. In the Risk treatment, based on the results of the risks assessment process and recognized levels of risks options for the risk treatment are considered. These options are: a) risk avoidance, b) risk mitigation/reduction, c) risk sharing, and d) risk acceptance. The most common option for risk treatment is risk mitigation i.e. risk reduction which is achieved through the implementation of security controls presented in the Annex A of the ISO 27001 standard (further explained and elaborated in the ISO 27002 standard).
5. In order to create a fully operational management system, the ISO/IEC 27001 standard also requires organizations to implement various mechanisms which enable true systematic approach. Some of these mechanisms are:
   - processes of monitoring, measuring, analysis and evaluation of implemented system,
   - conducting regular, periodic internal audits,
   - dealing with nonconformities and undertaking corrective actions,
   - as well as conducting periodic management review of the whole management system with the idea to continuously improve the effectiveness and efficiency of implemented processes.

As we mentioned earlier, ISMS is based on the set of generic requirements presented in the international standard ISO/IEC 27001. These requirements are scripted in such a manner that allows for the implementation of the standard in any type of an organization, in any industry, with respect to any type of internal structure or processes within an organization. This is one of the main advantages of this standard – its adaptability to the various businesses and its needs. However, being written in such a generic manner it presents itself as a somewhat difficult reading for an untrained eye. Nevertheless, organizations that consider the implementation of ISMS should have a substantial guidance in the ISO 27001 standard. Additionally, other standards in the ISO27k series may provide further support in the implementation efforts.

Criteria for the Selection of Suppliers of IT Systems and their Maintenance

One of the crucial risks in today's business environment is the reliance on the outside suppliers to provide implementation and maintenance of the IT systems within companies. Moreover, in their justifiable effort to focus on their core business, more and more organizations are opting to outsource some parts (or even the whole IT infrastructure) to an outside managed service provider. Outsourcing strategy aims to share some of the information security risks with an outside party, with hopes that a specialized organization is more competent and adequate to address

risks inherent to the usage of modern, always connected IT systems. Nevertheless, this does not absolve the organization of the ownership for these risks.

In any case, the organization implementing the ISMS must recognize the risks related to the IT systems and identify appropriate controls for their reduction, which will then communicate to the service provider/supplier as a set of requirements that are expected to be fulfilled. Furthermore, an organization must also consider additional risks related to the employment of supplier, service provider, or an outsourcer as these are commonly not addressed when initial risk assessment is undertaken.

Annex A of the ISO/IEC 27001 in section A.15 Supplier relationships (A.15.1 information security in supplier relationships, and A.15.2 supplier service delivery management) gives some guidelines on how to address the issue of suppliers in the context of information security.

6. Information Security Incident Management

Information Security Incident Management process is an essential part of the initial implementation and a foundation for further development and improvement of the ISMS. Through implementation of the Incident Management process an organization prepares for the inevitable case when some of the proactively managed risks are nevertheless realized and have negative impact on the organization. The process aims to resolve incidents in the shortest time, providing clear set of actions, communication channels, and resolve methods to limit or reduce the impact the incident has on the organization.

On the other hand, Incident management process is also focused on continuous improvement. The Incident Management process requires an organization to deal not only with major incidents but also requires it to continuously record any and all security events and recognized weaknesses. By insisting on recording of all events, weaknesses, and incidents the organization creates a very useful dataset that can be further analyzed to learn from and to identify certain trends to proactively act in order to not have weakness turn into incidents or to not have incidents unnecessarily repeat themselves. Without an adequately implemented process of learning from incidents, an organization robs itself of an opportunity to continuously improve information security posture based on past events and recorded data.

Related to the business resilience and business continuity aspects in any organization, the incident management process is a cornerstone of the whole BCM. An appropriately implemented incident management process will allow (at the point when all other incident dealing strategies are exhausted) a link to the business continuity arrangements and information continuity arrangements previously planned and implemented.

7. The Implementation of Information Security Management Systems into the Business Processes

As one can expect, the implementation of ISMS must be integrated with existing business processes, and not as a separate set of rules, policies, or procedures. In essence, an organization must recognize (within an existing process) additional activities, steps, or employment of specific

security technology in the process and change that process in order to comply with standard's requirements or in order to reduce the levels of anticipated risks.

To do this, full engagement of all levels in the organization is required, especially top and middle management. Top management will insist on compliance with newly designed processes, and middle management will be tasked to participate in the design and implementation of ISMS controls and mechanisms within their domain of control.

Furthermore, one of the most important activities in successful implementation of ISMS will be raising information security awareness among all interested parties. The aim of the awareness will be to first change people's attitude and perceptions (common misconceptions) about information security and the associated risks, and then to change their behavior (in line with a set of policies, procedures and rules defined and prescribed as an answer to the identified risks). This change in people's attitude and behavior cannot be done through a single activity (e.g. introductory awareness PowerPoint) but must be managed though carefully developed and executed awareness program which will encompass variety of activities sprinkled throughout the year (e.g. various topic-specific presentations, monthly emails with tips and tricks, posters throughout premises, organization of a security day event etc.).

8. Rationale for Engaging in ISMS Systems with View to Business Resilience

As mentioned earlier, information security (as ISO 27001 defines it) covers three main aspects of information security: a) Confidentiality, b) Integrity and c) Availability of information and information assets. With this in mind, it becomes apparent that implementation of ISMS offers organizations a systematic approach to ensuring continuing availability of information and

information processing facilities. Therefore, organizations that depend on the information as their main driver in daily operations (and one can argue that it is very hard to find an organization that does not) can benefit greatly from implementation of the ISMS. Implementation of ISMS creates a framework of policies, procedures, governance mechanisms, and security controls which improve organizations' overall security posture and consequently its ability to better respond to both, the negative changes but also to the presented opportunities.

9. Certification Against ISO/IEC 27001

Independent certification of the implemented information security management system (ISMS) serves as a proof to the interested parties (clients, suppliers, public etc.) that an organization has, in fact, functional and compliant ISMS - based on the requirements of ISO 27001. This gives a level of assurance to the interested parties that the organization has undertaken all steps to build a management system that will proactively deal with information security risks with intention to continually improve it.

Certification can be done by an accredited certification body. Even though marketplace is saturated with companies claiming to provide easy certification, organizations seeking certification should carefully investigate any potential certification agency in order to assess their accreditation, quality, technical competence, working practices, past performance etc.

One of the most critical factors should be their accreditation – meaning that they are accredited – i.e. their certification practices have been checked by a recognized accreditation body (usually on national level) to ensure that issued certificates meet minimum requirements defined in ISO/IEC 17021 (Conformity assessment – Requirements for bodies providing audit and certification of management systems).

The certification process is very similar for all management systems (ISO 9001, ISO 14001, ISO 22301 etc.), and is based on execution of an external audit(s) performed by competent certification auditors.

Certification audits are performed in two main phases: a) Stage 1 audit (sometimes called pre-audit) and Stage 2 audit (on-site, certification audit).

1. Purpose of the Stage 1 audit is to assess the organization's overall design of ISMS and its preparedness for the next stage. This usually includes review of critical documentation and a short on-site visit to ascertain ability to move to the next phase and to introduce themselves to the organization and to gain more information in preparation for the certification audit.
2. During Stage 2, certification audit, one or more formally appointed auditors work systematically to review and assess compliance to all requirements from ISO/IEC 27001 (there are no exclusions of requirements in ISO 27001 standard) as well as to assess implementation of Annex A controls. Based on the evidence gathered during the audit the auditors will compile audit findings which are usually summarised into following:
    a. Observation (also called Opportunities for Improvement): minor concerns or potential future issues that should be considered
    b. Minor Nonconformity (sometimes referred as Nonconformity Type B):
    Partial fulfilment of a requirement. Nonconformity does not impact system's ability to fulfil identified results
    c. Major Nonconformity (sometimes referred as Nonconformity Type A):

Requirement is not addressed, or there is a total failure of its effectiveness. Nonconformity raises significant doubt as to the adequacy of the ISMS to protect confidentiality, integrity, or availability of sensitive information.

Upon a successful certification audit a certificate of compliance is issued to the organization with the validity for a period of three years with obligation to perform the mandatory surveillance audits at least once each year following the initial certification audit.

10. Recommended Literature

The Case for ISO 27001, by Alan Calder
All information necessary to assess the value of implementing ISMS and to create a business case

Nine Steps to Success - An ISO 27001 Implementation Overview, by Alan Calder
Step-by-step guidance on successful ISO 27001 implementation

www.iso27001security.com
Treasure trove site with down-to-earth explanation of various ISO 27k standards and concepts

www.iso27001security.com/html/forum.html
User forum where experts and implementers of various skill levels meet to ask questions and share experiences

www.pecb.com
Certification body which provides education and certification for individuals on a wide range of disciplines (e.g. ISO 27001 Lead Auditor, ISO 27001 Lead Implementer etc.)

Chapter 4

Supply Chain Management

ISO 28000

By Violeta Haxhillazi

1. What is Supply Chain Management (SCM)?

The term ‘Supply Chain Management’ is relatively new. It first appeared in logistics literature in 1982 as an inventory management approach with an emphasis on the supply of raw materials

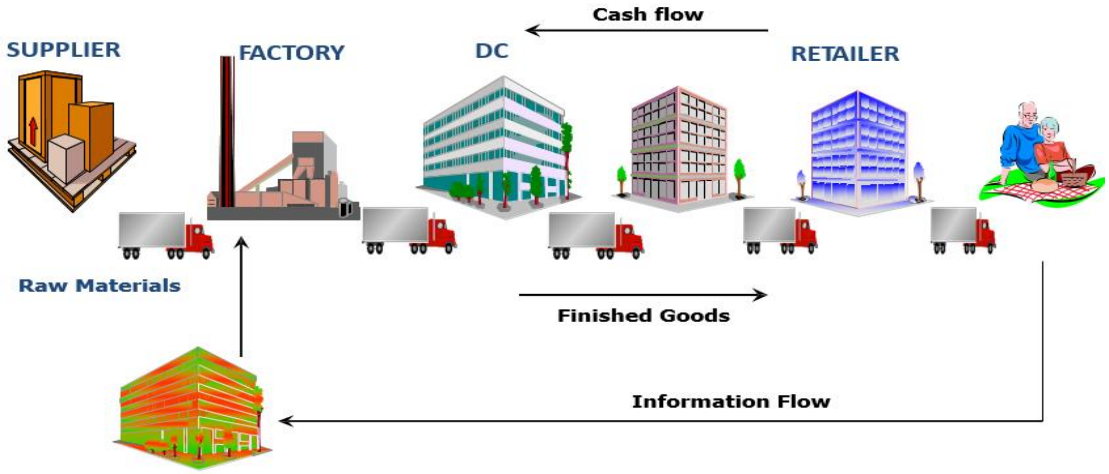
SCM is the integrated planning, co-ordination and control of all business processes 1 and activities in the supply chain to deliver superior consumer value at less cost to the supply chain as a whole whilst satisfying requirements of other stakeholders in the supply chain (e.g. government and NGO’s). (Jack Van der Vorst, 2004)

Supply chain management (SCM) is the active management of supply chain activities to maximize customer value and achieve a sustainable competitive advantage. It represents a conscious effort by the supply chain firms to develop and run supply chains in the most effective and efficient ways possible. Supply chain activities cover everything from product development, sourcing, production, and logistics, as well as the information systems needed to coordinate these activities. (Jack Van der Vorst, 2004)

The concept of Supply Chain Management (SCM) is based on two core ideas:

1. The first is that practically every product that reaches an end user represents the cumulative effort of multiple organizations. These organizations are referred to collectively as the supply chain.
2. The second idea is that while supply chains have existed for a long time, most organizations have only paid attention to what was happening within their “four walls.” Few businesses understood, much less managed, the entire chain of activities that ultimately delivered products to the final customer. The result was disjointed and often ineffective supply chains.

The organizations that make up the supply chain are “linked” together through physical flows and information flows. (Jack Van der Vorst, 2004)



Physical Flows

Physical flows involve the transformation, movement, and storage of goods and materials. They are the most visible piece of the supply chain. But just as important are information flows.

Information Flows

Information flows allow the various supply chain partners to coordinate their long-term plans, and to control the day-to-day flow of goods and materials up and down the supply chain.

A firm's SCM efforts start with the development and execution of a long-term supply chain strategy. Among other things, this strategy should:

- Identify what supply chains the firm wants to compete in.
- Help managers understand how the firm will provide value to the supply chain.
- Guide the selection of supply chain partners, including suppliers, subcontractors, transportation providers, and distributors.
- Quality Assurance and conformity assessment measures.

As firms struggle to understand what supply chains they compete in, it is often valuable to map the physical flows and information flows that make up these supply chains. From these maps, firms can begin to understand how they add value, and what information is needed to make the supply chain work in the most effective and efficient way possible.

Of course, the firm's supply chain strategy does not exist in a vacuum. It must be consistent with both the overall business strategy and efforts within such areas as purchasing, logistics, manufacturing and marketing. (SCRC SME, 2018)

2. Client and Relationship with Supply Chain Management

Supply chain management is as much a philosophical approach as it is a set of tools and techniques, and typically requires a great deal of interaction and trust between companies to

work. For right now, however, let's talk about three major developments that have brought SCM to the forefront of management's attention. *(SCRC SME, 2018)*

- The information revolution
- Increased competition and globalization in today's markets
- Relationship management

2.1. The Information Revolution

In the early 1960s when computers were first developed, a mainframe computer filled an entire room. With the development of the integrated circuit, the cost and speed of computer power increased exponentially. Today, a laptop computer exceeds the storage and computing capacity of mainframe computers made only 15 years ago. With the emergence of the personal computer, optical fiber networks, and the Internet, the cost and availability of information resources allows easy linkages and eliminates information-related time delays in any supply chain network. Wal-Mart's ability to send daily sales information to its suppliers is just one example. (SCRC SME, 2018)

Organizations are moving towards a concept known as electronic commerce, where information transactions are automatically completed via Electronic Data Interchange (EDI), Electronic Funds Transfer (EFT), Point of Sale (POS) devices, and a variety of other approaches. The late 1990s and early 2000s saw the emergence of on-line "trading communities" that put thousands of buyers and sellers in touch with one another. The old "paper"-type transactions are becoming increasingly obsolete. At the same time, the proliferation of new telecommunications and computer technology has made instantaneous communications a reality. Such information systems — like Wal-Mart's satellite network — can link together suppliers, manufacturers, distributors, retail outlets, and ultimately, customers, regardless of location. (SCRC SME, 2018)

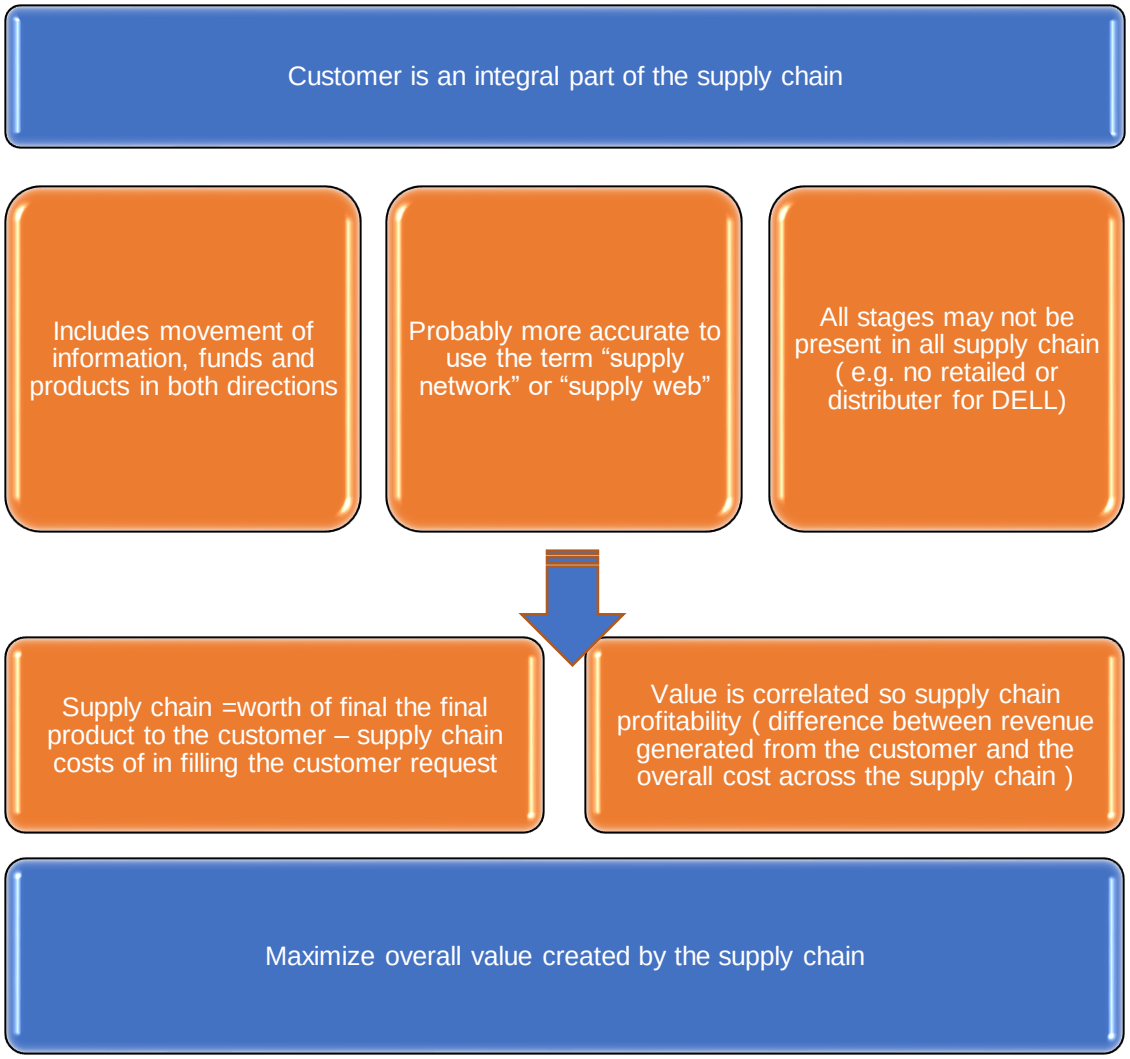
2.2. Increased Competition and Globalization

The second major trend is increased competition and globalization of businesses. The rate of change in markets, products, and technology is increasing, leading to situations where managers must make decisions on shorter notice, with less information, and with higher penalty costs. New competitors are entering into markets that have traditionally been dominated by "domestic" firms. At the same time, customers are demanding quicker delivery, state-of-the-art technology, and products and services better-suited to their individual needs. In some industries, product life cycles are shrinking from years to a matter of two or three months. One management guru even compared current global markets to the fashion industry, in which products go in and out of style with the season. (SCRC SME, 2018)

Despite the imposing challenges of today's competitive environment, some organizations are thriving. These firms have embraced the changes facing today's markets, and have put a renewed emphasis on improving their operations and, in particular, supply chain performance. For instance, Johnson Controls can now receive an order for seats from a Ford assembly plant, make the seats, and deliver the order — all within four hours. This requires incredibly flexible operations within Johnson's own manufacturing systems, as well as dependable information links with its supply chain partners. (SCRC SME, 2018)

To survive, many firms today find that they must increase market share on a global basis and be on the "ground floor" of rapid global economic expansion. Simultaneously, these firms must

vigorously defend their domestic market share from a host of “world class” international competitors. To meet this challenge, managers are seeking to find ways to rapidly expand their global presence. They must position inventories so products are available when customers (regardless of location) want them, in the right quantity, quality and for the right price. This level of performance is a constant challenge to organizations, and can only occur when all parties in a supply chain are “on the same wavelength”.



The information revolution has given companies a wide range of technologies for better managing their operations and supply chains. Furthermore, increasing customer demands and global competition have given firms the incentive to improve these areas. But this is not enough. Any efforts to improve operations and supply chain performance are likely to be inconsequential without the cooperation of other firms. As a result, more companies are putting an emphasis on relationship management. (SCRC SME, 2018)

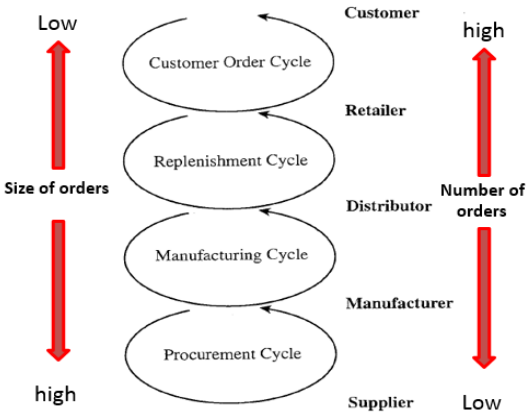
Of all the activities operations and supply chain managers perform, relationship management is perhaps the most difficult, and is therefore the most susceptible to break down. A poor relationship within any link of the supply chain can have disastrous consequences for all other supply chain members. For example, an unreliable supplier can virtually cripple a plant, leading to inflated lead times and resulting in problems across the chain, all the way to the final customer.

To avoid such problems, firms must manage the relationships with their upstream suppliers as well as their downstream customers. In many American industries, strong supply chain relationships like those found Japan might not develop readily.

Firms are often geographically distant, and there are not as many small, family-owned suppliers. In the case of high-tech firms, many components may be sole-sourced from overseas suppliers who are proprietary owners of the required technology. In such environments, it becomes more important to choose a few, select suppliers, thereby paving the way for informal interaction and information sharing. (SCRC SME, 2018)

3. Supply Chain Operations, Processes and Planning

- ***Cycle View:*** The processes in a supply chain are divided into a series of cycles, each performed at the interface between two successive stages of a supply chain.
  - *Customer order cycle*
  - *Replenishment cycle*
  - *Manufacturing cycle*
  - *Procurement cycle*



3.1. Customer Relationships

For a company to build a large following of loyal customers, it needs to build a solid relationship with each and every one of the people or organizations it does business with.

As with any type of relationship, the foundation has to be communication and trust. Regarding communication, suppliers need to be transparent with all information that may impact the customer in any way. As for trust, the customer needs to be confident that the supplier will follow through on their end of the deal.

