International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Implementation of ISO 22301:2019 using ISO 31000:2018 In a Pharmaceutical Organization

Prashant Magerde, Dr.Astitwa Bhargava

Abstract: - *The key advantage of modern business is that it operates continuously and effectively, is constructed in accordance with legal standards, and is focused on customer needs. Pharmaceutical companies were no different. They focus on both the management system and product quality in order to conduct successful business. The implementation of ISO 22301:2018, or the "Business Continuity Management System," will help to save the company and prevent or minimize the consequences of emergencies.*

To implement the project, it is necessary to assess the critical stages of the company's activities and establish the value of each process. This information is further required for the optimal allocation of resources and building a business continuity system for a pharmaceutical company with the regulation of measures to prevent or eliminate the consequences of emergency situations as soon as possible. In this research paper, researcher want to implement ISO 22301:2019 using risk management process given in ISO 31000:2018.

Keywords: Business Continuity Plan, Disaster Recovery Plans, BCMS, Risk management.

Introduction

The pharmaceutical sector ensures the growth of exports and the economic recovery. "The Indian pharmaceutical sector is worth US$ 42 billion worldwide. In August 2021, the Indian pharmaceutical market increased at 17.7% annually, up from 13.7% in July 2020. According to India Ratings & Research, the Indian pharmaceutical market revenue is expected to be over 12% 2022."[1]

"The Indian pharma industry is expected to grow to $130 billion by 2030 and become the leading provider of medicines to the world, said Indian Pharmaceutical Alliance (IPA) Secretary General, Sudarshan Jain on Thursday. The Indian pharma industry is currently valued at $49 billion and is the third largest in the

[1] IBEF (India Brand Equity Foundation), "Indian Pharmaceutical Industry" Aug 2022 <https://www.ibef.org/industry/pharmaceutical-india> accessed on 29th October 2022.

world. India supplied medicines to over 200 countries in the world, he said."[2] All of this demonstrates how pharmaceutical company management success helps to actively expand the economy as well as provide the populace with medicine. By actively implementing the integrated management approach, the market's leaders in pharmaceuticals are putting a number of international standards into practice aimed at raising the bar for the quality of their products and pharmaceutical services, giving them a competitive advantage and a guarantee of high-quality performance. First of all, pharmaceutical companies have implemented such standards as ISO 9001 «Quality Management System», ISO 22000 «Food Safety Management Systems», ISO 14001 «Environmental Management System», ISO 13485 «Medical Products. Quality management systems. Requirements» and a number of others, which promotes development. Integration of these standards is quite a hard work and it requires effective and constant planning and control. Based on the experience of foreign companies, we can say that the process approach used in the standards requires the assessment of risks and protection from crisis situations to fully ensure the quality of work. Today, the ISO 22301 «Business Continuity Management System» standard is quite relevant. Its principles can be used to stabilize the activities of pharmaceutical companies in our country. The approach to its implementation has become the goal of this research.

"Recent global events have demonstrated to pharmaceutical businesses the value of having a strong business continuity strategy (BCP). Given the complexity of the supply chains in the pharmaceutical sector, risk management can be difficult. However, it is an essential component of the business continuity strategy."[3]

One instance that sticks out in our minds is the creation of the COVID-19 vaccine. As you undoubtedly recall, a lot of renowned pharmaceutical businesses claimed a lack of suppliers as well as equipment, material, and staff shortages. which, unsurprisingly, led to a slowdown in the scaling-up of vaccine manufacturing and a delay in the provision of vaccines. Future medicine shortages can be prevented by using this experience to improve pharmaceutical companies' business continuity plans.

This business continuity guideline offers a series of recommendations for how to get ready for any emergency while limiting the impact on WHO operations. Business continuity strategies must be created, implemented, emulated, monitored, and often updated.

[2] Sudarshan Jain, secretary general, Indian Pharmaceutical Alliance (IPA), Business Standard September 2022, <https://www.business-standard.com/article/companies/indian-pharma-industry> accessed on 28th October 2022.

[3] TuneEngineering, "Business Continuity in Pharma: the role of Risk Management" 4TE Team (2022) <https://blog.4tuneengineering.com/business-continuity-in-pharma-the-role-of-risk-management/> accessed on 6th November 2022.

"The recommendations are based on standardized organizational practices for risk management and emergency response for all threats and at all organizational levels. The WHO corporate risk management strategy and methodology, as well as the ISO 22301 (Business Continuity Management System), are taken into consideration."[4]

Thomas M. Chen, Information Security and Risk Management "In this book provides the risk management process in steps. In this chapter the risk management process is divided into three steps risk assessment, mitigation and effectiveness evaluation of controls that you applied for risk management and provides steps how to evaluate risk in IT environment."[5]

Susan Snedaker, Business Continuity & Disaster Recovery "The author explored the idea and practical application of risk management in this chapter, as well as the broad company viewpoint, practical business continuity and disaster recovery planning perspective, and IT-centric perspective. The author also examines risk management to have a better understanding of the whole process before delving into the risk assessment procedure. The initial phase of project work begins here."[6]

Author also go over emergency activities including disaster response and business recovery, so author refer only briefly to those elements in this chapter where appropriate. The author also mentioned training, testing, and keeping the strategy up to date. All of these components should be included in your BC/DR strategy. The strategy should simply outline the risks, vulnerabilities, and potential effect on each of the mission-critical business operations. There should be mitigating techniques for each of them. In some circumstances, several mitigation options will be available; in others, you may have chosen to just accept the risk."[7]