Customer relationship management, then, intertwines with supply chain management in two key ways:

- Keeping the customer "in the know" with regard to their order status
- Ensuring the customer receives their order exactly as expected

While the bulk of supply chain management processes occur "behind the scenes," each of these processes ultimately impacts the customer. By keeping the customer in mind as you improve your supply chain processes, you'll ensure that any changes you make will provide a better experience for them. (Baldwin, R, 2020)

3.2. Customer Service

Customer service management takes the more abstract concepts involved with customer relationship management, and develops a concrete plan to actually put these ideas into action.

That said, customer service management involves defining how your team will:

- Optimize communication and the delivery of information between your team and your customers

- Streamline the delivery of technical and other operational support to your customers in need
- Improve your overall processes so as to avoid technical and operational issues in the first place

Again, supply chain management and customer service management go hand-in-hand: an issue in one area often means an issue in the other. For example, if a delivery is held up in any way, you'll need to know the best way to solve the problem from the customer's perspective.

Customer service issues are inevitable, especially when it comes to the unpredictable nature of supply chains. Rather than taking these issues as they come, you need to have a firm plan in place for dealing with them when and if they do. (Baldwin, R, 2020)

3.3. Demand Management

Demand forecasting is a key element in planning a supply chain strategy, and in turn determining the agility and responsiveness of a business to fluctuating demand.

With demand volatility at an all-time high, there is no ongoing "standard" for most businesses—which is why demand planning and inventory optimization are a necessity.

Creating a systematic process for forecasting helps businesses to do the following:

- Maintain optimal stock levels, regardless of fluctuations
- Effectively manage distribution networks
- Maximize warehousing and inventory cost efficiencies
- Make data informed decisions about sales and marketing
- Scale up and expand into new markets
- Respond quickly to changing market conditions
- Prepare budgets, bookkeeping, and accounting
- Reduce the need for safety stock

All of the above contribute to a more efficient supply chain, increased sales, and improved customer satisfaction.

3.4. Order Fulfillment

Order management and fulfillment is a major component of successful supply chains for both large and small businesses alike.

Modern order fulfillment revolves heavily around the use of technology. With automation at the forefront of eCommerce, consumers can now place orders at the touch of a button — *without* needing anyone from your team to walk them through the process. (Inoue, H and Y Todo, 2017)

If information regarding incoming orders isn't properly communicated to those responsible for supply chain-related duties, they aren't going to be able to fulfill these duties to the best of their ability.

Obviously, the worst-case scenario involves your fulfillment team completely overlooking orders as they come in from your customers. Needless to say, this can cause even the most loyal customers to defect to a competing brand.

But a suboptimal approach to order fulfillment can also lead to losses for your business in the form of wasted resources.

For example, if you don't have a strategic plan in place for your picking, packing, and fulfillment processes, you might end up overusing your shipping materials, facing operational redundancies and obstacles, and increasing the inherent risk of fulfilling the order altogether. (Inoue, H and Y Todo, 2017)

On the other hand, improving order fulfillment benefits your overall supply chain in that you'll be able to:

- Save time, money, and other resources
- Minimize room for error
- Consolidate real-time information throughout multiple channels
- Provide transparency to your audience
- Individualize the experience for your customers

3.5. Manufacturing Flow

Manufacturing flow management refers to the processes involved in ensuring manufacturing of products occurs in a way that is economical and profitable.

Essentially, manufacturing flow management involves knowing how much of a given product will need to be produced at a given point in time—and creating *just* enough so as to not risk wasting inventory space, spoilage, etc.

Proper manufacturing flow management also decreases the potential for stock-outs due to insufficient orders on your company's part.

Since this all deals with the initial stages of the supply chain, it should be clear that anything that occurs throughout these stages — good or bad — will affect all else that goes on throughout the supply chain moving forward. (Robert Handfield, 2017)

3.6. Supplier Relationships

Whether you are an eCommerce retailer or a regular stockist, supplier relationship management should hover near the top of your must-do list.

- Because suppliers play a critical role in your business, it's only right to treat them as a partner. A strong relationship with your suppliers can allow you to further streamline your supply chain, enhance your ability to deliver value to your customers, and improve your company's bottom line.
- Forging and solidifying relationships with your suppliers involves:
- **Open and honest communication**: You need to make sure your suppliers know exactly what you need and expect from them, so they can easily tailor their services to these needs.

- **Forging a solid agreement**: In turn, you need to be clear about the value *your* company brings to the table. This extends past contractual, on-paper agreements and majors on the overarching benefits your company will have *on their business*.
- **Developing a solid plan of attack**: Forging a strong relationship isn't something that just "happens." Rather, you need to be systematic and strategic in how you engage with your suppliers to ensure a mutually-beneficial outcome for both parties.

3.7. Product Development and Commercialization

The reason you sell the products you do in the first place is because your target customers have a need for them.

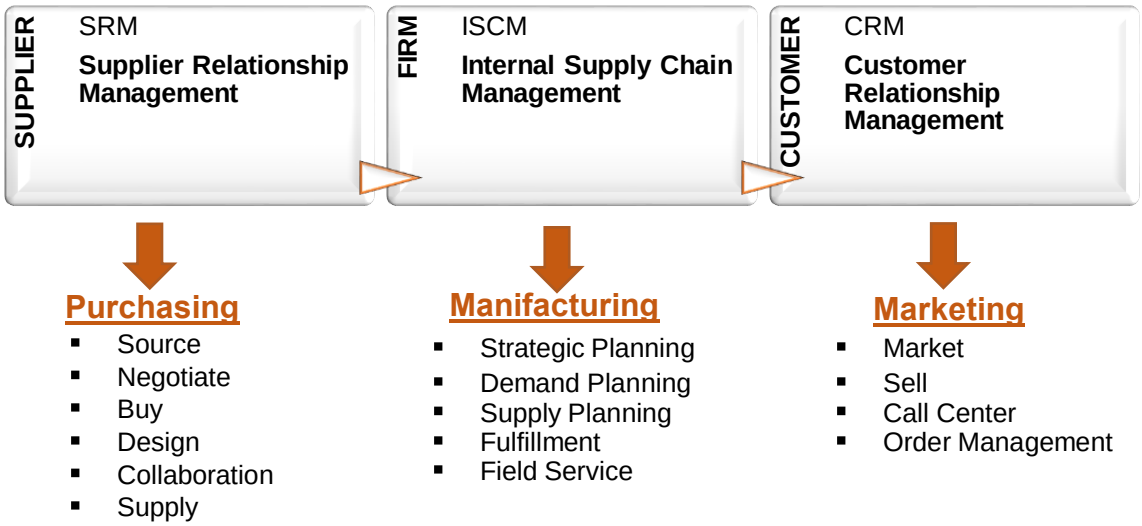
More accurately, your customers have a need for a product that delivers the value yours does. But, your individual customers' needs will likely vary in many different ways — and it's your job to ensure the product they receive from your company meets these various needs. (Baldwin, R, 2020)

This may mean:

- Making alterations to your products
- Changing its branding, packaging, and unboxing
- Providing bulk orders of various sizes or discounts, or even
- Developing additional features for a future version of a product
- QA measures.

Whatever the case may be, where and how you differentiate your products for your customer segments or individual customers will have a huge impact on the rest of your supply chain.

For this reason, it's vital that you make these individualized alterations as close to the end of the supply chain as possible.



3.8. Importance and Benefits Supply Chain Operations and Processes

To Achieve Economies of Scale and Scope – Costs are Significant

- Internal SC functions lack economies of scale when compared with the potential capacity of an independent provider of the same product / service.
- Attractive pricing – volume leverage.

To Improve Business Focus and Expertise

- Vertical integration multiplies the complexities of managing disparate businesses. An independent company that focuses entirely on a particular business can develop more expertise than an in-house department
- Higher Quality, Attractive Pricing or both

Customer Expectations are Increasing

- Rapid processing of Customer Request
- Quick delivery (shorter Order Cycle Time)
- High degree of Product Availability
- Lower Prices

Supply and Distribution Lines are Lengthening with Greater Complexity

- Cut costs and expand markets
- Trend towards an integrated world market
- Designing products for world market & producing them wherever raw material, labor, components, overhead etc are lower

Political Arrangements: European Union, ASEAN, SAARC

4. ISO 28000 Supply Chain Security Management Systems

The ISO 28000, Supply Chain Security Management System International Standard, has been developed in response to the high demand from industries. Increasingly, organizations are discovering that they must depend on effective supply chains to compete in the global market. Recent threats and incidents relating supply chains and their level of security have demonstrated that it is crucial for organizations to secure their supply chains to prevent risks. (ISO 28000)

Organizations of all sizes and types that are involved in production and services, storage or transportation at any stage of the product, should consider implementing or improving their Supply Chain Security Management System to determine adequate security measures and comply with regulatory requirements. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs.

Considering the dynamic nature of supply chains, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management.

A formal approach to security management can contribute directly to the business capability and credibility of the organization.

This International Standard is based on the ISO format adopted by ISO 14000:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2015) may be able to use their existing management system as a foundation for a security management system as prescribed in this International Standard.

The ISO 28000:2007 is based on the methodology known as Plan-Do-Check-Act (PDCA), which can be described as follows. (PECB)

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy.
- Do: implement the processes.
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.
- Act: take actions to continually improve the performance of the security management system.

ISO is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

- establish, implement, maintain and improve a security management system;
- assure conformance with stated security management policy;
- demonstrate such conformance to others;
- seek certification/registration of its security management system by an accredited third party certification body;
- make a self-determination and self-declaration of conformance with ISO 28000:2007.

5. Security Risk Assessment and Planning

Furthermore, the organization shall prepare the security risk assessment and planning for the supply chain security management system.

5.1. Security Risk Assessment

This assessment shall consider the likelihood of an event and all of its consequences which shall include:

- physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action;
- operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety;
- natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective;
- factors outside of the organization's control, such as failures in externally supplied equipment and services;
- stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand;
- design and installation of security equipment including replacement, maintenance, etc.
- information and data management and communications;
- a threat to continuity of operations.

5.2. Legal, Statutory and Other Security Regulatory Requirements

A procedure should be established, implemented and maintained to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and to determine how these requirements apply to its security threats and risks.

5.3. Security Management Objectives

A procedure should be established, implemented and maintained to document security management objectives at relevant functions and levels within the organization, which shall be consistent with the policy.

5.4. Security Management Targets

Documented management targets shall be appropriately established, implemented and maintained to the needs of the organization, which shall be consistent with the security management objectives. These targets shall be:

- to an appropriate level of detail;
- specific, measurable, achievable, relevant and time-based (where practicable);
- communicated to all relevant employees and third parties including contractors; and
- reviewed periodically to ensure that they remain relevant and consistent with the security management objectives. Where necessary the targets shall be amended accordingly.

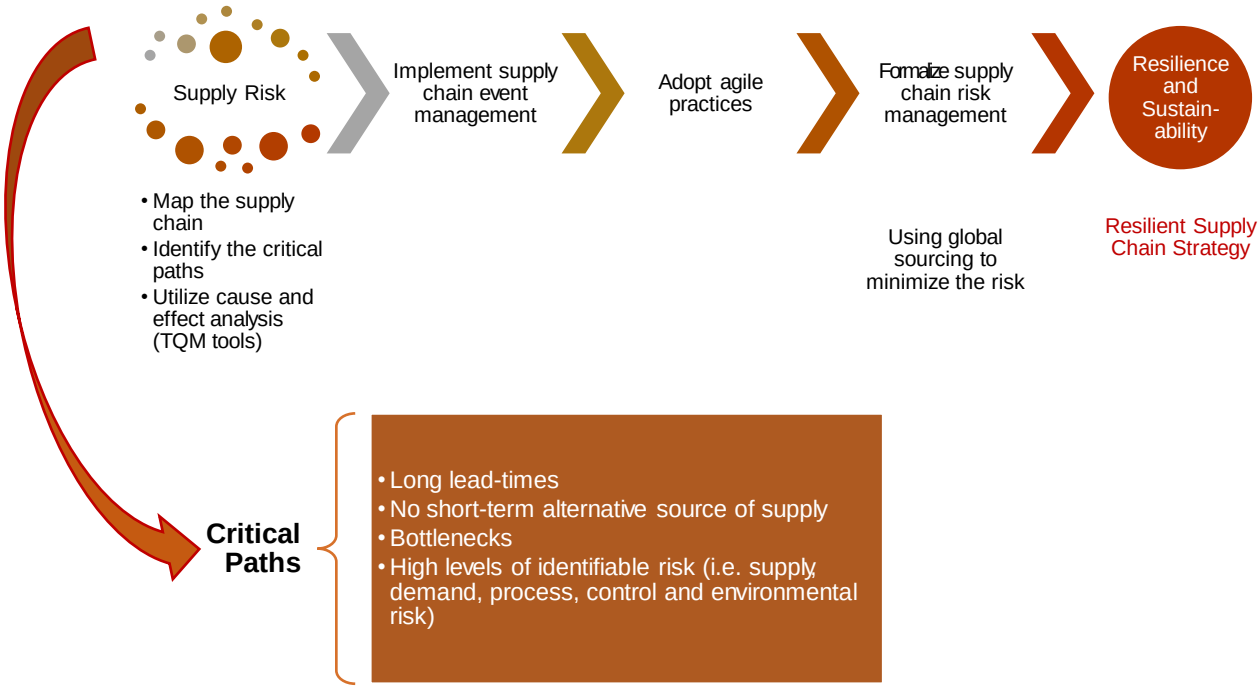
5.5. Security Management Programs

Management programs are established, implemented a maintained for achieving objectives and targets, which shall be optimized and then prioritized.

6. Managing SCM Risk

85% of surveyed global chains experienced at least one supply chain disruption risk in 2017. Deloitte has shown that organizations who proactively manage supply chain risk spend 50% less to manage disruptions (Rebecca Webb, 2019). As always, proactive risk management is more cost efficient than reactive action. An efficient supply chain is essential for the production of quality products and effective customer service. Supply chain management involves many changing factors. Of course, there are natural disasters, supplier changes, and system updates, all of which may inhibit one or more links of the supply chain. But risk managers must also keep on top of regular changes in supply and demand in rapidly growing (or shrinking) industries. (Rebecca Webb, 2019)

To manage supply chain risks, managers can do the following:

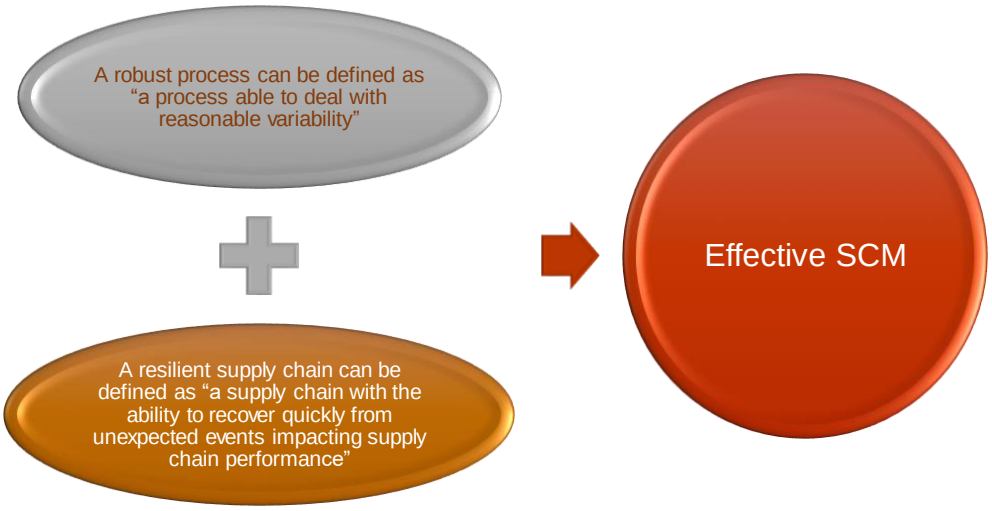


7. Robust or Resilient? Or Both?

The risk management literature makes an important distinction between resilience and robustness in supply chains. (Sébastien Miroudot, 2020)

- Resilience can be defined as the ability to return to normal operations over an acceptable period of time, post-disruption.
- Robustness is the ability to maintain operations during a crisis (Brandon-Jones et al. 2014).
- Building robustness requires different strategies, when compared to building resilience, and when it comes to the distribution of key medical supplies (such as face masks, ventilators, medicines), it is robustness that matters, not resilience.

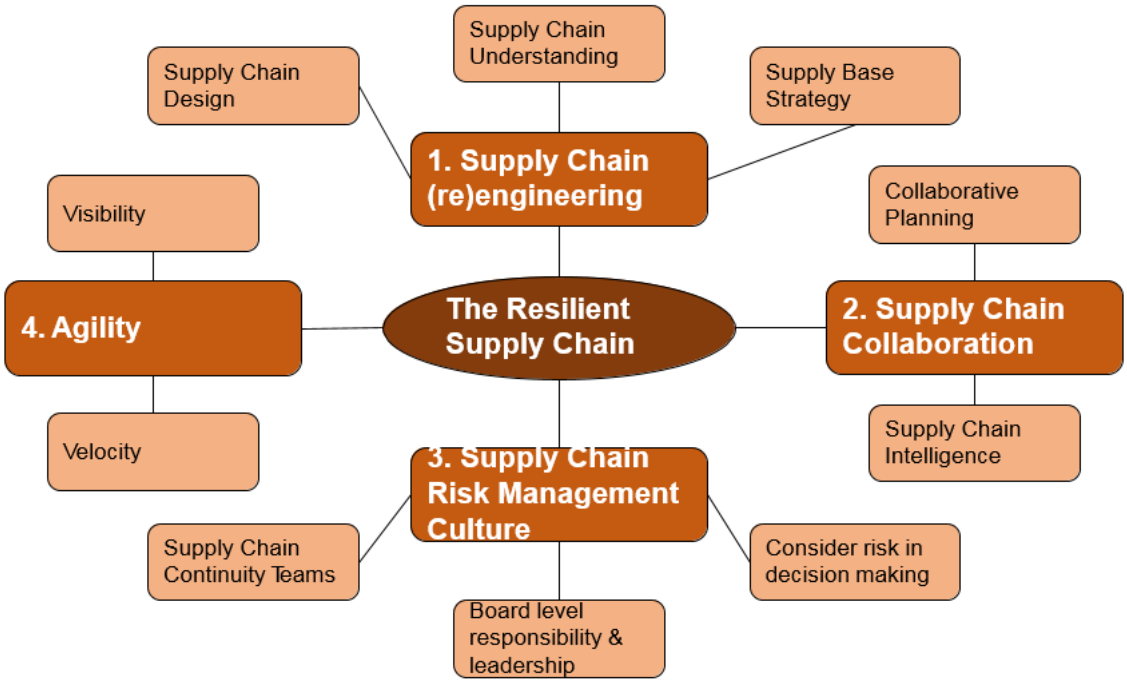
For example, the redundancy in suppliers or alternative locations of production is a strategy for *robustness*. Firms that have diversified suppliers and a production network across different countries can adjust their production when a disaster occurs in one place. After the earthquake in Japan in 2011, the experience led to manufacturers in the motor vehicles industry diversifying their suppliers (Matous and Todo 2017).



8. Resilient & Secure SCM Strategy

Supply chain resilience no longer implies merely the ability to manage risk. It now assumes that the ability to manage risk means being better positioned than competitors to deal with—and even gain advantage from—disruptions.

Companies can develop resilience in three main ways: increasing redundancy, building flexibility, and changing the corporate culture. The first has limited utility; the others are essential. . (Paul Michelman, 2007)



8.1. Redundancy.

Theoretically, a resilient enterprise can be built by creating redundancies throughout the supply chain. The organization could hold extra inventory, maintain low capacity utilization, have many suppliers, etc. Yet although redundancy can provide some breathing room to continue operating after a disruption, typically it is a temporary—and very expensive—measure. . (Paul Michelman, 2007)

8.2. Flexibility.

In contrast, when a company increases supply chain flexibility, it can both withstand significant disruptions and better respond to demand fluctuations.

8.3. Cultural Change.

After a disruption, the factor that clearly distinguishes those companies that recover quickly, and even profitably, from those that falter is corporate culture.

Continuous Communication Among Informed Employees.

They keep all personnel aware of the strategic goals, tactical factors, and day-by-day and even minute-by-minute pulse of the business. Thus, when a disruption takes place, employees know the company's status: what is selling, where the raw materials are, what it is they were trying to do before the disruption hit, and so on. They can use that knowledge to make better decisions in the face of the unforeseen. (Brandon-Jones, E, B Squire, C W Autry and K J Petersen, 2014)

Distributed Power, so that Teams and Individuals are Empowered to Take Necessary Actions.

Before a potential disruption is even visible to managers, those that are thus empowered and are "close to the action" can take necessary measures; moreover, they can respond quickly, significantly enhancing the chances of containing a disruption early on. . (Paul Michelman, 2007)

Passion for Work

Herb Kelleher Quote: "The important thing is to take the bricklayer and make him understand that he's building a home, not just laying bricks."

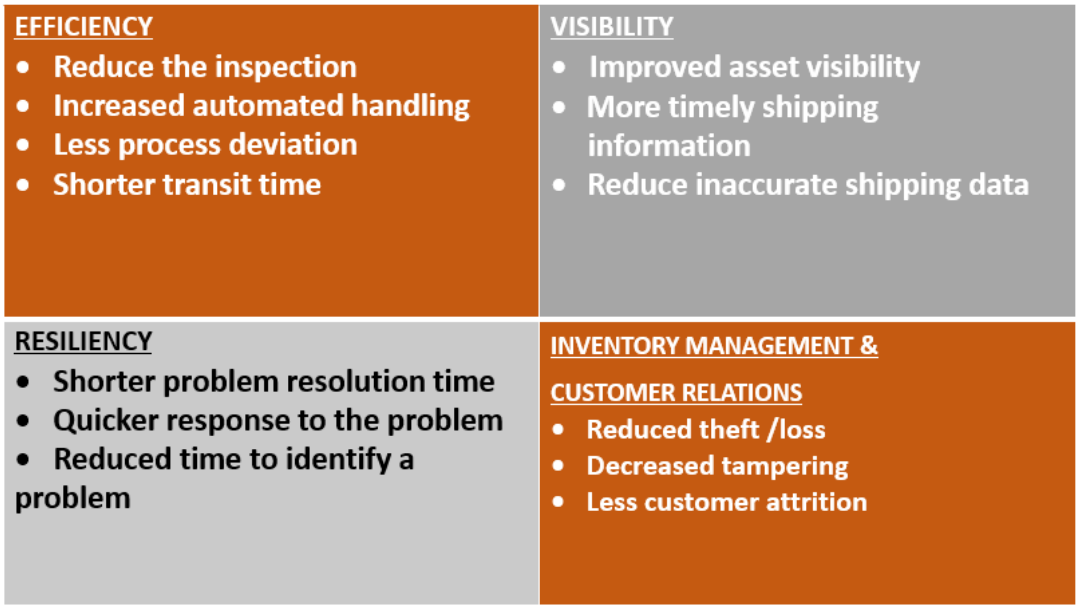
Conditioning for Disruptions

Resilient and flexible organizations are apparently conditioned, as a result of frequent and continuous "small" operational interruptions, to become innovative and flexible in the face of disruptions.