Michael Wallace and Lawrence Webber, The Disaster Recovery Handbook In this book "The author discusses ideas for identifying tasks that are essential to your organization's performance and the order of importance that these tasks should be completed. Functions ought to be brought back. Politically, conducting a BIA may be challenging since each department inside an organization will naturally think that its tasks are

[4] World Health Organization, "WHO guidance for business continuity planning" (2022) WHO/WHE/CPI/2018.60 <https://apps.who.int/iris/bitstream/handle/10665/324850/WHO-WHE-CPI-2018.60-eng.pdf> accessed on 6th November 2022.

[5] Thomas M. Chen, "Information Security and Risk Management" Southern Methodist University, USA "Encyclopedia of Multimedia Technology and Networking" (2009) page 668 2nd ed., Idea Group Publishing.

[6] Susan Snedaker, "Business Continuity & Disaster Recovery" Syngress Publishing, Inc "Risk Assessment" < https://b-ok.asia/book/486981/3b5df9> accessed on 29th October.

[7] Susan Snedaker, "Business Continuity & Disaster Recovery" Syngress Publishing, Inc "Business Continuity & Disaster Recovery" < https://b-ok.asia/book/486981/3b5df9> accessed on 29th October.

the most important and may be reluctant to divulge information to someone outside of the department.” [8]A successful BIA requires the following:

- Strong and vocal support from senior management
- A capable project leader
- A well-crafted questionnaire
- Complete and honest answers from each department

Andrea Ko, "Risks Evaluation and IT Audit Aspects of Business Intelligence Solutions" Academia (2014) “Many businesses are battling to make sense of massive amounts of data in order to acquire meaningful insights and assist in their decision-making process. The quality of decision-making is becoming increasingly dependent on information and the mechanisms that convey it. These services are fragile and dangerous in terms of security, and they must meet a number of standards, including transparency, availability, accessibility, convenience, and compliance. IT infrastructures are becoming increasingly complicated and dispersed, which increases security threats. In these complicated business settings, business intelligence tools can help. Their primary purpose is to help corporations make better decisions. Better decisions imply that these solutions aid in risk management and play an important role in increasing income and decreasing costs.”[9]

Hanane Anir, Mounia Fredj and Meryem Kassou, “Towards an approach for Integrating Business Continuity Management into Enterprise Architecture” International Journal of Computer Science & Information Technology (IJCSIT) (2019) “Security is a big problem for any corporation in the global and complex commercial environment of today. All businesses should be able to prepare for and react to incidents and other disruptions of business. Information security management includes business continuity management (BCM), which can be used to address these requirements. In fact, business continuity refers to a company's capacity to carry on with operations even in the event of a failure or tragedy. Business continuity management (BCM) demands a comprehensive strategy that takes organizational and technological factors into account. A comprehensive picture of organizational, business, and technological architecture as well as

[8] Michael Wallace and Lawrence Webber, "The Disaster Recovery Handbook" Amacom (2018) <http://www.amacombooks.org/go/DisasterRecovery3E> accessed on 29th October 2022.

[9] Andrea Ko, “Risks Evaluation and IT Audit Aspects of Business Intelligence Solutions” Academia (2014) <https://www.academia.edu/10744178/Risks_Evaluation_and_IT_Audit_Aspects_of_Business_Intelligence_Solutions> accessed on 26th October 2022.

their interactions is provided by enterprise architecture (EA). Numerous studies view EA as a foundation for BC and security management."[10]

Lebedinets Viacheslav, Romelashvili Olena and Stepanenko Serhiy, "Status of the Problem of Falsified Pharmaceutical Products on the World and National Pharmaceutical Markets" (2018), Science Review, "The article analyzed the possibility of drug fraud on the Ukrainian pharmaceutical market. This issue is taken into account in light of the ongoing trend toward an increase in the availability of fake medications on both the domestic and international pharmaceutical marketplaces. This endangers the lives and health of the populace and costs the government and domestic pharmaceutical manufacturers a sizable sum of money."[11]

Saiful Bahari Mohd Sabtu, Ganthan Narayana Samy and Bharanidharan Shanmugam, "Business Impact Analysis Ontology for Information Technology Continuity Management" (2014) "The ongoing work to create ontology for business impact analysis (BIA) in the area of information technology business continuity management for Malaysia's public sector is described in this proceeding paper. BIA is a process that looks at the importance of business functions and how they will be impacted by an incident, crisis, or disaster. The traditional BIA method involves straightforward information tabulation using tables, check lists, questionnaires, and surveys. This study investigates the use of ontology in providing a semantically rich knowledge representation for BIA as more complicated methodologies, such as that utilizing matrix representation, business process remodeling, and analytical tools, become more prevalent. The primary output is the creation of an appropriate ontology for BIA."[12]

The organization's Business Continuity Plan mainly fails due to an ineffective risk management implementation. Organizations can implement effective Business Continuity Plan with risk management frameworks like ISO 31000, 27005, etc.