9. Benefits of Resilient & Secure SCM

The rewards for building a resilient organization are substantial. The “hardened” enterprise will be able to not only withstand all manner of disruption but also increase its competitiveness. Unforeseen disruptions can create shortages that are not dissimilar to the demand spikes caused by supply/demand imbalances; resilient enterprises can thus react to changing market demand ahead of their competitors. Therefore, resilience increases the competeveness. (Paul Michelman, 2007)

That is reflected in different aspects as pictured in the below graph:



10. References

Baldwin, R, 2020 “Supply Chain contagion waves: Thinking ahead on manufacturing ‘contagion and reinfection’ from the COVID concussion”

Brandon-Jones, E, B Squire, C W Autry and K J Petersen, 2014, A contingent resource-based perspective of supply chain resilience and robustness

Inoue, H and Y Todo, 2017, Mitigating the propagation of negative shocks due to supply chain disruptions

ISO 28000 Supply Chain Security Management Systems

Jack Van der Vorst, 2004,Supply Chain Management: theory and practices

Paul Michelman, 2007, HBR-Building a Resilient Supply Chain

PECB: Standards in the supply chain management (ISO 28000 and ISO/TS 22318)

Rebecca Webb, 2019, 4 Ways to Manage Supply Chain Risks

Robert Handfield, 2017, Supply Chain Resource Cooperative

Saenz and Revilla, 2014, Building resilient supply chains

Sébastien Miroudot, 2020, Resilience versus robustness in global value chains: Some policy implications

SCRC SME, 2018, Author at Supply Chain Resource Cooperative

Chapter 5

Occupational Health and Safety Management

By Suzana Temelkoska

1. Foster a Healthy and Safe Environment in Crisis Situations

The health crisis generated by the global pandemic of COVID-19 has affected all economies, impacting the health and safety of workers.

Although some economic sectors and companies have been able to implement remote work policies, an important number of workers continue to commute to their workplaces (e.g. workers in the health and public sectors, commerce, transport, agriculture, food, utilities, and security forces). In all cases, new and increased occupational risks are presently urging stakeholders to undertake risk assessments and implement preventive measures.

Moreover, workers and their families and business owners are facing increasing mental health challenges. The key risk factor that could lead to depression and other mental illnesses are psychosocial factors (such as work-life balance, isolation, anxiety, and stress from work overload combined) and job-related uncertainties (such as possible closure of businesses and the threat to employment security, return to the workplace and employer-employee issues).

The management of the safety and health of workplaces should start with risk assessments and the adoption of prevention and protection measures. Strict protocols such as hygiene and sanitation measures, the use of adequate and sufficient personal protective equipment, the (re)design of jobs and functions, the organization of work, preventive training, and monitoring of the health of workers must be implemented. The sudden shift to remote work for a great number of workers has increased risks because the workplace at home is inadequate. Inadequate ergonomics, as well as pre-existing health conditions, can be exacerbated working from home.

Amid the COVID-19 outbreak, it's now more important than ever to become ISO 45001 certified and implement an effective safety management system to keep your team safe no matter what happens.

To be ISO 45001 certified, first, you must complete an analysis of your business from top to bottom and identify any existing gaps, incompetence, resources, or safety measures. These gaps will need to be filled before your business can become ISO 45001 certified. Amid the COVID-19 outbreak, it's important to remember that no one is ever fully prepared for a global pandemic. You're bound to find at least a few new gaps. For example, you may have noticed a need for further staff training in cleanliness or disease control, a requirement for face masks and gloves to be available on-site (regardless of your industry), or best practice guidelines for team members working off-site.

At best, companies would need to maintain business as usual, in fact, all businesses need to be committed more than ever to improving and adapting the certification process to manage pandemic events like COVID-19. A team of professional assessors can assess your business' management system responses to COVID-19 at the strategic, operational, and frontline levels, so you can adjust your business continuity plans for the short, medium, and long term.

Initial measures adopted by some countries were oriented to provide information and advice to workers and employers about the pandemic and to promote healthy and safer workplaces. Access to paid leave has been one of the measures proposed to workers to comply with physical isolation measures recommended by public authorities. Employment injury schemes have provided support to workers affected by the disease, including medical benefits. Some occupational diseases derived from the pandemic have also been covered by these schemes. Sickness benefits provided by social security organizations have been amended to guarantee income replacement to workers affected and infected by COVID-19. Measures are also being designed to facilitate a safe return to workplaces after the pandemic. The current crisis is a unique opportunity to reassess the central role of occupational safety and health and its eventual recognition as a fundamental right and principle at work, following the recommendation of the World Commission on the Future of Work.

The ISO 45001 standard does not only reflect the risk to the health and safety of workers during the ongoing COVID-19 pandemic but also the overall risks assessments and preventive measures that all workplaces need to be undertaking to protect the health and safety of their workers.

OH&S has grown increasingly complicated with many of today's businesses crossing national boundaries. The dispersed nature of supply chains creates escalating levels of risk for multinational businesses, making OH&S both critical and complex. Consider this. Without effective OH&S in their supply chains, management potentially has a significant blind spot in their enterprise management structure, from which substantial legal, financial and reputational exposure could emerge. An organization must therefore look beyond its immediate health and safety issues and take into account what the wider society expects of it. What's more, it also has to think about its contractors and suppliers, since the way they do their work might affect their neighbors in the surrounding area.

ISO 45001 provides valuable information on the requirements of a health and safety management system. To this end, the standard describes the important elements and also provides systematic guidance to help organizations and businesses of all sizes and types provide safe workplaces, whether they are a non-profit organization, a ministry, a micro-enterprise, or a global conglomerate.

As a result of the high-level structure, which is basically a standardized process description for ISO standards, ISO 45001 contains a lot of content that has great similarities to the standards ISO 9001 (quality management) and ISO 14001 (environmental management) that have already been mentioned. These include, for example, explanations of the context of the organization or company, which not only consider the impact of health and safety aspects on their own operations but also take into account external interest groups such as suppliers and authorities.

This means that top management must take a visible, direct role and be actively involved in the system's implementation and ensuring its integration with other business systems. The system needs to be proportionate to the organization's risk profile and complexity. For example, in smaller organizations, effective worker participation can be more direct and straightforward to achieve, without the need for formal committee structures and so forth.

2. ILO Policies and Documents Referring to Safety and Health

The International Labor Organization (ILO) has a goal to design worldwide awareness of the result and dimensions of the work-related injuries, impaired health, diseases and to promote the health and safety of all workers on an international level, to stimulate and give support practical action measures at all levels. Every work should be safe work.

The International Labor Organization (ILO) has published policies, codes of practices, guidelines to give practical arrows in the fundamental areas of the employees' health and safety. Their published documents are helping the organizations to meet the legal obligations, protect the employees, and to raise the health and safety environment to the next level.

The standards that are published by ILO (International labor standards) represent a legal instrument prepared by ILO's components such as employers, workers, and governments. They aim to set up basic principles and rights at work. The main principles are conventions, which are legally binding international treaties that might be ratified by member states, or recommendations that serve as nonbinding guidelines. The ILO's standards for occupational health and safety are providing the essential main instrument for employers, workers, governments to prevent, report, and inspect practices and give maximum safety at work. The ILO has adopted more than 40 standards for dealing with occupational health and safety. Almost, half of ILO documents and policies are connected directly or indirectly with occupational health and safety.

ILO Constitution aims to the principle that workers must be protected from disease, illness, injuries starting from their employment, even though the reality for millions of workers on a global level is quite different. Accordingly, in the recent period, ILO global has estimated that 2.78 million work-related deaths are noticed every year, of which 2.4 million are noticed to occupational diseases.

Additionally, there are identified losses in terms of compensation, lost workdays, interrupted production, training, health care expenses that are 3.94 % of the world's annual GDP. The employers are facing costs for early retirements, losses of skilled staff, high insurance premiums. However, many of the tragedies that are identified during work time are preventable, through the implementation of sound prevention, reports, and inspection practices. ILO standards on OHS provide main tools for the ILO's components (employers, workers, and governments), such as practices, measures in order to achieve maximum safety at work.

© istockphoto

ILO has provided the main key instruments on occupational health and safety. On the following link, you can check all of the instruments that are provided by ILO:

https://www.ilo.org/dyn/normlex/en/f?p=1000:12030:0::NO:::#Occupational_safety_and_health

These are the main key instruments for occupational health and safety at work:

- Promotional Framework for Occupational Safety and Health Convention – Represents an instrument setting out a promotional framework, to provide a coherent and systematic treatment of OHS issues and to offer a promotion on the Conventions of OHS. Their purpose is to establish and implement national policies on OHS through a dialogue between the interested parties and to promote a national preventive safety and health culture.
- Occupational Safety and Health Convention - The convention provides for the adoption of a coherent national occupational safety and health policy, and action to be taken by governments and within enterprises to promote occupational safety and health and to improve working conditions. The Protocol calls for the establishment and the periodic review of requirements and procedures for the recording and notification of occupational accidents and diseases.
- Occupational Health Services Convention - This convention provides for the establishment of enterprise-level occupational health services which are entrusted with essentially preventive functions and which are responsible for advising the employer, the workers, and their representatives in the enterprise on maintaining a safe and healthy working environment.

The following conventions that are published by ILO represent health and safety in particular branches of economic activity:

- Hygiene (Commerce and Offices) Convention that has a purpose of preserving the health and welfare of workers employed in trading establishments, and institutions and administrative services in which workers are mainly engaged in office work and other related services through elementary hygiene measures.
- Health and Safety in Construction Convention that purpose is to provide preventive measures according to the specifics of this sector. The measures include safety of the workplace, machines and used equipment in construction, working in heights, and the work performed in compressed air.
- Health and Safety in Mines Convention has a purpose to regulate aspects of health and safety for workers in mines and perform activities in the mines, such as inspection, working equipment, the needed protective equipment for the workers, and rescue in mines.
- Health and Safety in Agriculture Convention has a purpose to set up measures and activities of preventing accidents, injuries in agricultural and forestry work. This includes measures according to the machinery safety and ergonomics, transport and handling of materials, chemical management, measures according to the biological risks and, etc.

Besides the mentioned and described conventions as most important that should be considered and published by ILO, also there are available and published Codes of Practices.

ILO Codes of practices set out practical guidelines for public authorities, employers, workers, enterprises, and specialized occupational safety and health protection bodies (such as enterprise safety committees). They are not legally binding instruments and are not intended to replace the provisions of national laws or regulations or accepted standards. Codes of Practice provide guidance on safety and health at work in certain economic sectors (construction, opencast mines, coal mines, iron and steel industries, non-ferrous metals industries, agriculture, shipbuilding and ship repairing, forestry), on protecting workers against certain hazards (radiation, lasers, visual display units, chemicals, asbestos, airborne substances), and on certain safety and health measures (occupational safety and health management systems; ethical guidelines for workers' health surveillance; recording and notification of occupational accidents and diseases; protection

of workers' personal data; safety, health and working conditions in the transfer of technology to developing countries).

One of the most important documents published by ILO is the Guidelines on occupational safety and health management systems, ILO-OSH 2001, second edition.

According to this Guideline, every organization should have an OSH management system with the following elements: policy, organizing, planning and implementation, evaluation, and action for improvement.

The positive impact of introducing OSH management systems at the organization level, both on the reduction of hazards and risks and on productivity, is now recognized by governments, employers, and workers.

All of the published documents by ILO could be checked on their website on the following link: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/WCMS_107727/lang--en/index.htm

A very useful tool is that all of the documents could be searched by areas of work, and they are divided into the following areas:

- National OSH Systems and Programs
- OSH Management Systems
- Information and Knowledge Sharing
- Occupational Health
- Chemical Safety and the Environment
- Hazardous Work
- Radiation Protection
- Workplace health promotion and well-being
- Occupational Safety and Health Inspection
- Economic Aspects
- Gender and OSH
- Prevention of Major Industrial Accidents

Besides the division on the areas of work, all of the ILO's documents that are ratified and used in the countries could be found on the following link: https://www.ilo.org/global/topics/safety-and-health-at-work/country-profiles/europe/lang--en/index.htm

Every country has its own profile by which the ILO ratified conventions, policies and programs, laws and regulations, and the country authorities and bodies.

According to this pandemic period that the world is facing, and the spread of COVID-19, ILO has published a document publication: In the face of a pandemic: Ensuring Safety and Health at Work (could be checked at the following link: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/publication/wcms_742463.pdf)

By having a comprehensive emergency preparedness plan in the workplace crafted to address health crises and pandemics, workplaces may be better prepared to develop a quick, coordinated, and effective response, while adapting the measures to the specific emergency situation that the enterprise is facing (ILO, 2020i).1 A continuous monitoring of OSH conditions and appropriate risk assessment will be required to ensure that control measures related to the risk of contagion are adapted to the specific evolving processes, conditions of work, and characteristics of the

workforce during the critical period of contagion and afterward, so that recurrences may be prevented.

The ILO has developed a general action checklist for the prevention and mitigation of COVID-19 at work (the action list could be checked on the following link: https://www.ilo.org/global/topics/safety-and-health-at-work/resources-library/publications/WCMS_741813/lang--en/index.htm), a policy brief on a safe and healthy return to work during the COVID-19 pandemic (it could be checked at the following link: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/briefingnote/wcms_745549.pdf) and ten action points for a safe return to work, along with general guidance for employers on COVID-19 prevention: (https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/instructionalmaterial/wcms_745541.pdf)

Also, all of the published documents for occupational health and safety during covid-19 divided by sector could be found on the following link: https://www.ilo.org/sector/Resources/WCMS_746337/lang--en/index.htm

3. The Standard ISO 45001

Standards are a strategic tool that guides more efficient operation, increased productivity, and reduced costs. Aligning the criteria facilitates free and fair trade for developing countries.

Daily application of standards in operations provides confidence in the quality of service/product, high professionalism in operations, and long-term survival in the market.

ISO 45001:2018 - Occupational safety and health management system is a standard that defines the requirements for the occupational safety and health management system. The purpose of the standard is to establish control over the risks that cause harm and dangers, and thus to ensure the continuity of the organization.

ISO 45001 is a global standard for Occupational Health and Safety Management Systems that provides a practical solution to improve the safety and health of both employees and other personnel. This standard has been designed with the intention to be applicable for any company regardless of its size, type, and nature.

The main purpose of the OH&S management system is to secure a frame for the management of occupational health and safety risks and opportunities. Another purpose and predicted results of the OH&S management system is the prevention of workplace injuries and the deterioration of workers' health and the provision of safe and healthy workplaces. The application of the OH&S management system enables the organization to manage its OH&S risks and improve its OH&S performance.

The application of the OH&S management system is a strategic and operational decision of the organization.

The success of the OH&S management system depends on leadership, commitment, and participation at all levels and functions in the organization.

The former label OHSAS - Occupational Health and Safety Assessment Series translates a system for managing the protection of health and safety at work. The standard also uses the abbreviation OH&S, which indicates the affiliation of the elements of the management system in the field of occupational health and safety (For example, policies, objectives, programs).

The ISO 45001 standard is applicable to all organizations. This standard is compatible with ISO 9001, ISO 14001, ISO 27001, ISO 50001 standards by its form and can be easily integrated with them.

The purpose of the management system for the protection of health and safety at work is to translate uncontrolled hazards as much as possible into controlled risk and thus to better protect employees, but also to ensure smooth operation.

Advantages of implementing the ISO 45001 standard:

- Workplace injuries are kept to a minimum
- Protection against possible injuries is provided
- It contributes to the readiness of the organization to eliminate the dangers in the first place
- Complies the work processes with the legal requirements
- Improves the overall image of the organization and makes it attractive for collaboration and investment
- Provides users with confidence that there is a defined health and safety management that can be proven
- Opens new market opportunities for cooperation with international organizations

The basis of the system is the safety of employees in the workplace which is achieved by:

- Defining and assessing hazards in accordance with legal regulations
- Defining a Safety and Health Policy
- Defining hazards in the workplace
- Planning, development and implementation of a safety and health management system
- System certification

The standard:

12.03.2018 the standard is published

ISO 45001: 2018 replaces BS OHSAS 18001: 2007

- The structure of the standard follows Annex SL

From March 2018. begins the 3 year old transition cycle that lasts until 03.2021.

The certification according to OHSAS 18001 will not be valid after 03.2021.

3.1. Characteristics of ISO 45001

Thousands of lives are lost every day due to workplace accidents or deadly work-related illnesses. According to various sources, about 7,600 people die every day from work-related accidents or illnesses, amounting to 2.8 million a year. Injuries and illnesses related to the workplace

significantly burden employers and affect the general economy, which has encouraged the work of preparing a new standard, ie. ISO 45001.

This standard will help organizations improve their health and safety performance to create a work environment that will prevent injuries and illness, but also save lives. The ISO 45001 standard is intended for any type of organization and can be interpreted in other health and safety programs. The application of the new international standard is expected to reduce the number of injuries and accidents at work.

The ISO 45001 standard is aimed at the top management of the organization and aims to provide a safe and healthy workplace for employees and visitors.

The standard refers to the OHSAS 18001 standard, but this is still a new standard, not a revision of the existing one. ISO 45001 helps the organization achieve the planned results of its OH&S management system.

The standard does not provide specific criteria for OHSAS performance, does not address product safety and environmental impact issues. Because ISO 45001 is designed to integrate with other ISO standards for management systems, it provides a high level of compatibility with the new versions of ISO 9001: 2015 and ISO 14001: 2015.

These are the factors of success of the OH&S system:

- Leadership, commitment, and ultimate responsibility of top management
- Top management develops, leads and promotes a culture in the organization that supports the intended outcomes of the OH&S management system
- Communication - external and internal communication
- Consultation and employee participation, and where appropriate, employee representatives
- Allocation of the necessary resources for its maintenance
- OH&S policies that are compatible with the strategic goals and directions of the organization
- Effective process for identifying hazards, managing OH&S risks and exploiting OH&S opportunities
- Continuous performance evaluation and monitoring of the OH&S system, in order to improve OH&S performance
- Integration of the OH&S system in the business processes of the organization
- OH&S objectives that are in line with OH&S policy and that take into account the organization's risks, OH&S risks and OH&S opportunities
- Compliance with legal requirements and other requirements

3.2. The Structure of the Standard

The ISO 45001 standard is divided into 10 requirements, designed to provide the user with a clear and defined structure and set of requirements that must be met for the OH & S management system. The structure from 1 to 3 provides details of the scope of this standard, normative references, and explanation/terminology that helps to understand this standard, while sections 4 to 10 are composed of the requirements to be met by the organization.

3.3. Risks and Opportunities According to ISO 45001

Organizations need to be more proactive in the process of identifying, assessing, and monitoring health and safety risks and opportunities.

Process risk assessment requirements are still part of the OH&S management system planning. Process risk control is an important part of ensuring the health and safety of people within the organization.

As a pillar of the OH&S management system, assessing the hazards and risks of an organization's activities is still a key part of what is needed to have an occupational health and safety performance.

According to the identified problems, stakeholders and expectations, organizations must assess the risks and opportunities in relation to the occupational safety and health management system. The OH&S management system means risks and opportunities that may affect the company's ability to improve OH&S performance, meet compliance obligations, and achieve the OH&S objectives.

Every company that has implemented an occupational health and safety management system knows that the risk assessment and the management of risk management controls are crucial for occupational health and safety management. Risk assessment and determination of what needs to be done about them has always been part of OH&S and has not changed. The only real change is to include additional focus on the important task of risk assessment and assessing the opportunities that can be used to benefit your company.

4. Determination of the Scope of an OH&S System with View to Business Resilience

Integration of an OH&S System into the Business Process Management System

According to requirement 1, but also the requirement 4.3 of the standard ISO 45001:2018, the organization that has implemented the standard and has set up an occupational health and safety management system, must determine the scope of the system must have appropriate documented information for that. If we consider the overall requirement 4 of the standard – Context of the organization, we can see that this clause is found in all of the ISO management system standards and is required to determine all of the external and internal issues that may be relevant to the achievement of the setup OHS objectives. This requirement of the standard gives

an opportunity to identify all of the internal and external issues that might affect the organization, as well as the strategic direction of the OHS management system. It is also required to identify and specify the needs and the expectations of the workers and the other interested parties that are considered into the management system. The group that the part of the standard is requiring to be specified are the workers, shareholders, regulatory parties, investors, subcontractors, etc.

This important clause of the standard is setting the scene for the organization and the scope and boundaries for the OHS system. When the scope is set up, should be aligned within the strategies of the organization. According to the clause, it has to be determined the internal and external factors that will or might affect the ability of the organization to achieve the desired and intended outcomes of the system. For example, externally might be the issues, such as socio-economic and instability, and internally, might be the issues such as new products, or acquisitions, etc. It is also required to determine the needs and expectations of the interested parties regarding the system of OHS. All of the interested parties should be considered.

However, it is very important to be considered all of the issues against the intended outcomes of the OHS management system. The scope must be documented. It is unacceptable to exclude some part of the business or site of the business according to poor safety and health performance of that particular part. The main purpose of the OHS management system is to prevent injuries, illness of the workers and to provide a healthy and safe workplace for everybody. If a part of a business is excluded, then the credibility of the organization is undermined.

This requires the organization to access the internal and external factors in the process of preparation and implementation of the health and safety management system. Additionally, the economical and completeness factor, it requires to include the laws, the technological development, as well as the outside factors such as political, social, and cultural, might influence the organization’s mission, no matter if its local, regional, national, and international.

The organization needs to understand and estimate the internal and external factors that will impact positively or negatively on the health and safety management performance and includes organizational culture and structure, market competition, technological and financial market, etc. The main purpose of the standard is to identify the relevant mentioned above issues that could affect the OHS management system and those issues further need to be addressed.

By defining the scope of the occupational health and safety management system and understanding the organizational context, the best way to perform is that the organization develops analysis. And by analysis, it means SWOT and PEST analysis. The SWOT analysis includes techniques to identify the strength, weaknesses, opportunities, and threats that the organization has to be perceived as the perfect management health and safety system. Also, another analysis that identifies and mirrors the organization towards the outside world, is the PESTLE analysis. PESTLE analysis includes political, economic, social, technological, legal, and environmental factors that face the organization to have appropriate health and a safe environment for its interested parties.

It is recommended the organization have documented the mentioned above results and periodically have an update to the result of this process. The results can be used to be:

- Set up the scope of the OHS management system
- Determined the risks and opportunities
- Defined OHS policy
- Defined OHS objectives
- Fulfilled the organization compliance within the regulations and laws

The main requirement of the standard is the scope of the OHS Management system to be widened and to include the relevant groups as well as interested parties, including in the management system, that are delivering products/services for the organization. Within the scope of the system must be defined the parts of the workplaces with the plant of the organization and the offices. In a word, should be included all of the locations that the organization has implemented the OHS management system. The organization must include the activities, products, and services that are controlling and that can impact the system performance.

Besides the location, while defining the scope, the organization must define the boundaries and the applicability of its OHS system into the organization. The scope can include but is not mandatory, the whole organization, or specific and identified activities/functions or sectors that function within the organization. Accordingly, the organization must define and make a statement that will confirm based on the requirements of the standards, how is defined the scope of the occupational health and safety management system. This statement is really important, so that the interested parties have a clear picture of the OHS management system and understand the parts of the organization that are covered.

The scope of the OHS management system should include all the activities that are under the control of the organization or the activities that could have an impact on the OHS performance. All of the credibility of the OHS systems depends on the extension of the boundaries. When the organization excludes activity, product, or a service, then the circumstances for this exclusion should be well defined and noted by the organization, because this exclusion could undermine the credibility of the system with the interested parties and could reduce the ability to achieve the defined outcomes and OHS objectives.

The scope represents well-defined statements by the organization management for the organization's business processes that are included within the OHS management system. The scope is a documented information, and this document should be available for all of the interested parties. This document should be maintained and updated whenever there are changes within the OHS management system. It is also recommendable to be published on the company webpage, or some other post of a public statement for its conformity. By defining the scope, should be considered the approach that will define the activities and the processes that are involved, the products/services that will occur, and the location where they ensue.

An OHS management system presents a set of organizational elements that are involved in the continual cycle of planning, implementation, evaluation, and improvements, with the main reason to be reduced the risks that have an impact on the occupational workplace risks. These kinds of elements are the policies, objectives, goals, decisions, procedures, technical resources, communication practices, hazards identified procedures, risk control, organizational learning practices.

5. How to Best Understand the Workers' Needs

Health and safety in the workplace are the number one concern of most businesses, yet still deaths and injuries occur. ISO 45001 sets up to the executives.

Company-wide engagement is one of the key benefits of ISO 45001. The new standard recognizes the value of worker consultation in the development of better OH&S practices and places greater emphasis on employees actively participating in the development, planning, implementation, and continual improvement of the OH&S management system.

Top management must take an active role, promote a positive culture and communicate what needs to be done and, more to the point, why it's important. Senior leaders need to demonstrate that they are actively involved and taking steps to integrate the OH&S management system into the overall business processes. "ISO 45001 means more focus on leadership and worker participation as well as ensuring the system takes into account the 'world' the organization operates in and the internal and external factors affecting it – known as its context," says Richard Jones - Head of Policy and Public Affairs at IOSH. "It means that top management must take a visible, directing role and be actively involved in the system's implementation and ensuring its integration with other business systems."

According to Jones, the system needs to be proportionate to the organization's risk profile and complexity. For example, in smaller organizations, effective worker parti-cipation can be more direct and straightforward to achieve, without the need for formal committee structures and so forth. And there may be additional drivers for improvement, he says. "Client organizations will increasingly require demonstration of good OH&S from those supplying their goods and services so that they can ensure they are compatible with their system."

So, what responsibilities do companies have to protect their employees? Employers have a duty to either reduce exposure or equip employees with preventative skills and tools to minimize risk. In other words: prevention pays. It's not surprising, therefore, that the motto of the XXI World Congress 2017 was "A Global Vision of Prevention".

Prevention is key to tackling the burden of worker safety and is considered to be more effective (and less costly) than treatment and rehabilitation. In line with the World Congress motto, ISO 45001 takes on a risk-based approach to managing OH&S.

Understanding the needs and expectations of workers and other interested parties requires that the organization first and foremost needs to assess the internal and external issues that can impact positively or negatively its health and safety performance including, inter alia, organizational culture and structure, and the external environment including cultural, social, political, legal, financial, technological, economic, market competition and natural factors of significance to its performance.

The organization may also decide to voluntarily agree to, or adopt, other needs and expectations such as subscribing to a voluntary initiative. Once the organization adopts these needs and expectations they are addressed when planning and establishing the OH&S management system.

Employees indubitably constitute the organization's most significant interested party, whose needs and expectations must be identified and addressed. The organization should seek out their views on health and safety concerns regarding work activities, products, or services. It should follow up on inquiries, requests, complaints, or suggestions made by employees to learn more about their expectations. The health and safety committee is an excellent forum for the gathering and evaluation of workers' concerns.

The organizations should take the time to understand the relevant interested parties' needs and expectations and determine the ones that are relevant to the OH&S management system and should be addressed.

But going back to the workers being the most significant party, any conversation on OH&S has to include them in as the minimum standard of practice to protect employees worldwide. Applicable to all organizations, regardless of size, industry, or nature of business, it is designed to be integrated into an organization's existing management processes and follows the same high-level structure as other ISO management system standards, such as ISO 9001 (quality management) and ISO 14001 (environmental management).

Many employers recognize that successfully managing OH&S risk not only prevents injury, ill health, and death, it supports livelihoods, businesses, and communities. And the systems approach used by ISO 45001 can help more organizations achieve this.

But what does that look like in practical terms? For an OH&S to be strong and healthy, everyone in the organization must feel that he or she shares some responsibility for maintaining a safe environment. This includes all employees,

many specifics as possible. Because when an employee is injured, companies lose out on that person's experience and knowledge, as well as their labor of course. Multiply this out over several hundred (or thousand) employees and the costs can become quite severe.

As part of its OH&S, the company engages employees in many ways, including the creation of a proactive safety committee that raises awareness of issues such as ergonomics hazards and an internal blog where employees report safety risks, with improvements made in response to their reports and suggestions.

Imagine dedicating countless years to honing your professional skills and abilities, only to have all that work crumble down like an avalanche. That's what having an injury is like for most workplace accidents.

Significantly reducing the incidence of injuries and occupational diseases is not that simple, however. It can be an arduous task and it will not happen overnight, but progress is certainly feasible. Enthusiasts of ISO 45001 believe organizations that implement the standard will be better positioned to control risks related to OH&S issues, improve their overall safety performance, and provide solid evidence to buyers and consumers of their commitment to health and safety of their employees.

Building OH&S in the current global environment is an opportunity, not a burden. Companies taking it seriously communicate to workers and the community that their time and well-being are valued, and are secured from loss of lives, property, and even their entire business.

6. Analyzing Risks and Opportunities Related to OH&S and Planning of Action

Risk definition is the following: uncertain event, that when it occurs, the result is positive or negative. This concept of the approach to the risk definition is important to be known because often people think that the risk can have a negative effect. Whenever we realize that the risk could have a positive effect, then we can spot the opportunities. According to this, we should be able to use the identified risks and turn them into opportunities.

Uncertainty presents the core of risk management. We never know if the predicted event will happen or not. Accordingly, the consequences when it occurs will be uncertain too. The likelihood, the uncertainty is described as the chance one event will happen, and the consequences are defined as the outcome of that event. Together, these elements will determine the magnitude or the size of the risk.

The risk management process follows a couple of steps, in order to have effective risk management. These are the 5 steps risk management process:

1. Risk identification: The first step is risk identification, which can be realized by the risk-based thinking. Besides the identification of the potential risks, more should be considered, and more actions should be taken about them. When the risk is uncovered, it must be recognized and described the potential effects techniques that are available for risk identification. The best way is for the identified risk to be documented and registered in a risk register.
2. Risk analysis – When the risks are identified, the risks should be analyzed, and needs to be determined the consequences of each risk. The nature of the risk should be understood and how this risk will affect the health and safety objectives and goals. It is recommended this information be noticed in the risk register.
3. Risk evaluation – Risk evaluation is performed by determination of the magnitude of the risk, which represents a combination of the risk happening and the severity of the risk consequences. When the risk magnitude is established, it should be decided if the risk is acceptable or is not. If it's not acceptable, then should be determined the activities that need to be done to mitigate the risk. Also, this step needs to be documented in the risk register.
4. Risk treatment – Risk treatment is known as Risk Response Planning. All of the identified risks should be evaluated, and after it should be created and implemented action plans that will mitigate the risk until they become lower than the acceptable levels. Besides the negative risks, the opportunities should be identified and enhanced as well. As a part of this process presents the preventive plan, mitigation strategies, and contingency plan. It is recommendable to add a risk treatment plan in the risk register.
5. Risk monitoring and review – Once the risks are identified, evaluated, action plans are set up, the risks should be reviewed and monitored for a proper period of time, at least once a year. Even though it is not possible to completely remove the risk, the process of identification and management of all risks needs to prevent unpleasant activities that might happen. This process aims to implement and plan the proper activities in order to exceed the surprises that can come out of the risks.

While maintaining the OHS management system, one of the most important things is that the risk should be managed on a daily level. The following process above will help every organization to apply risk management processes systematically, and the result will come out with a positive result for all the interested parties of the organization.

What actually is risk and opportunity management? By definition, it presents a continuous, proactive process of implementation of action plans, identifying program risks and opportunities. The continuous, proactive process of implementing action plans, identifying program risks and opportunities and final monitor for completion.

The main purpose of actions taken as follow up on risk assessment findings is to boost the effectiveness of the existing OHS management system. This kind of action additionally will help the organizations to fulfil the legal requirements. These effects include the following in order to enable organization to:

- By identification of the risk assessment and meeting the systematic management requirements will be achieved occupation health and safety improvements if the proper measures are adopted
- All of the stakeholders will be engaged in performance improvement of the existence OHS management system
- Ensured working productivity by improved working conditions and to be placed greater emphasis on the workers protection for health and safety

When we mention risk and hazard, they are often used mutually, however there is a difference between these two notions. There are six categories of hazards:

1. Biological hazards – Hazards that include viruses, bacteria, insects, animals, etc., that can cause adverse health impacts. For example, mold, blood and other bodily fluids, harmful plants, sewage, dust, and vermin.
2. Chemical hazards – Hazardous substances that can cause harm. These hazards can result in both health and physical impacts, such as skin irritation, respiratory system irritation, blindness, corrosion, and explosions.
3. Physical hazards – Environmental factors that can harm an employee such as heights, noise, radiation, pressures.
4. Safety hazards - Hazards that create unsafe working conditions. These hazards include exposed wires or damaged carpet that can result in a tripping hazard. These kinds of hazards are sometimes part of the category of physical hazards.
5. Ergonomic – Result of physical factors that can result in musculoskeletal injuries. For example, harm through manual handling.
6. Psychosocial - Hazards that have an adverse effect on employee's mental health. For example, mobbing, workplace violence, stress.

For every risk management, including hazards it is important to protect every employee, to prevent legal penalties, and to have a continuous improvement of the system. It is vital to manage workplace hazards. It is recommendable to be taken the following steps to protect the employees:

- Execute appropriate risk assessment according to the nature of the work and hazards
- Implement appropriate control measures – According to the risk assessment, controls must be executed to reduce and eliminate hazards
- Employee training – According to the legal requirements, as well as the standard requirements it is a must to have proper training to every employee according to the identified dangers and harms for the employee workplace.

When planning to address risks related to COVID-19, the organization should consider existing OH&S risks and measures already in place to manage these. The organization should:

- assess existing OH&S measures and controls that need to be adjusted, considering any changes to work processes.
- consider new OH&S risks (e.g., impact on fire safety arrangements) and other risks (e.g., security risks) that can be introduced by implementing additional safety measures to manage the risks related to COVID-19;
- plan actions to address new risks
- plan for changes and restrictions at short notice, whether at local, regional, national, or international level

7. Operation and Performance Evaluation of an OH&S System

An OHS Management System (OHSMS) is a set of plans, actions, and procedures to systematically manage health and safety in the workplace. The occupational health and safety (OHS) management system encompass more than just your health and safety program. It includes health and safety policies, systems, standards, and records, and involves incorporating your health and safety activities and program into your other business processes.

The most effective OHS systems are developed jointly by management and staff. At the same time, ISO 45001 defines the requirements for an occupational health & safety management system.

What represents an occupational health & safety management system? To understand we need to go to the definition of a management system in general.

And this represents a set of interrelated or interacting elements of an organization, to establish policies and objectives and processes to achieve those objectives.

The policies and objectives can refer to different topics like quality, information security, environment.

The purpose of an occupational health & safety management system is to provide the framework for managing risks and opportunities to prevent work-related injuries and ill-health and to provide safe and healthy workplaces.

If this happens it's considered that the occupational health and safety performance of the company is improving.

The decision to implement a management system, any management system, is an important decision for an organization.

The implementation process depends on a large number of factors like the size of the company, the activities of the company, the culture in the company, and the competence of its people.

But there are some elements considered to be success factors for the effective implementation of a management system, regardless of the specifics of the company.

Among them, the involvement of top management and the support it provides to the management system; the communication processes and how effective they are.

The resources made available to this management system and the integration of this management system into the day-to-day operations of the company and into the normal business processes.

8. Rationale for Engaging in OH&S Systems with View to Business Resilience

The application of the concept to the field of OSH seems to be a natural result of both, research on resilience in various fields, including organizational studies, disaster studies, and psychology, and the fact that research on resilience involves an interest in problems such as safety, danger, stress, adversity, recovery, disturbance, and disaster. The concept of resilience corresponds well to ideas such as the need for proactivity, anticipation, and the need to reformulate the traditional approach to safety because it allows, at some point, a limited increment of safety.

Some approaches to resilience concerning safety and health focus on the psychological and behavioral aspects of resilience and the organization and on the influence of the individual on performance in terms of resilience and on individual resilience itself.

The best known and developed approach to resilience in relation to OSH is most probably resilience engineering, which mainly originated from research on the functioning of complex socio-technical systems.

In addition, are the activities that can be undertaken by the organization that defines the resilience of the organization in terms of the system for health and safety at work:

- Determination of the needs and expectations of stakeholders
- Establishment of an OHS policy - The policy for safety and health at work must be developed by the management of the organization and is required in order for the employees to be met with the mission, vision, and requirements for healthy and safe at work
- Assignment of organizational roles, responsibility, and authority, as appropriate- Responsible persons for the system of safety and health at work are appointed. All work tasks of the workers in the organization are listed in the Rulebook for systematization and organization of workplaces.
- Determining how to meet legal and other requirements - Legal requirements are regularly reviewed and implemented in the organization by management and occupational safety professionals. The employees of the organization should be informed about any change in the legal regulations.
- Establishment of OSH goals and planning their achievement - Occupational safety goals are established at the organizational level and each manager has the authority to meet them.
- Determining applicable controls to ensure outsourcing, procurement, and contractors - All outsourcing processes are controlled and managed. The selection criteria should be defined by the management.

9. References

International Labour Organization: NORMLEX Information System on International Labour Standards - Occupational Safety and Health [online] Available at: https://www.ilo.org/dyn/normlex/en/f?p=1000:12030:0::NO:::#Occupational_safety_and_health [Accessed: 14 June 2021]

International Labour Organization: Guidelines on occupational safety and health management systems, ILO-OSH 2001 [online] Available at: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/WCMS_107727/lang--en/index.htm [Accessed: 14 June 2021]

International Labour Organization: Occupational safety and health in Europe and Central Asia [online] Available at: https://www.ilo.org/global/topics/safety-and-health-at-work/country-profiles/europe/lang--en/index.htm [Accessed: 14 June 2021]

International Labour Organization: Prevention and Mitigation of COVID-19 at Work ACTION CHECKLIST [online] Available at: https://www.ilo.org/global/topics/safety-and-health-at-work/resources-library/publications/WCMS_741813/lang--en/index.htm [Accessed: 14 June 2021]

International Labour Organization: A safe and healthy return to work during the COVID-19 pandemic [online] Available at: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/briefingnote/wcms_745549.pdf [Accessed: 14 June 2021]

International Labour Organization: STOP Covid-19 at work! [online] Available at: https://www.ilo.org/sector/Resources/WCMS_746337/lang--en/index.htm [Accessed: 14 June 2021]

ISO Org News: WHY THE FUTURE BELONGS TO STANDARDS [online] Available at: https://www.iso.org/news/ref2201.html [Accessed: 14 June 2021]

ISO Org: WHY THE WORLD NEEDS ISO 45001 FOR WORKPLACE SAFETY [online] Available at:thttps://www.iso.org/2015/11/Ref2016.html [Accessed: 14 June 2021]

World Health Organization: World Day for Safety and Health at Work [online] Available at: https://www.who.int/occupational_health/mediacentre/pr280405/en/ [Accessed: 14 June 2021]

International Labour Organization: Safety and Health at Work [online] Available at: https://www.ilo.org/global/topics/safety-and-health-at-work/lang--en/index.htm [Accessed: 14 June 2021]

PEGASUS Legal Register: Practical Ways of Demonstrating Top Management Involvement in ISO 45001 for OH&S Management System [online] Available at: https://pegasuslegalregister.com/2018/11/07/management-involvement-iso-45001-ohs-management-system/. [Accessed: 14 June 2021]

PEGASUS Legal Register: ISO 45001 – Clause 5.1 Leadership & Commitment [online] Available at: https://pegasuslegalregister.com/2018/02/20/iso-45001-leadership/ [Accessed 14 June 2021]

PEGASUS Legal Register: ISO 45001 – Clause 6.1.2: Hazard Identification and Assessment of Risks and Opportunities [online] Available at: https://www.pegasuslegalregister.com/2018/04/04/iso-45001-clause-6-1-2-hazard-identification/ [Accessed: 14 June 2021]

ISO Org: ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use [online] Available at: https://www.iso.org/obp/ui/#iso:std:iso:45001:ed-1:v1:en [Accessed: 14 June 2021]

NQA Global Certification Body: ISO 45001:2018 OCCUPATIONAL HEALTH & SAFETY IMPLEMENTATION GUIDE [online] Available at: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-45001-Implementation-Guide.pdf [Accessed: 14 June 2021]

Afnor Group: ISO 45001 OCCUPATIONAL HEALTH AND SAFETY [online] Available at: https://www.afnor.org/en/wp-content/uploads/sites/2/2018/06/AFNOR_Guide_Transition_ISO_45001_EN_loRES.pdf [Accessed: 14 June 2021]

World Health Organization: When is a Risk not a Risk? by Dr David Hillson [online] Available at: https://www.who.int/management/general/risk/WhenRiskNotRisk.pdf [Accessed: 14 June 2021]

Health and Safety Authority: Health and Safety Management System [online] Available at: https://www.hsa.ie/eng/Topics/Managing_Health_and_Safety/Safety_and_Health_Management_Systems/ [Accessed: 14 June 2021]

United States Department of Labour: Guidance on Preparing Workplaces for COVID-19 [online] Available at: https://www.osha.gov/sites/default/files/publications/OSHA3990.pdf [Accessed: 14 June 2021]

Work Safe BC: Occupational health & safety management systems [online] Available at: https://www.worksafebc.com/en/health-safety/create-manage/certificate-recognition/occupational-health-safety-management-systems [Accessed: 14 June 2021]

US National Library of Medicine National Institutes of Health: The concept of resilience in OSH management: a review of approaches [online] Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4867880/ [Accessed: 14 June 2021]

Chapter 6

Innovation Management

ISO 56000

By Liridona Cani

1. Introduction of Innovation

ISO 56000 opens the series of standards explaining how innovation has become critical in today's world as a result of rapid change and the rapid growth in knowledge. A systems approach enables an organization to respond to change and pursue new opportunities by leveraging internal knowledge and collaborating externally with a key aspect of the systems approach, being that the systems themselves are continually improved.

The scope of ISO 56000 application is products, services, processes, and business models and all types of organizations, whether manufacturing, service, government or non-profit organizations.

Innovation is triggered by identifying unmet needs that create business opportunities and innovation is necessary for competitive advantage. In the long term, all of this strengthens survivability. Innovation also leads to radical changes in people's lives. Innovation activities include exploration to gain knowledge and reduce uncertainty and experimentation to test ideas and gain new learning.

Innovation impacts the market by creating new benefits. However, benefits created by one organization can lead to negative impacts on others.

For instance, the rise of Netflix led to the demise of Blockbuster. There are challenges to innovation due to organization structure, risk aversion and resistance to change and a key task of leadership is removal of barriers.

There is a difference between **creativity** and **innovation** and creativity is mainly applied in the early part of the innovation process. Innovation is the term applied to the entire process. The process starts with market or product research finding new opportunities, and creativity leads to new conceptual solutions. Proof of concept is established at the validation step, and after this the requirements in the concept are used to develop the product or service. Subsequent delivery to users completes the innovation process.

For some, a new offering may be seen as an innovation, whereas for others it may be just an improvement. Improvement tends to refer to change in an existing entity, whereas innovation relates to an entity that did not previously exist. Throughout the process, the level of risk an organization adopts depends on what is often called its "ambition level" and depends on the organization's culture. An organization can allow these activities (creativity, new offering, improvements etc.) to occur in an ad-hoc manner, but experience has shown that managing activities with a systems approach ensures alignment with strategy and produces better results. Innovation strategy is likely to change as new knowledge is gained. Finally, using an ISO management system enables integration with other management systems such as ISO 9001:2015.

The benefit of an organization using the ISO 56000 series is to give customers, business partners, funders, or academia the confidence that an organization can consistently deliver innovation.