[10] Hanane Anir, Mounia Fredj and Meryem Kassou, "Towards an approach for Integrating Business Continuity Management into Enterprise Architecture" International Journal of Computer Science & Information Technology (IJCSIT) (2019) <https://aircconline.com/ijcsit/V11N2/11219ijcsit01.pdf> accessed on 22nd October 2022.

[11] Lebedinets Viacheslav, Romelashvili Olena and Stepanenko Serhiy, "Status of the Problem of Falsified Pharmaceutical Products on the World and National Pharmaceutical Markets" (2018), Science Review, <https://doi.org/10.31435/RSGLOBAL_SR/01072018/5922> accessed on 21st October 2022.

[12] Saiful Bahari Mohd Sabtu, Ganthan Narayana Samy and Bharanidharan Shanmugam, "Business Impact Analysis Ontology for Information Technology Continuity Management" (2014) < https://www.academia.edu/40371152/Business_Impact_Analysis_Ontology_for_Information_Technology_Continuity_Management > accessed on 25th October 2022.

The main objective of the researcher to prepare a plan and process for implementation of ISO 22301 “Business Continuity Management System” using ISO 31000 “Risk management – Principles and Guidelines” in pharmaceutical company and also:

- To understand issues and challenges in implementation of ISO 22301 in Pharmaceutical sectors.
- To analyze use of ISO 31000 in implementation of ISO 22301.
- To analyze critical processes and functions in pharmaceutical sector.
- What elements affect pharmaceutical organization readiness for disasters?
- How pharmaceutical can effectively prepare for disasters?
- How pharmaceutical organization can use ISO 31000 in implementation of ISO 22301 for better Information Security and Business Continuity?
- How effective risk management framework like ISO 31000 can help pharmaceutical organization to manage disaster situation?
- Does catastrophe preparedness affect pharmaceutical company continuity in any way?

This study's focus is solely on using international standards and the controls that are mandated by them. The results of this study might be impacted by a number of uncontrollable circumstances. Investigation may be challenging due to the difficulty of accessing the interesting environment, activity, or event.

Role of ISO 27001, ISO 31000 and ISO 22301 Standards in Pharmaceutical

ISO 27001: ISO 27001 is an information security management systems standard that provides a framework for safeguarding and protecting confidential and sensitive data to enterprises of any size and sector.

Healthcare companies have recently become targets of cyber assaults, raising concerns about the protection of their medical information. Hackers utilise sensitive information to falsely charge hospitals and patients for surgeries or costly medical equipment, which they subsequently resell. Because many healthcare institutions are transitioning to digital record keeping or are still utilising antiquated technologies. As a result, they are particularly vulnerable to cyber assaults. ISO 27001 may assist healthcare businesses in identifying and mitigating risk, safeguarding sensitive medical information, and informing the public that their confidentiality is treated seriously.

With such substantial security dangers in the healthcare business, the government's next logical move would be to begin enacting stronger rules. With ISO 27001 certification, your firm will not only be prepared for these upcoming standards, but will also set an industry-wide example.

An ISO 27001 certification may help organisations of all sizes and types. Assure your clients that you are concerned about their safety and confidentiality by implementing ISO 27001.

ISO 31000: Pharmaceutical regulatory bodies now demand that “effective” risk management systems be integrated into the product life cycle. The definition of effective as an adjective is “successful in attaining a desired or planned consequence.” So, how do we know our risk management method is effective? What proof do we have that it works? The risk management process itself may pose the greatest danger if it accidentally leads us in the wrong path, causing us to make mistakes, some of which are more serious than others. The goal of risk review is to find proof that we made the right decisions based on our risk management outputs.

The effectiveness of risk management is an indirect measurement. This is due to the fact that ISO 31000 (2018) defines risk as the “impact of uncertainty on objectives” (www.iso.org). For pharmaceuticals, it should be about effectively managing uncertainty and its consequences in relation to business objectives such as product quality and patient safety.

ISO 22301: The ISO 22301 standard is a global framework designed to assist enterprises in identifying possible risks to core business processes and developing a business continuity management strategy. The ISO 22301 standard assists businesses in developing adequate backup systems and processes to protect against theft, natural catastrophes, disease outbreaks, terrorist attacks, and other exceptional events. The ISO 22301 standard provides the criteria for a company's business continuity management system to be planned, implemented, monitored, reviewed, and improved in order to reduce the effect of interruptions.

ISO 22301 Integrated with ISO 31000 (Framework)

Using Risk Management framework like ISO 31000 in implementation of ISO 22301 Business Continuity Management System organizations can achieve more stability in business. A Integrated procedure is suggested below for the same.

Plan – Do – Check – Act

Plan –

1) Management support

2) Identification of requirements

3) Business continuity policy & objectives

4) Support documents for management system

Do –

5) Risk assessment & treatment

6) Business impact assessment

7) Business continuity strategy

8) Business continuity plan

9) Training & awareness

10) Documentation maintenance

Check –

11) Exercising & testing

12) Post-incident reviews

13) Communication with interested parties

14) Measurement and evaluation

15) Internal audit

Act –

16) Corrective actions

17) Management review

PLAN – Do – Check – Act

1) Management support

It doesn't make sense to start any kind of project (especially this one) if your management isn't willing to invest both financial and human resources, and to do this, they have to see clear benefits – this is where your job begins: with diplomacy.

2) Identification of requirements

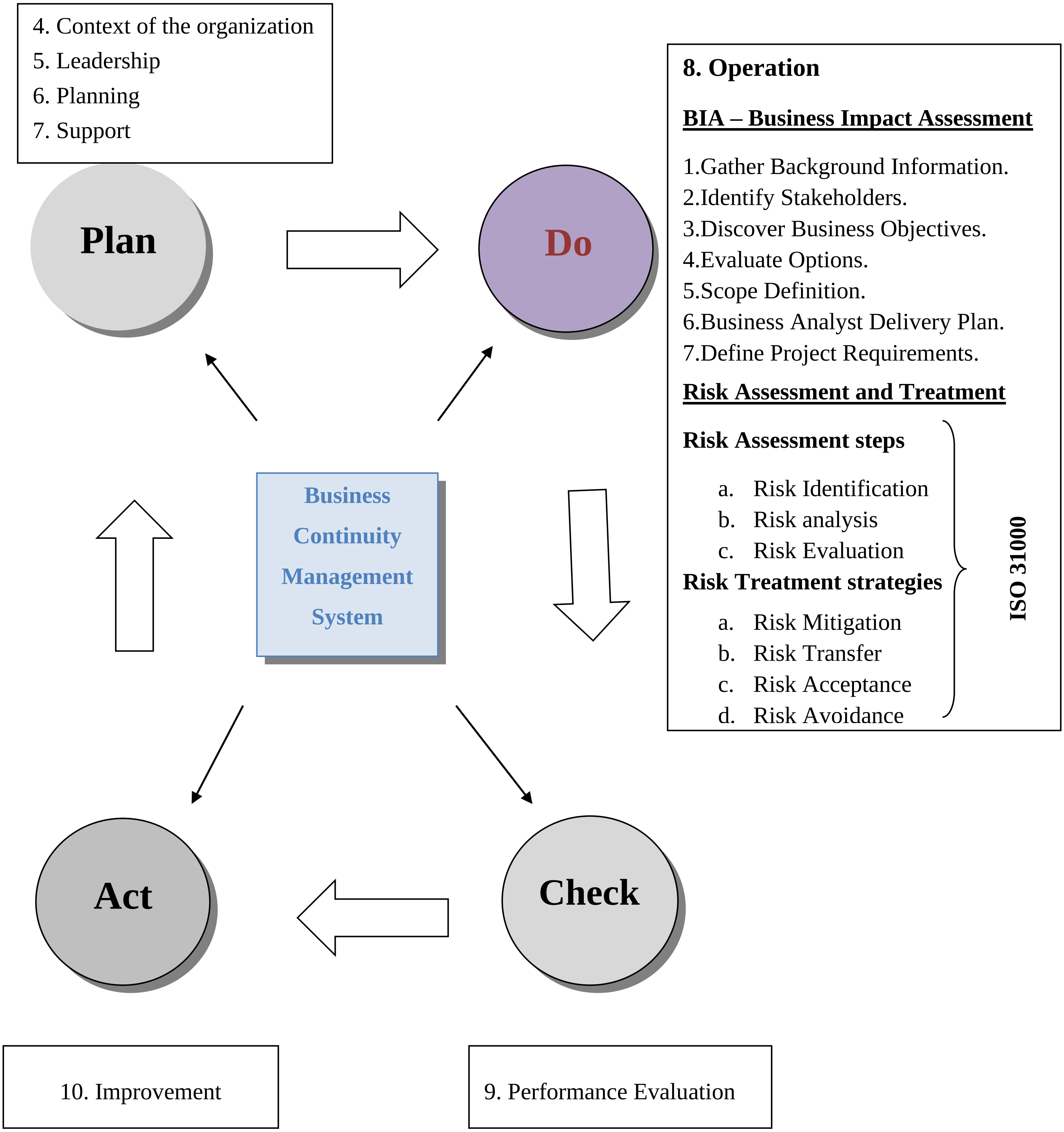
Before taking any concrete steps, you want to make sure you'll be compliant with everything the stakeholders (at least the ones you consider important) want from you. Remember, it is not only the laws and regulations – it is also the requirements in the agreements with your clients (e.g., SLAs), wishes of the owners of the company and the local community, etc. You have to list all of these requirements and define how to communicate with each of the stakeholders/interested parties.

3) Business continuity policy & objectives

Top management needs to define some of the main responsibilities and rules for business continuity, and this is what a business continuity policy is used for, but top management also needs to define exactly what is expected from business continuity – by setting measurable objectives. This is not easy, but is certainly necessary if you want to measure whether business continuity has fulfilled its purpose.

4) Support documents for management system

Management systems, whether business continuity, information security, quality management, or environmental protection, all have in common a set of procedures upon which such systems rely. These procedures are: documents and records control, internal audit, and corrective actions – once you have these in place, you'll find it much easier to run your system.



4. Context of the organization
5. Leadership
6. Planning
7. Support

Plan

Do

8. Operation

BIA – Business Impact Assessment

1.Gather Background Information.
2.Identify Stakeholders.
3.Discover Business Objectives.
4.Evaluate Options.
5.Scope Definition.
6.Business Analyst Delivery Plan.
7.Define Project Requirements.