To illustrate this point, take a simple need. You would like a picture of yourself. Two hundred years ago you would employ an artist. One hundred years ago photographic film provided a cheaper and sometimes quicker solution. Digital photography now enables a picture to be retaken in seconds at zero cost if it does not meet a person's need. Steven Sasson at Kodak created this technology in 1975, and Kodak refused to implement it because of its investment in film manufacturing. Kodak differentiated its existing solution by **being faster on delivery, cheaper on price**, and **more reliable on performance**. Kodak failed to the Innovation. It "chipped away" at the "cost" factors. Someone else implemented the "game changer" that made yesterday's

solution obsolete. We know what this did to Kodak, and if we fail to define our “unmet customer opportunity” and just focus on today’s requirements, our own company will have a similar fate. It can be said that the job of leadership is to identify the driving forces for innovation, assess their impact, and then set direction for the business.

Innovation management is based on a systems approach with interrelated and interacting elements, and regular performance evaluation and improvements of the system.

Companies that are serial innovators have a systems approach to innovation. They continuously generate new ideas and are able to stop those that don’t meet agreed-upon criteria.

They attract the best talent in design and marketing. They also have the ability to stop projects that are cash cows so they can move on. As a result, they attract long-term investors.

These companies develop new offerings ahead of the market. Netflix developed internet movies in 2007 well before the internet had the capability to deliver. IBM moved out of hardware and into software in the 1990s, and Amazon started selling books and now hosts other retailers.

Amazon’s web services generate more revenue than retailing. Companies like Google, Amazon, and Facebook have developed data analysis, simple payment methods, and the infrastructure to support their development. These companies have often moved from products to services. Importantly, they have a strong QMS. At the outset GE *(General Electric),* Nokia, and RIM *(BlackBerry Limited)* were exploratory, fun, tolerant of mistakes, and groundbreakers, but, as they succeeded, they shifted to rejecting important innovations and killing great ideas. **Continual improvement is a constant challenge.**

Social media spreads information at an incredible speed and people learn fast about new ideas.

They can buy new offerings quickly and buy them cheaply online. These new offerings then become obsolete just as fast.

We have to drive improvement in our innovation management system (IMS) as Innovation never stops.

Innovation Versus Continuous Improvement

What is more important to your business and its bottom line, continuous improvement or innovation?

As said previously, a new offering may be seen as an innovation, whereas for others it may be just an improvement. Both continuous improvement and innovation share many similarities. For example, when employed properly, both involve the entire organization, both can improve efficiency and productivity and both provide opportunities to improve quality and increase value to customers. However, there are differences.

Continuous Improvement Explained

Continuous improvement is a commitment to a philosophy and process of consistently looking at ways the organization can get better. And while most commonly associated with processes, it includes its people and its products as well.

Continuous improvement focuses on existing organizational elements and provides opportunities to identify and get rid of waste, reduce defects, improve the quality of your products and services, generate greater customer satisfaction, as well as getting rid of the road blocks and frustrations that kills employee morale.

Innovation Explained

Innovation involves turning a creative idea or a concept into reality. It means doing something new, different or better that results in a positive difference for your organization. It means understanding customer unmet expectations and hearing every customer's voice.

Innovation can come from anywhere. It can arise organically from within the organization, from employees with an idea. Innovation can also come from a systematic approach beginning with analyzing the marketplace or environment, recognizing a need and utilizing a creative process to generate ideas, develop and test, and then launch.

What is the Difference?

The difference means that continuous improvement deals with things that currently exist and consistently strives to make them better. Innovation, on the other hand, takes something that does not exist and translates it into something that does exist. You can continue to refine a candle (continuous improvement), but it will never be a light bulb (if you could; now that would be innovative!)

So, which is the more important to your organization and its bottom line, continuous improvement, or innovation?

Both.

By leveraging a culture of continuous improvement you realize gains in efficiency and productivity that can lead to increased profitability. Being committed to innovation ensures your organization has a process, organic or otherwise, to continually develop and produce products and processes that deliver positive results. The combination of the two pack a real one-two punch and deliver great benefits for your organization's people, products, and processes, and its bottom line.

2. Radical and Incremental Innovation: The Importance of Both Types of Innovation with View to Resilience

A radical or disruptive innovation is an innovation that has a significant impact on a market and on the economic activity of firms in that market. This concept focuses on the impact of innovations as opposed to their novelty. The innovation could, for example, change the structure of the market, create new markets or render existing products obsolete. However, it might not be apparent that an innovation is disruptive until long after it has been introduced, and the cut-off point between incremental and radical innovation might be set at different levels. This makes it difficult to collect data on disruptive innovations within the period reviewed in an innovation survey, typically two years. In Schumpeter's view "radical" innovations create major disruptive changes, whereas "incremental" innovations continuously advance the process of change (Schumpeter, 1942).

Radical innovation is a transformative business model that seeks to completely demolish and replace an existing industry or create a whole new industry. It takes an existing system, design or invention and turns it into something brand new. It may change the parts of the system, the processes of the system or both.

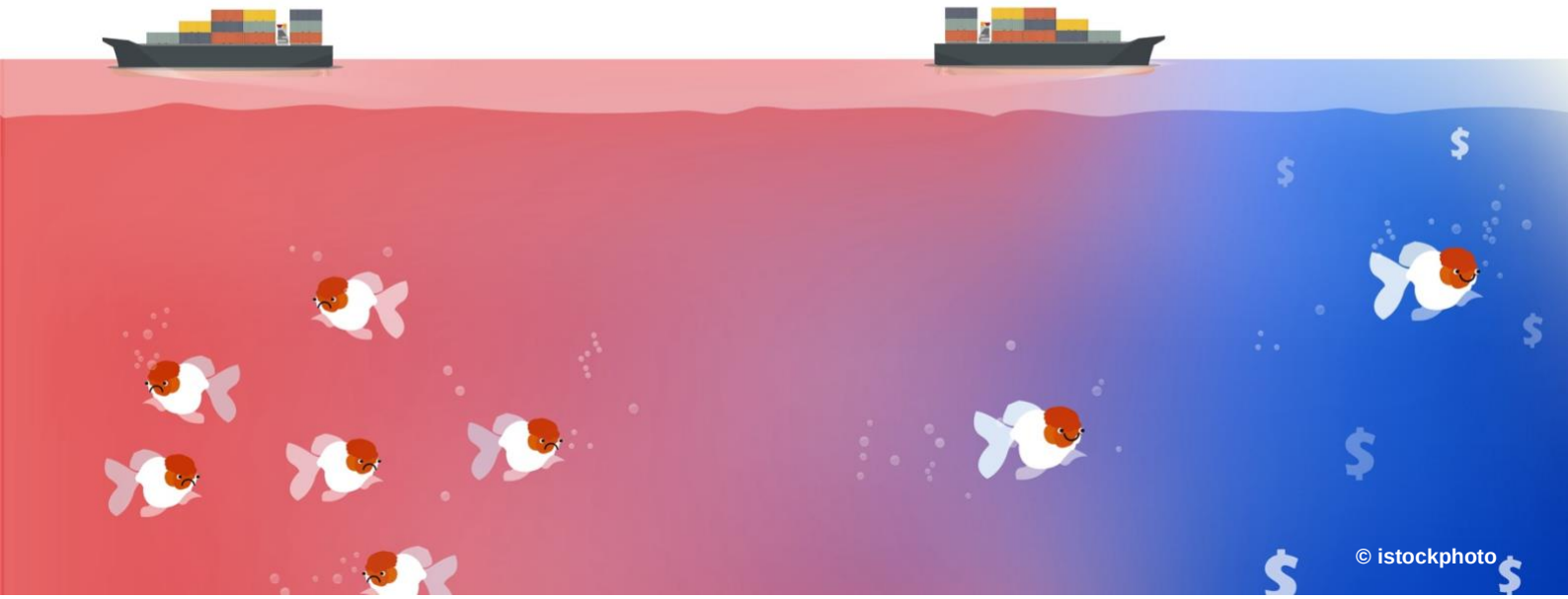
Still wondering, "What is radical innovation?" You can often spot radical innovation examples by the way they affect other businesses. If a new invention or industry is putting others out of business – or destroying an entire industry – that's probably radical innovation. It may sound harsh, but it's the only way progress is made.

As mentioned previously, Netflix is an excellent example of the role radical innovation can play to disrupt an industry. When Netflix entered the home entertainment industry in 1997 (as a mail-order DVD rental service), Blockbuster, an established company and Netflix's main competitor, underestimated Netflix's threat. Instead of clamoring for radically innovative change to counter Netflix's market entry, Blockbuster sat back and did nothing. We know how this story ends: Netflix disrupted the industry, claiming smaller markets' loyalty and putting Blockbuster out of business. Now, Blockbuster is obsolete, and Netflix is a household name.

The iPhone is another example of radically innovative change. Despite the device's worldwide popularity, many do not know how it came about. The iPhone was not new technology – its software and interface were derived from the iPod, an existing Apple technology. It was the iPhone's computer capacity that was the real radical innovation. Rather than add a few new features to an existing phone (i.e. incremental innovation), Apple shifted its concept underpinning the iPhone. By introducing a product equipped to meet users' total communication needs in real time, Apple transformed the digital communications industry. By applying its core competencies

(technology) to a future goal (hand-held computers), Apple achieved a radical innovation whose impact is felt worldwide.

Radical innovation is a complex process, rather than a discrete event, and implies a difficult, lengthy and risky process. We can define it in several ways, but probably will be accurate to describe it as a “blue ocean strategy”.



A blue ocean strategy means that a company does not fight for a slice of the market cake. It rather creates a new market, stepping aside from the crowd. This strategy has many clear advantages:

It gives the chance to get a huge win, as long as the innovator will be the pioneer in the field, with no competitors. A significant advantage for any company.

This advantage could give the chance to own an entire market, at least during the first stages, setting up the rules for the own profit.

New markets are wide open to further development and innovations. Once you have created a new one, the options for further innovations are usually very high. This means that capturing value will be much easier than in mature markets.

Nevertheless, creating a new blue ocean is not easy, in fact, it is quite risky. Timing should be perfect, in order to deliver your brand new product to the right people at the right time. Slow market adoption is a clear possibility, hindering market growth, and the investment needed is usually quite big, without clear return perspectives.

A clear example for this kind of innovation is the digital camera. The history of this device resumes how this kind of approach works. First digital sensors were invented in 1975, and mounted into cameras in 1976 in Japan, by the company Nikon. At first, its adoption was slow and didn´t threaten the traditional industry. As previously mentioned, Kodak itself did not consider digital cameras as a real competitor. As long as digital cameras improved their design and became cheaper, their adoption was growing exponentially, displacing former technologies and all those

companies that failed to adapt, including Kodak. A new huge market followed in a few years, full of devices, products, and services attached to this technology.

Incremental innovation concerns an existing product, service, process, organization or method whose performance has been significantly enhanced or upgraded. This can take two forms: For example, a simple product may be improved (in terms of improved performance or lower cost) through use of higher performance components or materials, or a complex product comprising a number of integrated technical subsystems may be improved by partial changes to one of the subsystems. It involves making small scale improvements to add or sustain value to existing products, services and processes. This can be simple as adding a new feature to an existing product or it can be more complex, for example developing a line extension. One of its key elements is that it harnesses existing technology and an existing business model so it's often easier to execute than breakthrough or radical innovation. I will provide you with one of the best cases of incremental innovation.

A great example comes from Coca-Cola. The brand's line extensions such as Cherry Coke, Coca-Cola Zero Sugar and more recently Coca-Cola Life have enabled a 130 year-old brand to stay relevant, tap into emerging trends and bring something new to its customers over the years.

When setting up an innovation strategy, there are many decisions to take. And, probably, one of the first challenges is to choose between two different approaches.

Should I choose an incremental innovation path? Or should I rather look for a radical, or disruptive, approach? Both choices have advantages and disadvantages and serve different goals.

Incremental Innovation

This is a common approach in many established companies, which focus on creating new products and services, with several goals:

- To grow sales and profits for existing products and services.
- To protect current business models.
- To create new business models without cannibalizing current ones.

This approach is very popular because it reduces the risk that radical innovation usually takes. Moreover, companies with great human capital, resources, and capital find that is much easy for them to follow this innovation path, which brings clear advantages, such as:

- Helps companies remain competitive. While profiting from a product they are already developing the next generation.
- Ideas are easier to sell. When customers are used to a type of product or service they find easier to understand and buy new improvements.
- Affordability. The development process is not unsurmountable, as long as the company already has all the capital and infrastructure needed to keep innovating on the same kind of products and services.

The smartphone industry is a great example of this kind of innovation. Previously, we spoke about the radical change that was made by Apple. When the first iPhone was designed, it helped to create a new huge market. Following this track, many companies developed their own first smartphones, willing to get some slices of the cake. From this first move, all tech companies in this sector started a race to deliver the next generation of their models, profiting in the meanwhile from previous ones. Once they have the resources to do that, is just about keep the wheel turning on, just improving step by step. This makes companies relevant to the customers, reducing uncertainty and keeping costs under control. At least, until someone else disrupt the market again!

Of course, this comes with some disadvantages. In mature markets, with many competitors, is much harder getting notice. Huge marketing expenses became mandatory, as well as the R&D resources to remain competitive. Is not an easy race, and Nokia gives us an example of a big player that clearly lost its market position as result of a failing innovation strategy.

3. What is the Most Suitable Approach for Your Firm?

Today incremental innovation is the most prominent approach for many companies since it suits better with their resources and strategies. Is far easier to introduce new improvements in your products to keep being competitive, rather than trying to create a whole new market with some brand new thing.

For new companies or market entrants it is far more interesting to choose radical innovation, rather than incremental, since it opens wide opportunities that mature markets simply do not have. Nevertheless, they are not opposed approaches. In fact, smart-phones and digital cameras show how they depend on each other. The first iPhone and the first Nikon camera created a blue ocean of opportunities, but after that the market grew and matured because companies chosen incremental innovation, improving their products step by step, following users' needs.

Therefore, we can choose which path should we follow depending on our goals. If we want to become better competitors and increase our market share and profits, incremental innovation with its steady rhythm should be our choice. But bears the risk that a (new) competitor arises with a radical innovation that we did not foresee. Opposite to that, if we want to dive ourselves in new,

unrivaled and undiscovered new markets, probably we should choose radical innovation, developing a new technology and bringing it to the market (if we want to take the risk). Anyway, we must be aware of the consequences and prepare ourselves to face the challenges attached to both kind of innovation strategies

4. Learning in Organizations

Learning in an organization is a crucial point in the success of the company. Different organizations chose different types of learning or a combined learning in the organization. Learning in the organization is closely related to the culture of the organization that will be elaborated on in the following subchapters.

4.1. Formal and Informal Learning in Organisations

Every learning and development team has one ultimate goal. They want to ensure that every member of the organization is given every opportunity available to train.

There are two types of learning, formal and informal learning. Both of them have their advantages and can be easily combined with each other in the same organisation even though they are quite the opposite to each other.

In order to decide which is the best for the organization is to check the needs and the gaps of the staff members.

Formal learning is learning that is delivered “in a systematic intentional way”. It’s planned and guided by an instructor and it usually occurs in a face-to-face setting or through an online learning platform.

In a work environment, think of formal training in the context of compliance training or new hire onboarding. These are training types that need structure, have deadlines, and there’s a definitive goal. In

Informal learning is on the other end of the spectrum. It’s unstructured, often unintended, and it occurs outside of a conventional learning setting. Importantly, it’s self-directed, and has no real objectives, rather it just happens naturally.

Within your business, it can happen whenever and wherever. For example, you could be chatting with a co-worker and they mention that they found a more efficient way to automate a manual process that you can use too. Although it wasn’t deliberate, you’ve still learned something. See also section about learning organisation. Organising or participating in different events that are connected with your organization field helps people to network and share their experience. Informal learning costs less but it is quite productive.

4.2. Establishment of a Culture Allowing to Learn

An old saying, “Culture eats strategy for breakfast,” is attributed to Peter Drucker. However, culture must align with strategy. Culture achieves goals through group behaviors, whereas strategy makes goals logical through plans and options that will narrow over time. Culture often has unwritten rules, is based on shared behavior and develops over time as a result of how people

in an organization respond to events. Leaders take the initiative in these events and so are primarily responsible for the way people respond; Hence, their behaviors greatly influence the organizational culture.

Leaders have a vital role in creating this culture. Leaders establish a culture by their own behavior. They must demand challenges for their own ideas. In Eisenhower's battle plan to invade Normandy, unlike normal military practice, he insisted on criticism from his generals.

At the same time, middle managers are often overlooked but have a critical role. They spend the most time with the people and have huge influence. Philip Crosby recognized this when he developed quality culture change through the quality education system (QES). He had the supervisors train as instructors and made the material easy to teach.

The actions needed to develop this culture are first that leaders show a commitment to innovation. This has a familiar sound from the early days of quality management. This is not just about providing resources but also being directly involved. Others will follow the way leaders behave. If leaders don't take risks, others don't take risks. The leader has a key role in ensuring the change from creative culture to execution culture during an innovation initiative.

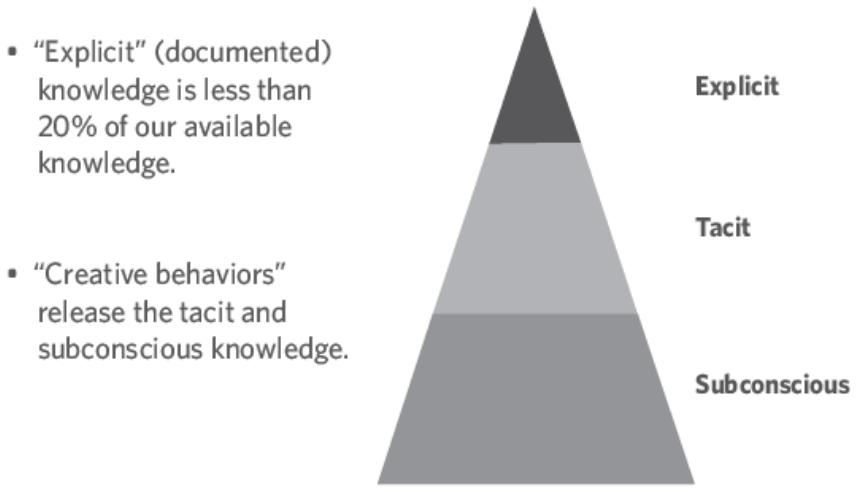
"Top management should demonstrate leadership by promoting perseverance and timely deployment of innovations.

Creativity

Creativity is the ability to produce new ideas through imagination and unconventional approaches to problems.

Creativity occurs when people have the freedom to think and interact with new stimuli, and it is the vital initiator of the innovation process.

Knowledge is the fuel of innovation. A creative culture embraces behaviors that will release knowledge that we do not realize we have. It will also create new knowledge. Back in the 1990s, people mistakenly thought it was possible to document all the knowledge in an organization. This led to the nightmare of over-documentation at that time. In the late 1990s, as the discipline of knowledge management emerged, it became recognized that typically only 20% of an organization's knowledge can be documented and that the vast majority of knowledge is the tacit and subconscious knowledge in people's minds

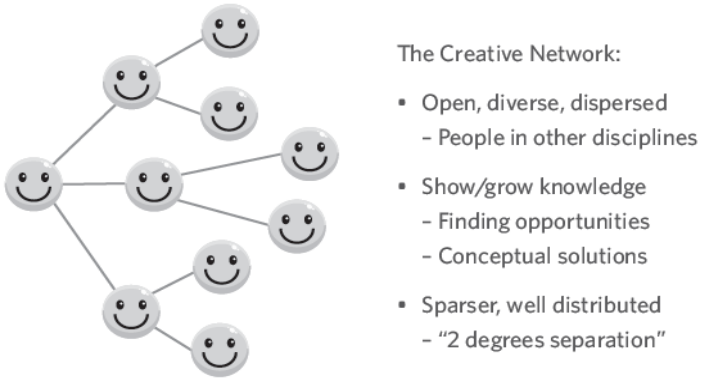


An innovative culture releases knowledge (ISO 56000 : building an innovation management system : bring creativity and curiosity to your QMS https://questmgt.com/iso56000-book © 2020 by Peter Merrill)

The initial creative phase of the innovation process uncovers undocumented knowledge. If you combine the tacit and subconscious knowledge of a group of people, you have a powerful combination.

Creative Behaviors

A culture of creativity allows time and space for people to explore, collaborate, and experiment. It needs an open network and a loose process for new ideas to emerge. It requires a "user focus," which does not mean finding the customer's requirements but finding their unmet needs. Knowledge will increase, and the direction of an initiative will change as this new knowledge emerges.



Open networks—creative behavior (ISO 56000 : building an innovation management system : bring creativity and curiosity to your QMS https://questmgt.com/iso56000-book © 2020 by Peter Merrill).

The behaviors that will release and develop knowledge are first exploration, and second, interaction with new people and having new experiences. You may have heard the expression, "step out of the box."

Today, we work in a box, have lunch in a box, and so think in a box. People want to be released from this mental prison. Giving people time and space initiates a creative culture. It is this "release from prison" that makes it so easy to engage people in creative thinking. The third creative behavior is experimentation. Willingness to take risks and experiment was suppressed in the 1990s and post-2000. A willingness to try things out and not be afraid to fail is a major source of new learning.

Learning from Failure

Perhaps one of the best stories celebrating learning from failure is WD-40. When Norman Larsen finally found his solution to dispelling dampness from spark plugs back in 1953, he recognized the learning from 39 previous failures by naming his product WD (water displacement) number 40. Google encourages risk taking and learning from failure, but its culture has a focus on high levels of competence. High competence means that when failure occurs, it is a consequence of uncertainty, and we challenge the process and not the person. Productive failures yield valuable

information, and we celebrate learning not failure. However, tolerance of failure can encourage loose thinking. Striking a balance is hard because the causes of failure are not always clear. It's worth noting that generally, smaller companies and new industries have a higher learning focus than large organizations.

Leadership must manage this behavior change from creativity to execution with regular monthly or quarterly reviews to ensure initiatives stay on track while focusing on the finish line.

It is also worth noting that people have natural aptitudes to fit in either the creative phase of innovation or the execution phase

Diversity

Diversity is a vital attribute for finding creative solutions and interacting with people who are different than we are is not easy. People are drawn to a culture with their own characteristics. The "mirror effect" draws us to people of similar background and experience. Diversity creates tension, and respect for different views becomes essential. Collaborating with people who are different is vital, so we must discover and respect their strengths. As Stephen Covey said in 7 *Habits of Highly Effective People,* "Seek to understand before you seek to be understood." Diversity is a vital component for an innovation culture, and the greater tensions in diverse groups help create new knowledge. The research by Scott Page at Caltech12 showed how a group of ordinary but diverse people had far greater collective knowledge than a group of Mensa level people. The ordinary guys consistently outperformed the folks with the high IQ at problem solving.