Risk Assessment and Treatment

Risk Assessment steps

a. Risk Identification
b. Risk analysis
c. Risk Evaluation

Risk Treatment strategies

a. Risk Mitigation
b. Risk Transfer
c. Risk Acceptance
d. Risk Avoidance

ISO 31000

Business Continuity Management System

Act

Check

10. Improvement

9. Performance Evaluation

Plan – DO – Check – Act

5) Risk assessment & treatment

Would you like to be prepared for disruptive incidents? Perhaps even prevent some of them? First you need to find out which incidents can happen, and then define which controls (i.e., safeguards) you can apply to mitigate them – this is basically what risk assessment and treatment is all about.

6) Business impact assessment

Your assessment doesn't finish with risk assessment – you also need to find out two basic things: (1) how quickly you need to recover (before you go bankrupt), and (2) what you need in order to succeed with such recovery. Therefore, the purpose of business impact analysis is to define the recovery time objective (RTO) and required resources.

7) Business continuity strategy

Given the inputs (various requirements, RTO, resources, most likely incidents) you need to figure out how to achieve all this with a minimum level of investment. This can be quite demanding, but without this step your business continuity would be simply a house of cards.

8) Business continuity plan

Actually, there are several types of BC plans – at a minimum, there are incident response plans (they define the initial reaction to an incident), and recovery plans (what needs to be done to start the activities running). All of these need to be based on strategy, because otherwise they would lack the resources (information, technology, people, etc.) to enable such plans.

9) Training & awareness

Having plans in place is not enough – if no one knows how to implement them (or where to find them!), you can rest assure that in case of a real incident they certainly wouldn't work. Therefore, you need to explain to your employees (and third parties who have a role in your plans) not only how to perform certain steps in your plan, but also why this is important in the first place.

10) Documentation maintenance

Written documents have one nasty habit – they become outdated very quickly. Someone leaves the company, or new hires come in; you change the working processes or a technology, you add new products –

all that needs to be reflected in your documentation, especially the plans. Without such changes you wouldn’t be able to implement your plans when they are needed the most.

Plan – Do – CHECK – Act

11) Exercising & testing

However necessary, training is not going to be enough – if you don’t try the plans to discover how they perform in (almost) real situations, you’ll never know where they are deficient. So, performing regular exercising and testing is of paramount importance, and such testing shouldn’t be limited to IT only – everyone, including top management and outsourcing partners and suppliers, must be included.

12) Post-incident reviews

No matter how hard you try, you’ll never be able to prevent incidents from happening; what you can do, however, is learn from such incidents. And you can learn quite a lot – how people react, how ready they are, what improvements are needed in the plans, etc., and most importantly – did you achieve your recovery time objective?

13) Communication with interested parties

This is actually not a 13th step (not that I try to avoid this one), because this is a step that should run in parallel to all the other steps. This is because business continuity heavily depends on regulatory bodies, authorities, owners, employee’s families, media, etc., and you need to keep these interested parties informed as early as when you write your policy and set the objectives, all the way to when an incident actually occurs.

14) Measurement and evaluation

The basic idea here is – it doesn’t make sense to do something unless you know whether you’ve achieved what you wanted or not. In the case of business continuity, the objectives are set in step #3, while finding out if you achieved those objectives must be done through some kind of metrics. It could be something sophisticated like Balanced Scorecard, but could also be as basic as measuring the achievement of RTO during exercising & testing.

15) Internal audit

It is impossible to be 100% objective about your own work. Therefore, someone who is less subjective than you should review your work and suggest improvements – that is what an internal audit is all about. Though it is often considered as overhead, an internal audit is actually very useful when it comes to facing reality.

Plan – Do – Check – ACT

16) Corrective actions

All of us are making daily improvements in the things we are doing, but ISO 22301 wants us to do it systematically – it forces an organization to find out why the problem has happened, and to make sure it never happens again. Or, as the standard says, "ensure that nonconformities do not recur" – it needs to be done systematically, and in a transparent way.

17) Management review

Once all of these steps are performed, top management needs to evaluate them and reach some crucial decisions – like updating the objectives, providing the funding, making larger improvements, etc. After all, it is their ultimate responsibility that the company survives larger incidents.

Implementation of ISO 22301 using ISO 31000 in Pharmaceutical organization (Procedure):

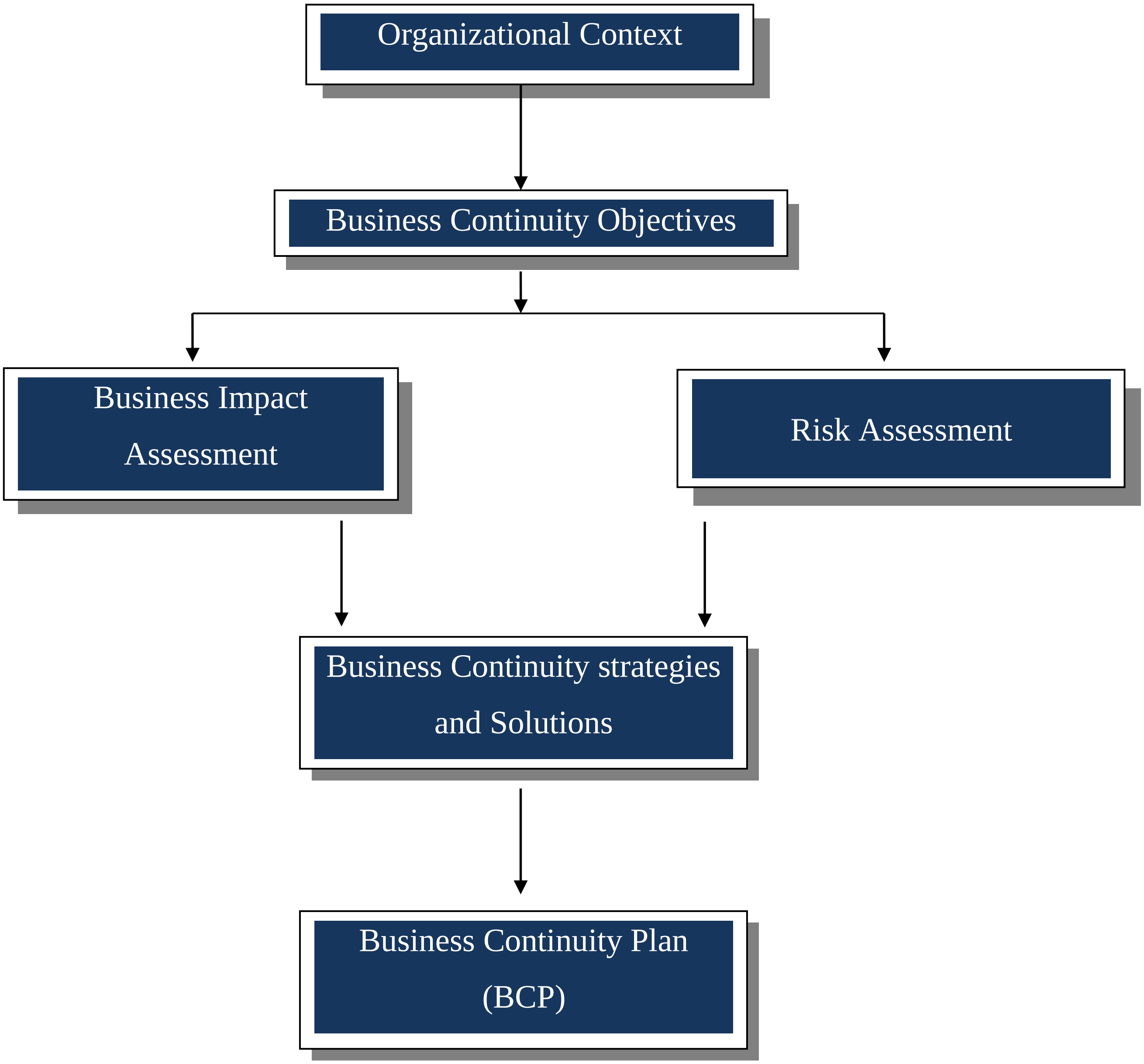
ISO 22301 is the world's first standard that provides a framework for Business Continuity Management System (BCMS). As we know pharmaceutical organizations is one of the most important organizations for us researcher want to implement it with an effective risk management framework like ISO 31000 for more effective business continuity and aims to provide more resilience to organizations to prevent, minimize and recover from disruptive incidents or crisis. Researcher suggested a merged framework below.

- Business Requirements
- Define Scope of Business Continuity
- Establish Product Priority
- Risk Assessment
- Business Impact Analysis
- Business Continuity Plan
- Training & Awareness
- Internal Audit
- Corrective Actions