Execution Behavior

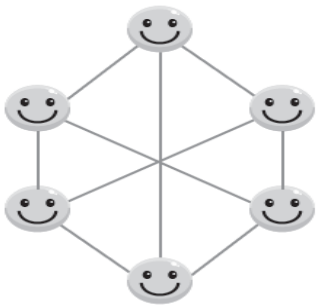
The transition between the two types of behavior involves selecting preferred solutions from those identified in the creative phase and narrowing the focus. We switch from open to closed networking and start to move with speed and a high degree of discipline. In the execution phase of innovation, we need a tight team and good project management. As Thomas Edison said, "Genius is 1% inspiration and 99% perspiration."

The mission becomes "make the solution user friendly and deliver the solution." This requires a strong work ethic. The danger is that the project team reverts to that very enjoyable creative behavior and starts adding bells and whistles, which make the solution complex and hard to use.

I recently bought a new car. Many of the functions are so complex I don't have the time to work out how to use them. Designers of technology often assume users have nothing else to do except learn how to use their new offering.

The Execution Network:

- Closed network
- High level of trust and collaboration
- Forms more easily
- Gravitate to similar people
  - Reinforce existing beliefs
  - Mirror other thoughts



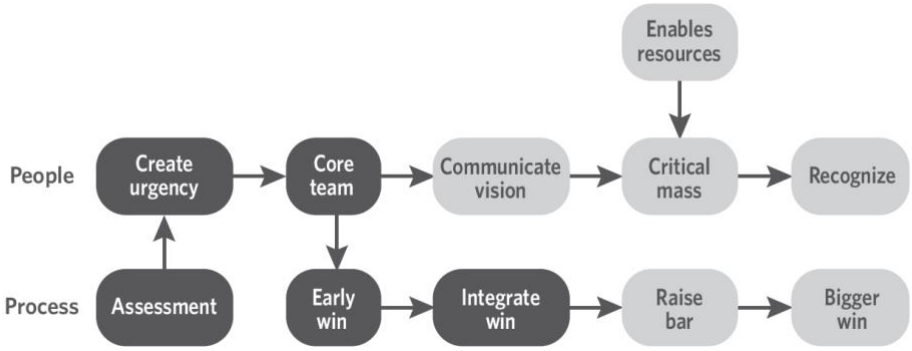
Closed networks—execution behavior (Scott Page, *The Difference: How the Power of Diversity Creates Better Groups, Firms,Schools and Societies* (Princeton, NJ: Princeton University Press, 2007- Ref ISO 56000 : building an innovation management system © 2020 by Peter Merrill).

Culture Change

Everyone is for innovation, but nobody wants to change. Cultural change is difficult, and innovative cultures can be confusing. Some behaviors are easily accepted, and people love the freedom. However, they see execution discipline as restrictive. Consensus removes accountability, but accountability is necessary. The various behaviors are all interlinked and cannot be developed one at a time. There are no shortcuts to this culture.

So How Do We Begin this Change of Behavior and Culture?

There are a few issues that will create resistance to a change to an innovative culture. You see these from the new behaviors described and also from looking at your existing culture. Resistance will be especially strong if you have a history of success. You will need to create a sense that the change is necessary. The process for handling change can follow the approach in this model. Business leaders play a key role in all of this. The essential steps for change are shown below:



Change to an innovative culture (John P. Kotter, “Leading Change,” Harvard Business Review (November 2012). Ref ISO 56000 : building an innovation management system © 2020 by Peter Merrill)

Culture assessment: This is necessary before considering change. There are assessment tools for this.

Create a sense of urgency: Identify a falling revenue item or market share with a key product, service, or customer. Pick a significant item to work on or a high-profile customer and develop a sense of crisis and a desire for action. This is Kotter’s “burning platform.”

The core team: A change agent team must include people outside management and must be designed carefully. Their mission is to quickly create a critical mass of believers in the organization and do this by replacing a dying product. The new product will be the first visible evidence of developing an innovative culture.

Early win: The “low-hanging fruit” is captured. This is a product, service, or customer opportunity with high benefit. Wins must be created and not just based on hope. The win must produce a quick result and then be published.

Integrate win: This is systems thinking. Unless the early change in culture is integrated and protected, it will not survive. Until innovation becomes business as usual, innovations must be explained, and the participants must be recognized.

Communicate vision: The change team must draw in the people by focusing on the important aspects from the early win. These successes must be easily communicated in concise and simple wording. The team must keep repeating the successes. A “one-minute message” should be developed. Communicating the vision becomes a key task for the business leader.

Enable action: People must be given the authority and time to innovate. Leaders must find the obstacles and remove them.

Critical mass: The short-term win creates danger as people relax. The outcome must be monitored, and negative side effects must be dealt with. Generally, you should aim for real momentum within a year and expect two years for real culture change.

Raise the bar: Significant culture change must be ensured before moving on to bigger issues.

Recognize success: The behaviors described earlier are endorsed. Building trust reinforces new behaviors when they are based on the new values. Recognition and reward are aligned. Rewards must be structured to support innovation.

The aforementioned model and the description give you an outline of the change process; the business leader plays a key role in all of this. An excellent way of driving this change is by linking it with the planning of an initiative, Innovation Initiatives.

You must recognize new behaviors, not results. Endorse the behaviors already described. Reinforcing new behaviors builds trust, especially when they are based on the new values that they imply. Philip Crosby, said, “Appreciate those who participate.” Recognition of innovative behaviors will encourage behavior change, and incentives should align with the recognition of behaviors.

One more consideration when going through change is that performance management encourages values and behaviors, and people’s engagement in change should be recognized during their review.

Training and mentoring will also become essential for the development of these new behaviors Competence (clause 7.2). Culture change also means being careful about recruitment, so know what type of people you want (see clause 7.1.2 Resources).

4.3. Learning Organisations

The leadership recognizes the importance of providing the motive, means, and opportunity for learning: (i) the motive being the “why?”—the purpose and reason for learning; (ii) the means being the “how and what?”—the models, methods, and competencies required; and (iii) the opportunity being the “where and when?”—the spaces for learning. Leaders take an exemplary leading role in creating and sustaining a supportive learning culture.

The structure of a learning organization takes into account the common obstacles to learning so it is carefully aligned with strategy, avoiding the development of “silos” and minimizing unnecessary levels of hierarchy.

Communication systems are used to facilitate the lateral transfer of information and knowledge across formal structural boundaries. In decentralized and geographically spread organizations,

particular care is taken to use communication to encourage lateral communication and to overcome the increased danger of the development of “silos”.

Adequate resources are allocated for learning in terms of time, space, specialist support staff, and budgets for knowledge management and learning infrastructure, formal and informal communities of practice and other value networks (both internal and external) and learning and development programs. Support to communities of practice, for example, is extended in a structured manner throughout their life cycle.

To stimulate creativity and generate new insights and innovative practices, a learning organization takes a balanced approach to the importance of both planned and emergent learning. Planned learning is addressed through the careful development of strategy, structure, systems, procedures, and plans. In a learning organization, planning is based on careful reflection through probing questions that draw on data and information from monitoring, review, and self- and independent evaluation.

Emergent learning is equally important but takes an inherently more speculative and opportunistic approach. It is dependent on encouraging a passion for learning and knowledge sharing among staff members, developing learning competencies, creating opportunities for informal sharing, and cultivating a supportive learning culture.

Failures and unintended outcomes are the focus of constructive discussions leading to new approaches. When such incidents involve clients, care is taken to protect their reputation.

5. Precondition of Innovation – Organisational Preconditions, Leadership Aspects

Leadership is not just a title; it is an attribute and an activity. This attribute, “the leadership of innovation,” has to be encouraged throughout the organization. The leadership principle in ISO 56000 states: “Leaders at all levels, driven by curiosity and courage, challenge the status quo by building an inspiring vision and purpose, and by continuously engaging people to achieve those aims.”

Leaders who are curious gain more respect. Henry Ford was curious and looking for a solution for mass production. He found his solution when he was touring a meat factory. He saw meat being transported between workstations by hanging it on hooks. For decades after that, car components were moved between workstations by hanging them on hooks. Discoveries come from curiosity. When Ford stopped being curious, General Motors took away his business.

Curiosity increases creativity. The Model T in 1908 captured the majority of the U.S. car market. However, curiosity declines over time, and work pressure reduces the opportunity to be curious. By the 1920s, people wanted variety. Ford stopped innovating and famously said, “You can have any color as long as it’s black.” General Motors captured the market. It’s hard to keep being curious when you are being successful. Success breeds complacency. Many leaders stifle curiosity, as they fear inefficiency. Another essential component of this principle is the role of leaders in engaging people. This is one of the leader’s most important jobs. Joe Robles, the CEO of USAA Insurance, had the organization’s people immerse themselves in a four-day cultural orientation. Gerry Anderson of DTE Energy had videos developed of each person’s job and explained the impact on the community of their work in the energy sector. These videos were built into onboarding and training (Robert E. Quinn and Anjan V. Thakor, “Creating a Purpose-Driven Organization,”Harvard Business Review (July 2018): 78. Ref: ISO 56000 : building an innovation

management system : bring creativity and curiosity to your QMS https://questmgt.com/iso56000-book © 2020 by Peter Merrill).

The Standard: General (Clause 5.1.1) clause provides a very detailed checklist of the leader's job. The clause opens by listing: *the actions for leadership to demonstrate commitment.*

The clause numbers shown in parentheses after the italicized text show where more explanation is provided in other clauses.

Commitment is Demonstrated by:

Establishing innovation vision, strategy, policy, and objectives (clause 5.1.3, Vision, clause 5.1.4, Strategy, clause 5.2, Policy, and clause 6.2, Objectives)

A primary difference from ISO 9001 is the need for leaders to address vision and strategy, which are not contained in ISO 9001. Leaders may not necessarily have direct participation in the creative phase, but they should ensure strategy flows and will certainly be involved directly in the execution phase. In the creative phase, even if they don't feel especially creative, leaders should observe, learn, and understand.

Developing an Innovation Culture (Clause 4.4.2, Culture)

Leaders must take ownership of the culture, as previously described. A difficult task for leaders is managing the coexistence of the values, beliefs, and behaviors. This takes time, and they will especially need to ensure the change in behavior moving from the creative to execution stages of an initiative. Leaders' behaviors set the culture. Good leaders understand the different behaviors in the organization, but many struggle with this and give the job to HR.

Integrating any IMS Requirements into the Business

One of the most important messages is that the management system should be "built in" and not be a "bolt on" entity. Historically, this has been a major problem for ISO 9001 and is a legacy from the 1990s when it was a quality assurance standard. Now that ISO management systems start with strategy development, integration with the business is much easier.

Ensuring IMS Resources are Available (Clause 7.1, Resources)

Leaders will also have a very specific task in ensuring resources for the development of the IMS,

Creating Awareness and Engaging People (Clause 7.3, Awareness, Clause 7.4, Communication)

Engagement of people is addressed very lightly in ISO 9001, and given that successful innovation comes from collective knowledge, leaders must ensure the right people are engaged in an initiative at each of its stages. This may involve change in the team content as the initiative progresses. The execution phase of innovation will demand speed to market. After the creative work, we may take some creative people out of an initiative and add the operations and salespeople, who will understand the practical aspects of implementing a solution. People have different aptitudes.

6. Standards in the Field of Innovation Management (ISO 56000 Series of Standards)

ISO 56000 opens the series of standards explaining how innovation has become critical in today's world as a result of rapid change and the rapid growth in knowledge. A systems approach enables an organization to respond to change and pursue new opportunities by leveraging internal knowledge and collaborating externally with a key aspect of the systems approach, being that the systems themselves are continually improved. Then, as with all ISO standards, ISO 56000 opens with three introductory parts. The scope of ISO 56000 application is products, services, processes, and business models and all types of organizations, whether manufacturing, service, government, or not-for-profit.

The principles are the foundation of the IMS and serve as a transition between the fundamental concepts in ISO 56000 and the system described in ISO 56002. With each of the principles, ISO 56000 provides benefits that come from that principle and actions that can be taken to embed the principle.

The principles are:

1. Realization of value
2. Future-focused leaders
3. Strategic direction
4. Culture
5. Exploiting insights
6. Managing uncertainty
7. Adaptability
8. Systems approach

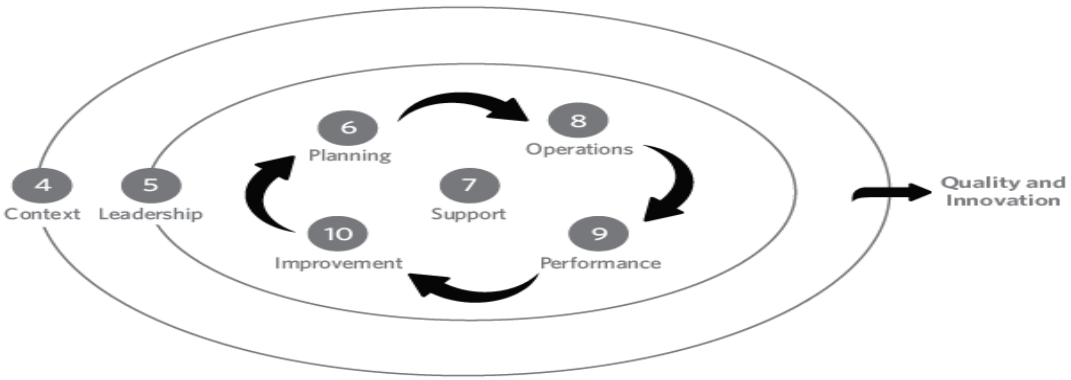
ISO 56000 series of standards on innovation management. The primary focus of ISO 56002 is how to use this innovation management system guidance standard. This standard shows how to initiate and how to execute innovation, and it shows how a systems approach to innovation is without a doubt the best approach. It also shows that if you have a quality management system that is based on ISO 9001, you can develop it into an innovation management system (IMS). ISO 56002 has been designed to integrate with ISO 9001 and has been developed through consensus of technical committees from nearly 40 countries. An auditable requirements version of this standard will be ISO 56001, and you can use ISO 56002 to develop your IMS ahead of that standard being written. You can start with strategy, as the standard does, or you can start with process, if you want to begin with a "contained" approach. ISO 56002 gives major guidance on culture and the key issues to look out for as you develop your IMS.

The number ISO 56001 an auditable version of this standard. There are additional supporting standards in the series, such as ISO 56003, Partnering; ISO 56005, Intellectual property; ISO 56006, Strategic intelligence; ISO 56007, Idea management; and ISO 56008, Measurement. TR 56004 is a technical report on assessment

7. Integrations of Innovation Management Systems into the Business Process Management System

In order to set the basis for a model that has innovation as a part of an integrated management system we need to identify the similarities and the parts where innovation can be introduced in an existing model of integrated management system

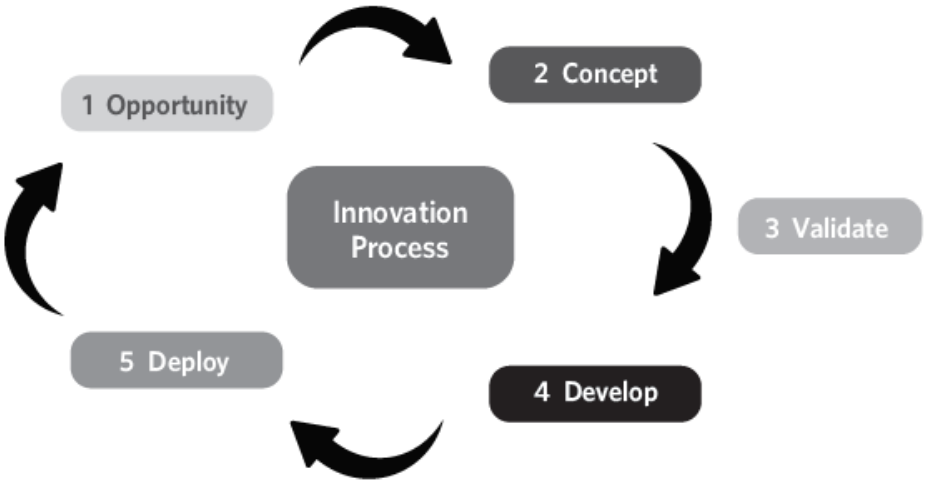
ISO 9001 in 2015, and the new ISO 56002 on innovation management is written with this same structure. ISO 56002 is preparing you for ISO 56001, which will be the requirements standard. Figure 1 is the essential framework of an ISO management system. This common, high-level structure (HLS) enables integration of different ISO management systems. With an integrated system, you can deliver both quality and innovation. Parts 1, 2, and 3 of every ISO standard are introductory. Part 4 is where we “observe” and identify the issues that affect the business internally and externally. Think of PLAN- DO-CHECK-ACTPDCA Good innovators are good observers, and the job of leadership in Part 5 is to link the issues identified to the setting of business objectives through risk analysis in Part 6, Planning.



The ISO management system (Framework of an ISO management system).

At the heart of the system is the PDCA cycle. Part 6, Planning, is where objectives are set for addressing the key business issues. Part 8 is the “do” where we carry out our business operations. We “check” performance in Part 9 and act on any shortfall in Part 10. At the heart of the PDCA is Part 7, Support, which provides the enablers such as people’s competence, infrastructure, communications, and information management.

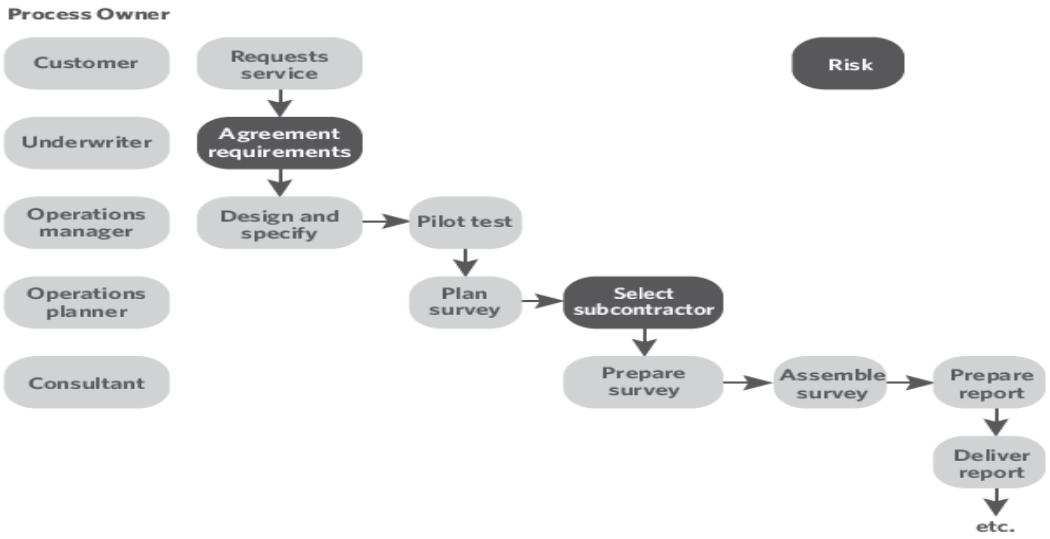
As it can be seen there are some common principles like leadership who is a common principle to the success of both innovation and quality. Developing an innovative culture in SMEs is a source of competitive advantages, leading to customer satisfaction and increasing the organization's focus on the customer. This is an obvious signal that the systematic management approach is essential for innovation. Also, acceptance of new technologies is an essential part of innovation.



Innovation process (ISO 56000 : building an innovation management system : bring creativity and curiosity to your QMS https://questmgt.com/iso56000-book © 2020 by Peter Merrill)

Process mapping is a great tool this and is a good way to determine boundaries.

Key lessons are: keep the map simple and use the “swim lane” method to show responsibilities. Figure below shows a map for an insurance company:



Swim lane process map (ISO 56000 : building an innovation management system : bring creativity and curiosity to your QMS https://questmgt.com/iso56000-book © 2020 by Peter Merrill)

8. Innovation Assessment

Many companies struggle to innovate their products and services to better fit their customers’ needs and desires. Luckily, there are resources out there that can help you analyze how well your company is performing and what areas you need to improve. The assessment helps organizations understand the ways in which they need to innovate. It also discusses what approaches work best for them based on their behavior and company culture.

9. Rationale for Engaging in Innovation Management Systems with View to Business Resilience

A complex, turbulent, and uncertain business environment creates a need for resilience, which could be beneficial to organizational innovation. The case study of Richtnér and Södergren (2008) shows that resilience enabled by four pre-conditional resources, that is, structural, cognitive, relational, and emotional resources, which are particularly important in innovation projects. Richtnér and Löfsten (2014) suggest that a resilient organization is also a creative organization, for organizational resilience is positively related to organizational creativity. Akgün and Keskin (2014) empirically test the impact of organizational resilience on firm product innovativeness and performance, and find that resilience is positively related to firm product innovativeness. Also, managing innovation could improve the organizational capacity for resilience. Resilience means a sustained superior performance, that is, resilient companies can always maintain a high performance and can self-renew over time through innovation. Reinmoeller and van Baardwijk (2005) indicate that the most resilient companies are those that continually orchestrate a dynamic balance of four innovation strategies, that is, knowledge management, exploration, cooperation, and entrepreneurship. Business models are structural templates of how firms run and develop their business on holistic and system-levels, which include three main dimensions, namely, value creation, value proposition, and value capture. Business model innovation requires these three dimensions to be adjusted in order to adapt to the changing environment. Therefore, business model innovation can improve organizational long-term resilience (Carayannis, E.G.; Grigoroudis, E.; Sindakis, S.; Walter, C. Business model innovation as antecedent ofsustainable enterprise excellence and resilience. J. Knowl. Econ. 2014, 5, 440–463). Business model innovation signifies a pronounced readiness for adaptation, and can be viewed as being corresponding to the adaptability pole of the resilience continuum (Yang, H.; Demirkan, I. The performance consequences of ambidexterity in strategic alliance formations: Empirical investigation and computational theorizing. Manag. Sci. 2007, 53, 1645–1658).

10. References

Peter Merril (2020), ISO 56000 : Building an innovation management system : bring creativity and curiosity to your QMS, the United States of America, American Society for Quality, Quality Press.