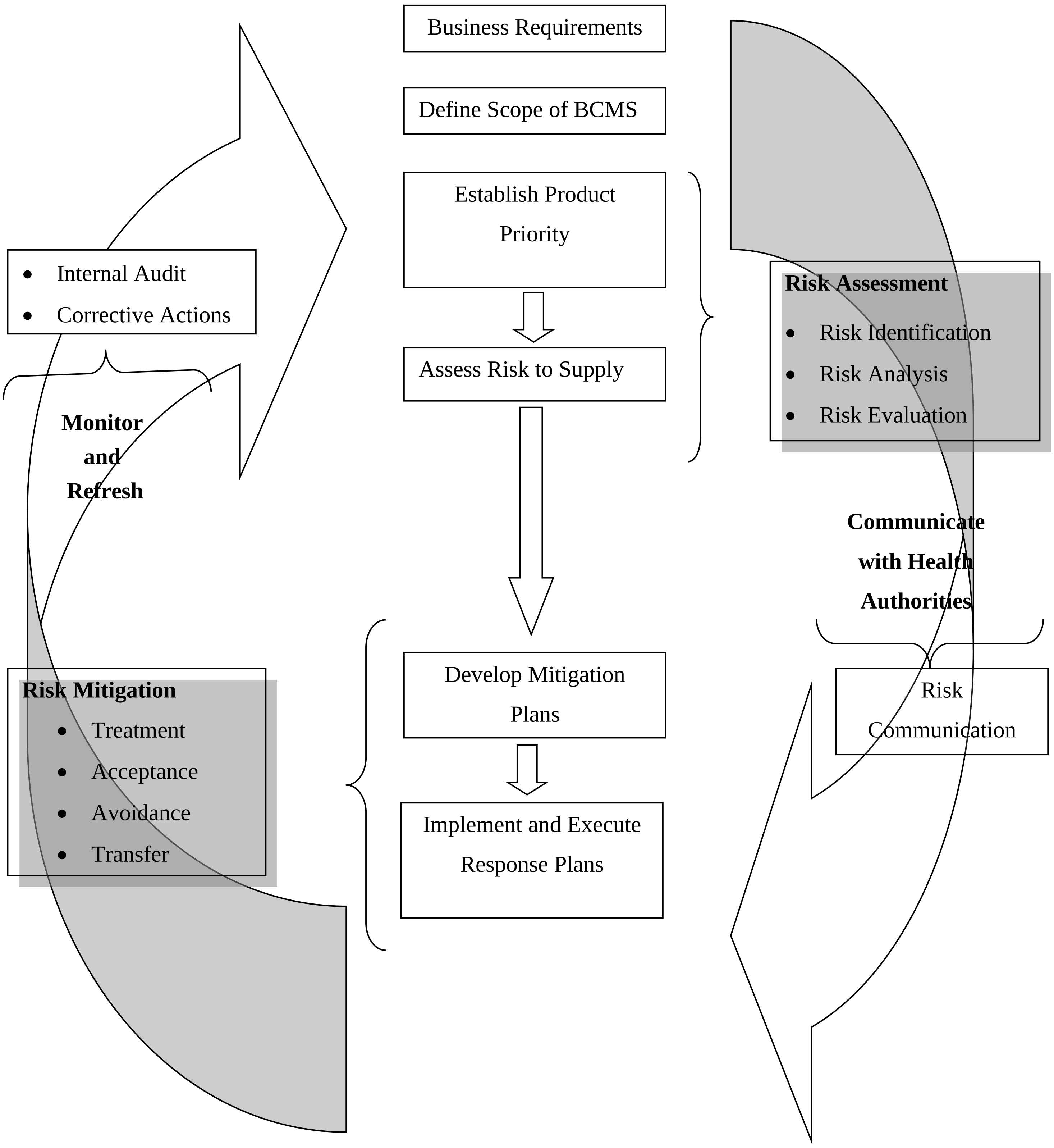
The guidance presented in this article is intended to assist pharmaceutical leaders in striking the right balance between critical patient needs and the business investment for drug shortage prevention measures. In general, the concepts described herein apply to all types of pharmaceutical products, including active pharmaceutical ingredients (APIs), finished drugs, biologics, vaccines, medical devices, and combination products.

At the outset of pursuing robust business continuity planning for preventing drug shortages, it is important to recognize this is not a one-time event. Rather, the four primary activities in business continuity planning—establishing product priority, evaluating risk to supply, developing mitigation options and agility strategy, and implementing response plans—will need to be revisited and adjusted as the product portfolio and business dynamics change over time (Below Figure 1 and 2). Therefore, companies should develop programs to support an ongoing refresh of their business continuity plans.

1) Key activities for strategic business continuity planning for preventing from a disaster,


Organizational Context
Business Continuity Objectives
Business Impact Assessment
Risk Assessment
Business Continuity strategies and Solutions
Business Continuity Plan (BCP)

2) The correlation of the four stages of Business Continuity to Risk Management principles and processes.



Generally, the four stages of business continuity planning will proceed in the order shown in Figure 1; however, as patient needs develop or business or regulatory landscapes change, it may be appropriate to make targeted adjustments within any one of the four stages to ensure the best outcomes.

In each of the four stages, a strong partnership between functional areas within a company will be required for success.

The functional areas typically involved in these activities are as follows:

- Customer relations
- External business partnerships
- Legal
- Manufacturing
- Medical affairs
- Procurement
- Quality
- Regulatory affairs
- Sales and marketing
- Supply chain
- Technical/manufacturing operations

Because many issues and decisions related to business continuity planning will be best addressed after input is considered from multiple functional areas, it is equally important to formally designate a business continuity planning team leader who will have the authority to exercise decisions on behalf of all.

Business Requirements

The organization must identify the prerequisites to establish business continuity and communicate them with all stakeholders and interested parties. An organization must win the support and confidence of all stakeholders to secure a successful implementation of the Business Continuity Management System integrated with Risk Management. Employees are the human capital of any organization, and their active participation plays a significant role.

This section of the document sets out the interested parties that are relevant to the implementation of Business Continuity Management System and their requirements. It also summarizes the applicable legal and regulatory requirements to which the organization subscribes.

An Interested party is defined as “a person or organization that can affected by, or perceive themselves to be affected by a decision or activity”.

The following are defined as interested parties that are relevant to BCMS:

- Stakeholders
- Board of Directors
- Suppliers
- Customer
- Regulatory bodies
- Customer user groups
- Employees of the organization
- Contractors providing services to the organizations
- Trade Unions etc

Applicable Legal and regulatory requirements arise from the following:

- Sarbanes-Oxley Act 2002 (USA)
- GDPR (EU)
- PCI-DSS Compliance
- National and International standards e.g. ISO9001
- Consumer protection legislation

Define Scope of Business Continuity

The management requires defining the policies and responsibilities for business continuity. An organization must determine the scope and objective of business continuity and review the effectiveness and efficiency of the business continuity system.

The defined scope of BCMS takes into account the internal and external factors and the requirements. It also reflects the needs of interested parties and the legal and regulatory requirements that are applicable to the organization.

The SCOPE is defined below in terms of the parts of the organization, products, and services and related activities.