Nemet, G. F. (2009), “Demand pull, technology push, and government-led incentives for non-incremental technical change”, Research Policy, Vol. 38/5, pp. 700–709.

OECD (2012), OECD Science, Technology and Industry Outlook 2012, OECD Publishing. doi: 10.1787/sti_outlook-2012-en

OECD (2010), “Fostering innovation: The policy challenge”, in The OECD Innovation Strategy: Getting a Head Start on Tomorrow, OECD Publishing. doi: 10.1787/9789264083479-en

OECD (2009), “Policies for Demand-led Innovation: Interim Report”, internal working document.

OECD/Eurostat (2005), The Measurement of Scientific and Technological Activities—Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd ed., OECD Publishing. doi: 10.1787/9789264013100-en

Puga, D. and D. Trefler (2010), “Wake up and smell the ginseng: International trade and the rise of incremental innovation in low-wage countries”, Journal of Development Economics, Vol. 91/1, January 2010, pp. 64–76. http://dx.doi.org/10.1016/j.jdeveco.2009.01.011

Schumpeter J. (1942), “Capitalism, Socialism, and Democracy”, Harper, New York

Smith, K. (2009), “Climate change and radical energy innovation: The policy issues”, TIK Working Papers on Innovation Studies No. 20090101, University of Oslo, Centre for Technology, Innovation and Culture, Oslo.

Von Tunzelmann, N. and V. Acha (2005), “Innovation in “low tech’ industries”, Chapter 15 in J. Fagerberg, D. Mowery and R.R. Nelson (eds), The Oxford Handbook of Innovation, Oxford University Press, Oxford, UK.

https://www.tonyrobbins.com/business/radical-innovation/

Chapter 7
Developing Modern Leadership Skills

By Antigona Limani

1. Recent Developments in Leadership Practises

The role of leaders is particularly important during times of uncertainty and crisis because people look to authority figures to provide direction. Leaders must not only provide this direction but do so in an empathetic manner that clearly demonstrates an understanding of the challenges whilst also projecting confidence about recovering from the crisis. (Leadership Development - Kotter, 2021)

In the 2021 business climate, organizations are facing a more complex and competitive environment than ever before. As a result, the competencies of the leader who thrives in the modern-day business world is changing as well.

There have been changes in the leadership developments before and after the crisis, and the following trends are seen to be happening in the changes in leadership and management. (Harris, 2021)

Flattening Organization Structures

The days of the who knows everything and micromanage his or her direct reports will be a thing of the past. Organizations are moving towards flatter structures and they will need leaders who can thrive in a collaborative and cross-functional environment. This helps communication between employees, increased morale, less bureaucracy, and the ability to make decisions and changes faster. Typically, employees' responsibility levels tend to be much higher in flatter organizations, thus improving job satisfaction, engagement and reducing the need for excess levels of management.

Increasing Need to Develop Self & Others

To keep on top of the rapidly changing technological environment, leaders can no longer sit back and say “I know everything I need to know” as what they do know today will be outdated tomorrow. There is now a greater need to develop their self and their teams.

When comparing the job culture to that of 10 years ago, there is less loyalty amongst employees to their employers, meaning employers need to do everything they can to keep the employees in the company as long as possible to improve staff turnover. A popular method is through offering additional development and training alongside the role.

Approaching the “Talent Cliff”

Firms must prepare as the largest workforce in history moves into retirement. Mentoring, coaching, and job shadowing are examples of how organizations can manage the transition of the millennial leader.

Many companies that are closer to this talent cliff are enrolling younger generations in apprenticeship programmes, to allow those interested in the industry to gain hands on experience, and for companies to be able to increase their workforce in a way that inexpensively gives back to the community, but also positively impacts the business.

Striving for Gender Balance and Diversity

Strong women's representation in leadership teams has been proven to bring organizations better results. A successful leadership development program thus needs to tap into an often underutilized resource - its female managers.

Achieving gender equality is important for workplaces not only because it is 'fair' and 'the right thing to do,' but because it is also directly linked to a country's overall economic performance and therefore growth.

Workplace gender equality is associated with:

- Improved national productivity and economic growth
- Increased organizational performance
- Enhanced ability of companies to attract talent and retain employees
- Enhanced organizational reputation.

Many workplaces are actively striving to reach equality but also complete diversity amongst their workforce, a movement pushed forward largely by generation Z and millennials.

Shifting Focus to Development on Soft Skills

As the role of a leader migrates towards managing teams of diverse members who have different technical skills and areas of expertise, there will be greater emphasis on the need for leaders to develop their "soft skills".

Whilst the focus in the past has been on 'hard skills' These types of skills include emotional intelligence, creativity, adaptability and time management. Employees can be taught "hard skills" such as the specific skills needed to carry out their role, however soft skills are learnt over time, and an employee failing in areas like time management could be detrimental to the business. The development of the soft skills results in an increase of leadership potential, satisfaction in the workplace, and work performance.

Adopting a Blended Approach to Leadership and Management Development

Leadership and management learning journeys will also need to evolve and use a wide variety of modalities to prepare the modern leader with the skills they need to thrive.

Using a blended approach to leadership development allows leaders to break up their courses into more manageable sessions of one to one/class tutoring, with some transportable materials such as online webinars, and on the go tutorials that leaders can easily fit into their day with little disruption. The flexibility of blended learning makes it much easier to keep up as your business scales and grows, particularly nowadays when working from home and remote working is much more common.

Remote and Flexible Working

It's quite likely that at least one member of your team works remotely, whether they're a contractor or just somebody who needs to due to factors such as childcare. Remote working offers better flexibility, and better work life balance to your employees, it also opens up the ability to employ

people from different backgrounds, and even countries, making the talent pool you're fishing from much richer, which in turn will help to grow your business.

Training Millennials

Developing training strategies now to ensure millennials are well prepared for leadership is an important way to ensure smooth transitions once the next generations of employees (Gen Z) enter the workforce. It's important to note that leadership styles have evolved with the ways of working and culture in many environments, and therefore the leadership styles that are taught should be aligned to this and also take into account the workforce of Gen Z.

Outside Consultants

It is really important to understand the need of the leadership development as well as to understand that a consultant can help, they bring in external information, knowledge and experiences. Consultants are often hired to improve communication skills, collaboration and organizational skills, as well as skills specific to the job.

Artificial intelligence

AI is gradually being developed and implemented to both augment and replace human customer service agents to save costs and reduce the needs for human customer service staff. Whilst these bots are able to answer basic questions, there is still a need for a strong presence of a customer services team in order to keep customers happy. Using bots to take away need to answer repetitive and simple questions will free up your team to put more focus on the more difficult questions, and ultimately keep your customers happy.

Establishing of a Culture Allowing Engagement and Motivation of Employees

As mentioned above it is very important to have engaged and motivated employees because it increases productivity, efficiency and decreases employee turnover. It is proven that employer cannot just force employees to be engaged in the workplace, there are certain ways to reach this. Because having a successful business is every employer's dream, employee engagement is very important.

Employee engagement is the level of commitment, passion, and loyalty a worker has toward their work and company. The more engaged an employee is, the more work they'll put forth.

Picture two employees: One comes into work 10 minutes early each day, is excited to be there, and constantly comes up with and shares ideas for improving operations. The other employee gets to work on time every day, does the bare minimum, and counts the time until they can leave. Which employee is highly engaged?

For a business owner, the answer is simple. You want hard-working employees who are actively engaged with the work they do. You can create a culture of organizational engagement by doing the following (Kappel, 2021):

Don’t Skip Onboarding and Training

Onboarding and training new hires are some of the most important steps you can take to ensure employees are engaged at work. One-third of new hires leave their jobs after only six months. With a successful onboarding and training program, employees will learn how to effectively do their job. This is the time they can engage with you and ask questions, offer ideas, and voice concerns. For most employees, onboarding and training is also the time when they bond with co-workers and develop a connection to the company. Studies have shown that the more friends employees have at work, the more engaged they are. Onboarding encourages relationships among employees.

Set Company Goals

To run a successful business, you need a business plan with a list of goals you want to accomplish. To engage employees, you need to involve them in reaching business goals. You should set annual, semi-annual, quarterly, and monthly goals so employees have something to work toward. Reaching goals is something that encourages employee engagement. You can set general company goals as well as goals within each department. That way, each employee knows how their work is impacting the departmental and overall success of your business.

Acknowledge Employees

Employees don’t automatically become engaged when you give them more praise, thanks, or any other type of acknowledgment. However, employees can quickly become disengaged if they feel like they’re invisible. Engaged employees have a sense of comfortability with your business. Again, it’s important for employees to know their co-workers and develop friendships with them. But it’s also important to develop a relationship of respect and friendship between employer and employee.

Focus on Employee Development

There are many reasons job seekers apply for and accept a position, like salary and benefits. But many workers also want the opportunity to grow their career. One Gallup poll found that 87% of millennials (and 69% of non-millennials) view development as important in their jobs. (Gallup, 2021)

Employees want to develop their skills and continue challenging themselves. They don’t want to do monotonous tasks that require minimal effort. Engaged employees constantly use their mind and enhance their skills.

You can focus on employee development in a few different ways. You might add new duties to the employee’s position to prevent boredom, allow room for growth in the position, or offer a job rotation program so employees do different tasks every so often.

Another way you can emphasize employee development is by offering educational assistance. This is a great perk that lets employees further their education. It shows employees that you value their career growth, and it also allows you to add new skills to your business.

Don’t Micromanage

If employees are told exactly what to do and how to do it, they won’t have the time or motivation to engage with the work. They’ll be more like robots. Employees can’t be engaged if they don’t have freedom in how to do their jobs.

Micromanaging can be damaging to your business. One business found that micromanaging resulted in 68% of employees saying their morale was dampened and 55% saying it led to a decrease in productivity. Lost morale and productivity lead to actively disengaged workers.

Start by looking at the big picture. Leave the details up to your employees, and you’ll end up with workers happy to put their own methods and ideas into action.

1.1. Organisational Structures Allowing Engagement and Motivation of Employees

Research shows that organization structure has an impact on the employee performance; a poor organized organization structure means that there will be low productivity, less delegation of work, no incentives provided and centralized decisions. In the end this affects how employees are satisfied with their work hence affect their performance. (Organizational Structures and Design, 2021)

In addition, the study also found out that a good organization structure helps in improving the performance of employees and motivates them to work hard which in the end increase productivity. Therefore, management must develop skills on how to develop their structures, they need to focus on what they can include in the structure or coming up with a new organization structure because this plays a great role for workers to experience job satisfaction. If organizations develop a good structure they have satisfied employees whose work not only achieves organization goals but also individual goals and hence achieving both individual and organization goals. (Grin, 2021)

Extrinsic and Intrinsic Motivation

Motivation is a driving force that determines the success of a person. There are two types of motivation: intrinsic and extrinsic.

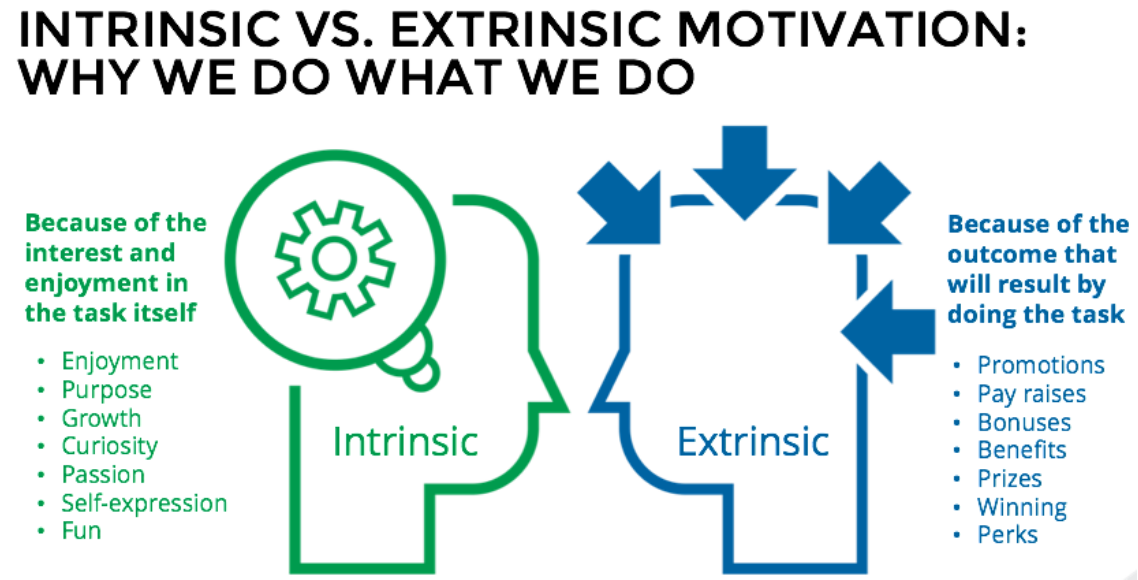


Figure1. Intrinsic vs. extrinsic motivation (J, 2021)

Intrinsic motivation comes from within and is characterized by a deep-seated interest in expanding one's own knowledge and abilities. When employees are intrinsically motivated their path to learning is accompanied by the enthusiasm, curiosity, passion and the joy of discovery. Such employees learn because they genuinely like to learn and do not expect anything external in return for their efforts apart from a sense of personal accomplishment and satisfaction after mastering a challenging topic or skill.

Extrinsic motivation, however, comes from without and is sustained by an external reward such as pay rise, promotion, bonus, etc.

The role of the leaders is to ensure employees are not just motivated but also correctly motivated to learn and perform. To achieve this, it is recommended to create a learning environment that instils and establishes the balance between both intrinsic and extrinsic motivation. (J, 2021)

1.2. Topic Centered Interaction according to Ruth Cohn

Topic Centered Interaction (TCI) is a concept for:

- Working with groups and teams
- Teaching in schools, the university or in continuing, adult education
- Counseling and Coaching
- Directing institutions and their employees
- a conceptual design for the art of living.

In essence it is the goal of TCI to facilitate the interaction between tasks and individuals in order to encourage the development of factual, social and self-competence.

During the past 30 years the concept of Theme-centered Interaction (TCI) has spread rapidly, and it is one of the most widely used methods in the areas of Humanistic Psychology and of Education. (English et al., 2021)

TCI aims to assist people to present and structure their interests in a responsible and self-determined way and to use resources creatively. The TCI training programme is intended to have a lasting effect, in the knowledge that quick successes are often unrealistic. People who think differently are treated with respect.

Individuals are seen holistically, meaning that there is room for the three dimensions of body, soul and mind. This allows for a working atmosphere that frees motivation and creative potentials. Disturbances are not disregarded. but used for improving cooperation thus making a climate of esteem and mutual respect possible.

TCI emphasizes both methodical skills and personal authenticity.

4-factor Model and Dynamic Balance

Every group is defined by the four factors: I (the individual), WE (the group interaction), IT (the task), the GLOBE (context). Appreciation and support of equilibrium among the I-We-It-factors in context represents the basis of the TCI group work.

It is the task of the TCI group leader to pay attention to the **"dynamic balance"** among the four factors.

Equilibrium between intellectual and emotional participation, exertion and relaxation, speaking, silence and activity are all a part of the dynamic balance.

The term "dynamic" means that balance is not static like a scale, but, similar to a bicycle, is part of the process.

Facilitating and leading groups according to the TCI concept permits a style of leadership that combines

- competence,
- motivation,
- mutual esteem and
- goal orientation.

It is appropriate for all areas in which people need to work together successfully in all kinds of teams and groups - e.g. management, education, social work. TCI is also helpful for people, who desire to use it to structure their personal lives creatively. (English et al., 2021)

2. Aspects of Change Management

With any activity that involves improvement, change is an inevitable part of the process. Managing change must remain a strong focus without distraction. In any process or project undertaken for improvement purposes managing change is a huge part of the process and not in any way separate from it. For this it is really important that the process starts with proper readiness assessment. (Change Management Process, 2021)

Readiness Assessments

Assessments are tools used by a change management team or project leader to assess the organization's readiness to change. Readiness assessments can include organizational assessments, culture and history assessments, employee assessments, sponsor assessments and change assessments. Each tool provides the project team with insights into the challenges and opportunities they may face during the change process. The three most important aspects to assess is (Creasey, 2021):

1. Assess the Scope of the Change:
   - How big is this change?
   - How many people are affected?
   - Is it a gradual or radical change?
2. Assess the Readiness of the Organization Impacted by the Change:
   - What is the value-system and background of the impacted groups?
   - How much change is already going on?
   - What type of resistance can be expected?

   You will also need to assess the strengths of your change management team and change sponsors, then take the first steps to enable them to effectively lead the change process.

Communication and Communication Planning

Many managers assume that if they communicate clearly with their employees, their job is done. However, there are many reasons why employees may not hear or understand what their managers are saying the first time around. In fact, you may have heard that messages need to be repeated five to seven times before they are cemented into the minds of employees.

Effective communicators carefully consider three components:

- The audience
- What is communicated
- When it is communicated

For example, the first step in managing change is building awareness around the need for change and creating a desire among employees. Therefore, initial communications are typically designed to create awareness around the business reasons for change and the risk of not changing. Likewise, at each step in the process, communications should be designed to share the right messages at the right time.

Communication planning, therefore, begins with a careful analysis of the audiences, key messages and the timing for those messages. The change management team or project leaders must design a communication plan that addresses the needs of frontline employees, supervisors

and executives. Each audience has particular needs for information based on their role in the implementation of the change.

Sponsor Activities and Sponsor Roadmaps

Business leaders and executives play a critical sponsor role in times of change. The change management team must develop a plan for sponsor activities and help key business leaders carry out these plans. Research shows that sponsorship is the most important success factor. The CEO of the company may support your project, but that is not the same as sponsoring your initiative. Sponsorship involves active and visible participation by senior business leaders throughout the process, building a coalition of support among other leaders and communicating directly with employees. Unfortunately, many executives do not know what this sponsorship looks like. A change manager or project leader's role includes helping senior executives do the right things to sponsor the project. (Best Practices in Change Management, 2021)

Figure 2. Sponsorship as part of change management (Best Practices in Change Management, 2021)

Change Management Training for Managers

Managers and supervisors play a key role in managing change. Ultimately, the manager has more influence over an employee's motivation to change than any other person. Unfortunately, managers can be the most difficult group to convince of the need for change and can be a source of resistance. It is vital for the change management team and executive sponsors to gain the support of managers and supervisors. Individual change management activities should be used to help these managers through the change process.

Once managers and supervisors are on board, the change management team must prepare a strategy to equip managers to successfully coach their employees through the change. They will need to provide training and guidance for managers, including how to use individual change management tools with their employees.

Training Development and Delivery

Training is the cornerstone for building knowledge about the change and the required skills to succeed in the future state. Ensuring impacted people receive the training they need at the right time is a primary role of change management. This means training should only be delivered after steps have been taken to ensure impacted employees have the awareness of the need for change

and desire to support the change. Change management and project team members will develop training requirements based on the skills, knowledge and behaviors necessary to implement the change. These training requirements will be the starting point for the training group or the project team to develop and deliver training programs.

Resistance Management

Resistance from employees and managers is normal and can be proactively addressed. Persistent resistance, however, can threaten a project. The change management team needs to identify, understand and help leaders manage resistance throughout the organization. Resistance management is the processes and tools used by managers and executives with the support of the change team to manage employee resistance.

Employee Feedback and Corrective Action

Managing change is not a one-way street; employee involvement is a necessary and integral part of managing change. Feedback from employees as a change is being implemented is a key element of the change management process. Change managers can analyze feedback and implement corrective action based on this feedback to ensure full adoption of the changes.

Recognizing Success and Reinforcing Change

Early adoption, successes and long-term wins must be recognized and celebrated. Individual and group recognition is a necessary component of change management in order to cement and reinforce the change in the organization. Continued adoption needs to be monitored to ensure employees do not slip back into their old ways of working.

After-Project Review

The final step in the change management process is the after-action review. It is at this point that you can stand back from the entire program, evaluate successes and failures, and identify process changes for the next project. This is part of the ongoing, continuous improvement of change management for your organization and ultimately leads to change competency.

These elements comprise the areas or components of a change management program. Along with the change management process, they create a system for managing change. Good project managers apply these components effectively to ensure project success, avoid the loss of valued employees and minimize the negative impact of the change on productivity and a company's customers. (Best Practices in Change Management, 2021)

3. Transactional and Transformational Leadership, Connected Leadership

Leadership can be described as transactional or transformational. Transactional leaders focus on the role of supervision, organization, and group performance. They are concerned about the status quo and day-to-day progress toward goals. Transformational leaders work to enhance the motivation and engagement of followers by directing their behavior toward a shared vision. While transactional leadership operates within existing boundaries of processes, structures, and goals,

transformational leadership challenges the current state and is change-oriented. (Types of Leaders | Boundless Management, 2021)

Transactional Leadership

Transactional leadership promotes compliance with existing organizational goals and performance expectations through supervision and the use of rewards and punishments. Transactional leaders are task- and outcome-oriented. Especially effective under strict time and resource constraints and in highly specified projects, this approach adheres to the status quo and employs a form of management that pays close attention to how employees perform their tasks.

Transformational Leadership

Transformational leadership focuses on increasing employee motivation and engagement and attempts to link employees' sense of self with organizational values. This leadership style emphasizes leading by example, so followers can identify with the leader's vision and values. A transformational approach focuses on individual strengths and weaknesses of employees and on enhancing their capabilities and their commitment to organizational goals, often by seeking their buy-in for decisions.

Comparing Leadership Types

Transactional and transformational leadership exhibit five key differences:

1. Transactional leadership reacts to problems as they arise, whereas transformational leadership is more likely to address issues before they become problematic.
2. Transactional leaders work within existing an organizational culture, while transformational leaders emphasize new ideas and thereby "transform" organizational culture.
3. Transactional leaders reward and punish in traditional ways according to organizational standards; transformational leaders attempt to achieve positive results from employees by keeping them invested in projects, leading to an internal, high-order reward system.
4. Transactional leaders appeal to the self-interest of employees who seek out rewards for themselves, in contrast to transformational leaders, who appeal to group interests and notions of organizational success.
5. Transactional leadership is more akin to the common notions of management, whereas transformational leadership adheres more closely to what is colloquially referred to as leadership.

Transactional leaders focus on performance, promote success with rewards and punishments, and maintain compliance with organizational norms. While transformational leaders exhibit individualized consideration, intellectual stimulation, inspirational motivation, and idealized influence.

A Blended Approach to Leadership

The full-range leadership theory blends the features of transactional and transformational leadership into one comprehensive approach.

The full-range theory of leadership seeks to blend the best aspects of transactional and transformational leadership into one comprehensive approach. Transactional leadership focuses on exchanges between leaders and followers. Transformational leadership deals with how

leaders help followers go beyond individual interests to pursue a shared vision. These two approaches are neither mutually exclusive, nor do leaders necessarily exhibit only one or the other set of behaviors. Depending on the objectives and the situation, a leader may move from using one approach to the other as needed.

4. Personality Development in Modern Organisations

At the beginning of every year, most people set goals for personal development, however, more than 96% fail to archive them. Research shows that 80% of New Year's resolutions are abandoned by February. Continuous personal development is fundamental to career growth, professional satisfaction, and having a broader impact on the world. (Personality Development and It's Importance - Management Study HQ, 2021)

It is very important that all individuals have personal development goals as part of their resolution, for the following reasons:

Ensures Continuous Improvement/Growth: You should always aim to be better than you were yesterday. As an individual, you should always keep on improving yourself. If you feel that there some things you don't like about yourself work on changing them. Don't stagnate always seek a better you.

Helps in Better Management: Personality development helps you have the right personality and social skills. With these two, team participation becomes easier because you can interact effortlessly with colleagues. With a good personality, your employees will enjoy working with you and most likely perform better because you're a good boss, who is full of positive energy.

Builds Balance in Life: Personality development can help you be more organized, punctual, a person who keeps his word, etc. When you acquire such skills, you are able to plan every area of your life so no one suffers. You create time for your family, time to exercise and meditate, work, and so on. Every area benefits from a good and developed personality.

Ensures Excellence in one's Field: If you are constantly developing yourself you will ultimately become the best version of yourself. You become the go-to person on any matter in your field. That is why you find many CEOs are very keen on theirs and staff development. You must keep learning new things to keep up with the ever-changing world. Personality development improves your chances of success in any undertaking-because you have the right mindset are goal-oriented and likable.

5. Internal Communication in Modern Leadership

Leadership communication is one of the most important factors that influences business success. Learning the skills necessary to have effective workplace conversations is critical if we want to implement changes and produce real business results.

Effective leadership communication is not just a new business buzz phrase. It has a clear and critical impact on an organization's bottom line. Moreover, good communication is one of the most important leadership traits.

Therefore, every leader should provide their employees with the tools, and the opportunities, to have meaningful and productive conversations. Leadership communication has changed significantly in the past few years, and it is now more important than ever before.

However, leaders need to be ready to deal with these changes and adjust their internal communications strategy.

Leadership communications trends that companies should consider for improvement 2021 and beyond are (18 Leadership Communication Trends to Look For in 2021, 2021):

Keeping Employees Engaged

Employee engagement drives employee productivity and business success. Yet, 85% of employees are not engaged in the workplace.

Leaders should, through good internal communication, be able to keep employees engaged and motivated. Quality conversations build trust, empathy and clarity, which are all key ingredients for healthy relationships in the workplace.

If you look at the biggest drivers of employee engagement, many of them revolve around poor communication. Disengaged employees don't understand how they fit into the culture, how managers view their performance, or where the company is headed.

Building an Effective Internal Communications Strategy

Even though companies are becoming aware of the importance of internal comms for business success, 60% of companies are still missing a long-term strategy for their internal communications.

Leaders should play the most important role in building this strategy and support its execution.

Aligning Employees with Strategic Goals

Leaders are responsible for creating synergy and organizational alignment within their companies. This is the most important prerequisite for creating a sense of commitment toward common goals.

When your employees have a good understanding of your company's vision, mission, strategic goals and company culture, they are likely to feel more motivated and engaged.

However, many leaders are still facing challenges related to employees' misalignment with the company's core values and goals.

Communicating More Often

Employees expect more from the leaders when it comes to communications.

Moreover, 71% of employees believe that their leaders do not spend enough time communicating goals and plans. Therefore, one of the most important leadership communications

trends to consider in 2021 is to implement a more robust and efficient internal communications strategy.

Building Stronger Relationships

There is a clear move towards more impactful leadership communication strategies among senior leaders. Leaders are now prioritizing the creation of more open and impactful connections with employees. Leaders should strive towards moving to a less top-down controlled approach and provide more opportunities for collaboration across the organization.

Great leaders are able to see that putting leadership communication strategies in place helps to overcome many internal communication challenges.

Developing an Efficient Content Strategy

Content lies at the heart of everything communicators do, but an increasing number of internal communications contents gets ignored by employees. Therefore, leaders should know how to implement a successful content strategy and management. Creating content that is personalized and relevant is now a must. Therefore, employers are turning to new technologies that can help them boost employee engagement by filtering content that is relevant to employees.

Making Content More Engaging

71% of employees don't read or engage with company emails or content. The main reason why employees don't engage with internal content is because they get too much information that is not relevant to them. For this reason, leaders are now turning to technology solutions that enable them to create personalized news feeds for the employees. Consider adding video to your internal communications strategy.

Building Trust and Encouraging Transparency

Trust is the foundation for successful business. To build trust within workplaces, leaders should communicate in a way that is truthful, open and transparent.

Reaching Every Employee

Making sure that important information reaches the right employees is the crucial part of every internal communication strategy. Moreover, 74% of employees have the feeling they are missing out on important information at work. Therefore, when communicating, leaders need to have a strategy about how the right information will reach the right employees at the right time.

Choosing the Right Communication Channels and Tools

Leaders should understand what is the best way to deliver important information to the employees.

Email is not the most effective way to reach and engage with employees anymore!

60.8% of employees in a survey about workplace communication preferences revealed that they either occasionally, often or always ignore emails at work. With so many people skimming their inboxes, leaders should now consider new internal communications channels and technologies.

Supporting Bottom-Up Conversations

Leaders need to do a better job in supporting two-way conversations and making employees feel like they can speak up. Roughly half of employees aren't regularly speaking their minds at work. Only 52% of employees say that they always or almost always speak their minds when having work-related conversations with their leaders.

Encouraging More Employee-Driven Content

Two-way conversations are impossible to achieve if you don't encourage employee-driven content.

In addition to leaders sharing important messages and information, engage your employees by letting them create and consume employee-generated content.

Switching to Mobile-First Employee Communication

It is not a secret that employees spend more time on their phones than any other device at home or in the workplace. Currently, the workforce is made up of 50% of millennials and by 2025, that number will reach 75%. The one thing we all know about millennials, is that they are tech-savvy and mobile-oriented. Therefore, if you want them to engage with the message you share, you have to adapt your internal communication to their smartphone habits. That means that leaders should now consider implementing mobile-first communication solutions.

Moreover, with the gig economy, freelancers, more part-timers and flexible working locations, it has become a real struggle to reach all employees and deliver important messages at the right time.

Therefore, leaders who enable mobile-first conversations within their workplace are much more likely to reach all their employees and increase engagement levels.

Building a Collaborative Workplace Culture

Good leadership communication helps people to connect and collaborate better, and it is the leaders' job to make that happen.

Effective communication keeps everyone on the same page. When people who work together know how to communicate clearly and respectfully, they can accomplish things more efficiently.

They work together as a unit, rather than as individuals with no clear game plan.

Making Information Easily Accessible

The most common reason why important information gets lost in the workplace is because the information is not easily accessible.

This doesn’t only create frustrations among employees but also has a very negative impact on employee engagement, motivation and productivity.

Preventing Miscommunications

Leaders are responsible for preventing miscommunication in the workplace. In a research, nearly 81% of employees indicated that miscommunication occurred in their organization very frequently, frequently, or occasionally.

To work effectively, employees need accurate information from their leaders. When communications systems aren't in place, that information may not reach everyone who needs it.

Employees may have to seek out the details that they are missing, which takes them away from other work and cuts down on their productivity. In other cases, employees might make mistakes because of lack of information.

Making Employees Brand Ambassadors

Every organization has its interesting moments that should also be seen by the external world. As employees' words are much more trusted than leaders', companies are now trying to make their employees brand ambassadors.

Employees who trust their leaders are willing to share their word both internally and externally. However, many organizations still don't have tools that enable employees to easily share interesting information with the outside world.

Measuring the Effectiveness of Leadership Communications

Today, leaders are able to better understand how efficient their communication towards employees is. Luckily, modern employee communication solutions enable leaders to measure how effective their internal communications efforts are.

6. Developing of a Leadership Concept

Leadership development refers to activities that improve the skills, abilities and confidence of leaders. Programmes vary massively in complexity, cost and style of teaching.

Coaching and mentoring are two forms of development often used to guide and develop leaders.

According to Baldwin and Ford (1988), the success of leadership development is influenced heavily by the quality of the programme, level of support and acceptance from superiors, and the characteristics/learning style of the person being developed.

Some commentators differentiate between leadership development and leader development, the former being used when referring to development programmes focusing on collective leadership in an organisation and the latter on individuals.

Leadership development is a common process in succession planning, which aims to produce high-calibre leaders to take over senior positions when they become vacant. High-performers are typically identified for these leadership development programmes, which may be longer-term and broader than programmes focusing on tighter end-goals. (What is Leadership Development?, 2021)

7. Leadership, Why is it Important to Enhance Resilience

Resilience is the human capacity to meet adversity, setbacks and trauma, and then recover from them in order to live life fully. Resilient leaders have the ability to sustain their energy level under pressure, to cope with disruptive changes and adapt. They bounce back from setbacks. They also overcome major difficulties without engaging in dysfunctional behavior or harming others. (Resilience – it's more important in a leadership role than talent | Penny de Valk, 2021)

Resilience is a crucial characteristic of high- performing leaders. Leaders must cultivate it in themselves in order to advance and thrive. They also carry the responsibility for helping to protect the energy of the people in their teams. Leadership is sustainable only if individuals and teams are able to consistently recover high energy levels. During the event, Professor Kohlrieser asked the audience: "How many of you have seen too much conflict in the workplace? How many of you have observed people getting sick or burning out?" A majority of audience members raised their hands, emphasizing the importance of fostering healthier human dynamics in the workplace.

Building resilience is essential, but we must also remember that the end goal is to find joy in life. We wish not just to survive, but also to thrive. To this end, it is useful to examine the combination of our organizational roles, professional roles and personal roles to ensure that the different aspects of our identity are in balance and that we are able to experience the joy of living.

8. Organizational Resilience Made Simple with ISO Standard

Resilience is the key for any business wanting to thrive in an ever-changing world. A standard was published in 2017 to help put organizations in a better position to meet the challenges ahead. (Organizational resilience made simple with new ISO standard, 2021)

Climate change, economic crises and consumer trends are just some of the pitfalls that can dramatically affect the way an organization does business and survives. Organizational resilience

is a company's ability to absorb and adapt to that unpredictability, while continuing to deliver on the objectives it is there to achieve.

A new standard, ISO 22316, Security and resilience – Organizational resilience – Principles and attributes, provides a framework to help organizations future-proof their business, detailing key principles, attributes and activities that have been agreed on by experts from all around the world.

Leadership & Strategy

- **A Shared Vision:** The members/employees of the organization clearly understand the purpose, vision, and values of the organization.
- **Understands Context:** There is a comprehensive understanding of both the internal and external dimensions of the organization.
- **Effective Leaders:** Leaders are effective and empowered, are trusted and respected, and leadership is distributed throughout the organization.

Culture & Behaviours

- **Healthy Culture:** The existence of core values and behaviors that support the health and welfare of its members/employees, foster creativity and empower members/employees to communicate effectively.
- **Shares Information:** Information and knowledge is shared to enable effective decision-making, learning from experience and from others is encouraged and valued, and is recognized as a critical resource of the organization.
- **Continually Improves:** Performance is continually monitored and a culture of continual improvement is encouraged.

Preparedness & Managing Risk

- **Available Resources**: Resources are adequate and available when needed in order to provide the ability to adapt to changing circumstances.

- **Manages Risk**: Risk is managed throughout the organization and the use of management systems used as appropriate.
- **Manages Change**: Ability to anticipate, plan, and respond to changing circumstances and incidents.

9. Resilient Leadership – After Pandemics for a Better World

The disruptive and converging forces of climate change, urbanization and the current technological revolution are eroding that foundation in new and profound ways. (Critical infrastructure resilience: securing our future - The Resilience Shift, 2021)

It is essential that business leaders make the right decisions now to ensure a safe, equitable and prosperous way forward for our planet and for everyone. To do this, they must understand the factors that brought us to this point and provide new methods, models, tools and approaches to ensure a **transformative approach** to building a more stable future in an increasingly uncertain world.

10. References

(Author), T., 2021. *GRIN - Impact of organization structure on employee performance*. [online] Grin.com. Available at: <https://www.grin.com/document/434752> [Accessed 14 May 2021].

Blog.smarp.com. 2021. *18 Leadership Communication Trends to Look For in 2021*. [online] Available at: <https://blog.smarp.com/18-leadership-communication-trends-to-look-for-in-2020> [Accessed 14 May 2021].

Courses.lumenlearning.com. 2021. *Types of Leaders | Boundless Management*. [online] Available at: <https://courses.lumenlearning.com/boundless-management/chapter/types-of-leaders/#:~:text=Transactional%20leadership%20focuses%20on%20exchanges,to%20pursue%20a%20shared%20vision.&text=Depending%20on%20the%20objectives%20and,to%20the%20other%20as%20needed.> [Accessed 14 May 2021].

Creasey, T., 2021. *When Should You Use a Change Management Readiness Assessment?*. [online] Blog.prosci.com. Available at: <https://blog.prosci.com/when-should-you-use-a-change-management-readiness-assessment> [Accessed 14 May 2021].

Engage Blog. 2021. *Why you should identify your employees' intrinsic and extrinsic motivators*. [online] Available at: <https://www.achievers.com/blog/why-you-should-identify-your-employees-intrinsic-and-extrinsic-motivators/#:~:text=Extrinsic%20motivators%3A%20An%20employee%20motivated,meted%20out%20by%20the%20employer.&text=Intrinsic%20motivators%3A%20Employees%20motivat].

English, I., TCI, W., TCI, W., TCI, H., Cohn, R., Us, A. and TCI, T., 2021. *TCI-Concept - RCI International*. [online] Ruth-cohn-institute.org. Available at: <https://www.ruth-cohn-institute.org/tci-concept.html> [Accessed 14 May 2021].

Gallup, I., 2021. *Millennials Want Jobs to Be Development Opportunities*. [online] Gallup.com. Available at: <https://www.gallup.com/workplace/236438/millennials-jobs-development-opportunities.aspx> [Accessed 14 May 2021].

Harris, A., 2021. *10 New Trends in Leadership & Management to Employ in 2021*. [online] Stratx-exl.com. Available at: <https://www.stratx-exl.com/industry-insights/leadership-management-trends> [Accessed 14 May 2021].

HRZone. 2021. *What is Leadership Development?*. [online] Available at: <https://www.hrzone.com/hr-glossary/what-is-leadership-development> [Accessed 14 May 2021].

ISO. 2021. *Organizational resilience made simple with new ISO standard*. [online] Available at: <https://www.iso.org/news/Ref2189.htm> [Accessed 14 May 2021].

J, J., 2021. *Motivation: Intrinsic vs Extrinsic | Newman Tuition*. [online] Newman Tuition. Available at: <https://www.newmantuition.co.uk/motivation-intrinsic-vs-extrinsic/> [Accessed 14 May 2021].

Kappel, M., 2021. *How To Establish A Culture Of Employee Engagement*. [online] Forbes. Available at: <https://www.forbes.com/sites/mikekappel/2018/01/04/how-to-establish-a-culture-of-employee-engagement/?sh=455999378dc4> [Accessed 14 May 2021].

Kotter. 2021. *Leadership Development - Kotter*. [online] Available at: <https://www.kotterinc.com/services/leadership-development/> [Accessed 14 May 2021].

Management Study HQ. 2021. *Personality Development And It's Importance - Management Study HQ*. [online] Available at: <https://www.managementstudyhq.com/personality-development-importance.html> [Accessed 14 May 2021].

Opentextbc.ca. 2021. *Organizational Structures and Design*. [online] Available at: <https://opentextbc.ca/principlesofmanagementopenstax/chapter/organizational-structures-and-design/> [Accessed 14 May 2021].

Penny de Valk. 2021. *Resilience – it's more important in a leadership role than talent | Penny de Valk*. [online] Available at: <https://pennydevalk.com/resilience-its-more-important-in-a-leadership-role-than-talent> [Accessed 14 May 2021].

Prosci.com. 2021. *Best Practices in Change Management*. [online] Available at: <https://www.prosci.com/resources/articles/change-management-best-practices> [Accessed 14 May 2021].

Prosci.com. 2021. *Change Management Process*. [online] Available at: <https://www.prosci.com/resources/articles/change-management-process> [Accessed 14 May 2021].

The Resilience Shift. 2021. *Critical infrastructure resilience: securing our future - The Resilience Shift*. [online] Available at: <https://www.resilienceshift.org/securing-our-future-through-resilient-infrastructure/> [Accessed 14 May 2021].

11. Recommended literature

Bennis, W. & Goldsmith, J. (2003). *Learning to lead: A workbook on becoming a leader (3rd Ed.).* New York, NY: Basic Books.

Bennis, W. & Nanus, B. (1985). *Leaders: The strategies for taking charge.* New York, NY: Harper Collins.

Bennis, W. (1959). Leadership theory and administrative behavior: The problems of authority. *Administrative Science Quarterly*. *4*(2): 259-301.

Bolman, L.G. & Deal, T.E. (2013). *Reframing organisations. Artistry, choice and leadership (5th Ed.).* San Francisco, CA: Jossey Bass.

Bowden, A.O. (1927). A study of the personality of student leadership in the United States. *Journal of Abnormal Social Psychology*. *21*: 149-160

Bass, B.M. Stogdill Handbook of Leadership: *A survey of theory and research* (2nd Ed.). New York, NY: The Free Press.

Crowe, B.J., Bochner, S. & Clarke, A.W. (1972). The effects of subordinates' behavior on managerial style. *Human Relations. 25*:215-237.

Covey, S. (1992). *Principle centred leadership*. London: Simon & Schuster.

Dansereau, F., Graen, G. & Haga, W.J. (1975). *A vertical dyad linkage approach to leadership in formal organizations.* Organizational behavior and performance. 13(1): 46-78.

Dienesh, R.M. & Liden, R.C. (1986). *Leader-member exchange model of leadership: A critique and further development.* Academy of Management Review. 11:618-634.

Emmons, M., 2021. *Key Statistics about Millennials in the Workplace | Dynamic Signal*. [online] Dynamic Signal. Available at: <https://dynamicsignal.com/2018/10/09/key-statistics-millennials-in-the-workplace/> [Accessed 14 May 2021].

Engage Blog. 2021. *Why you should identify your employees' intrinsic and extrinsic motivators*. [online] Available at: <https://www.achievers.com/blog/why-you-should-identify-your-employees-intrinsic-and-extrinsic-motivators> [Accessed 14 May 2021].

Fitzsimmons, T.W. & Callan, V.J. (2016). CEO selection: A capital perspective. *The Leadership Quarterly*. *27*(5): 765-787.

Global Citizen. 2021. *10 Reasons The World Needs More Sustainable Leadership*. [online] Available at: <https://www.globalcitizen.org/en/content/0-reasons-the-world-needs-sustainable-leadership> [Accessed 14 May 2021].

Gardner, J.W. (1989). *On leadership.* New York, NY: Free Press.

Hersey, P. & Blanchard, K. (1969). Life cycle theory of leadership. *Training and Development Journal. 23*(1): 26-34.

Haslam, S.A, Reicher, S.D., & Platow, M.J. (2011). *The new psychology of leadership: Identity, influence and power.* New York: Psychology Press.

Hunt, J. (2004). What is leadership? In J. Antonakis, A. Cianciolo & R. Sternberg (Eds.). *The nature of leadership.* London: Sage.

Iso.org. 2021. [online] Available at: <https://www.iso.org/obp/ui/#iso:std:iso:22316:ed-1:v1:en> [Accessed 14 May 2021].

Jenkins, W.O. (1947). A review of leadership studies with particular reference to military problems. *Psychological Bulletin*. *44:* 54-79.

Kets de Vries, M. 2001. *The leadership mystique: A user's manual for the human enterprise.* London: Prentice Hall.

Kotter, J. 1990. *A force for change. How leadership differs from management.* New York, NY: Free Press.

Lion & Gazelle. 2021. *5 Aspects of Change Management Necessary for Successful Process Improvement Projects - Lion & Gazelle*. [online] Available at: <https://www.lionandgazelle.com/5-aspects-of-change-management-necessary-for-successful-process-improvement-projects/> [Accessed 14 May 2021].

Management Study HQ. 2021. *Good Habits of Highly Effective People - Management Study HQ*. [online] Available at: <https://www.managementstudyhq.com/habits-of-highly-effective-people.html> [Accessed 14 May 2021].

Manz, C.C. & Sims, H.P (1987). *Leading workers to lead themselves: The external leadership of self-managing work teams.* Administrative Science Quarterly. 32: 106-128.

Mitchell, T.R. (1979). *Organizational behavior.* Annual review of psychology 30: 243-281.

Prosci.com. 2021. *Change Management Process*. [online] Available at: <https://www.prosci.com/resources/articles/change-management-process> [Accessed 14 May 2021].

Pfeffer, J. (1977). *The ambiguity of leadership.* Academy of Management Review. 2(1): 104-112.

ResearchGate. 2021. *(PDF) Sustainability Leadership: Linking Theory and Practice*. [online] Available at: <https://www.researchgate.net/publication/228320235_Sustainability_Leadership_Linking_Theory_and_Practice> [Accessed 14 May 2021].

Rhabitanalytics.com. 2021. [online] Available at: <https://rhabitanalytics.com/2019/04/18/the-importance-of-being-engaged-at-work/> [Accessed 14 May 2021].

Schein, E.H. (1985). *Organizational culture and leadership.* San Francisco, CA: Jossey-Bass.

Van Seters, D.A. & Field, H.G. (1990). The evolution of leadership theory. *The Journal of Organizational Change Management. 3*(3): 29-45.

Van Seters, D.A., & Field, H.G. (1990). The evolution of leadership theory. *The Journal of Organizational Change Management. 3*(3): 29-45.

Zaleznik, A. 1977. Managers and leaders: Are they different? *Harvard Business Review 55*:67-78