Organizational

The BCMS includes the following parts of the organizations:

Business function

Geographical location

Organizational boundary

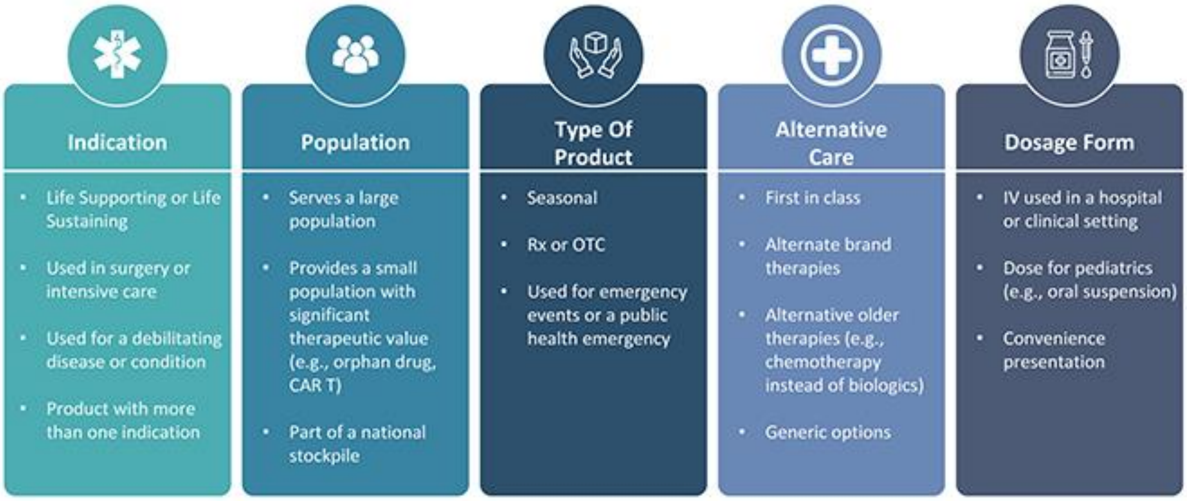
Establishing Product Priority

A foundational activity for business continuity planning is determining the priority of products. Not all products merit the same level of business continuity planning because the impact of supply disruptions is not equal for all products. Considering product priority becomes even more important when the resources required to develop business continuity plans may be constrained. The relative priority of each product will be more reliable if it has been determined by evaluating products individually, as well as across the portfolio of products for which the company is the marketing authorization holder (MAH). This is because there may be important connections between products, often business related, which can influence the priority of an individual product.

Three perspectives primarily drive prioritization of products: therapeutic importance, regulatory requirements, and business significance. Because of the numerous perspectives that must be considered within these three areas when establishing the product priority, the evaluation of priority is best completed as a cross-functional activity and experts in the business areas listed previously should be consulted.

Therapeutic Importance

The medical significance of a product for patients is the most significant consideration when determining that product’s overall priority. There are several ways to differentiate the therapeutic importance of a product (Figure below). Applying one therapeutic assessment globally is usually not sufficient because a product may have different therapeutic value across various markets. Additionally, within or across markets, each dosage form and strength within a product family may not always have the same medical priority. Sometimes, a specific dosage form and strength is developed to provide convenience to the health provider or patient and, as a result, its unavailability may not be as impactful as shortages of other dosage forms and strengths.



Indication

- Life Supporting or Life Sustaining
- Used in surgery or intensive care
- Used for a debilitating disease or condition
- Product with more than one indication

Population

- Serves a large population
- Provides a small population with significant therapeutic value (e.g., orphan drug, CAR T)
- Part of a national stockpile

Type Of Product

- Seasonal
- Rx or OTC
- Used for emergency events or a public health emergency

Alternative Care

- First in class
- Alternate brand therapies
- Alternative older therapies (e.g., chemotherapy instead of biologics)
- Generic options

Dosage Form

- IV used in a hospital or clinical setting
- Dose for pediatrics (e.g., oral suspension)
- Convenience presentation

Regulatory Requirements

“Health authorities (also known as national competent authorities) and health organizations, such as the World Health Organization (WHO), can influence product priority significantly through their definitions of what products may be critical, essential, or life-saving for patients in certain markets. They may also designate medically significant products through a set of criteria or through a list of products. For example, the WHO has long maintained an Essential Medicines List.”[13] Additionally, governments may establish incentives to prioritize products manufactured in a certain market. Typically, health authorities have higher expectations for risk management and business continuity planning for products deemed to be more significant in their market(s).

Currently, “there is no harmonized definition across markets regarding what products are significant to the patients. As a result, it is imperative that pharmaceutical companies have insight into the definitions or lists applicable for the markets where their products are sold, and which products may be assigned to a national

[13] World Health Organization “WHO Model Lists of Essential Medicines” (2020) <https://www.who.int/medicines/publications/essentialmedicines/en> accessed 1st February 2023.

stockpile. Notably, the priority may be dynamic in a market. For example, in a large-scale event, a product that is valuable for emergency use could rapidly become essential and in high demand."[14]

"In addition to considering all regulations and governmental expectations when assessing the priority of a product in each market, it is important for companies to maintain constructive interactions with health authorities."[15] "This will ensure that a company is able to develop a strategic approach to meet requirements across all markets and be poised to engage with the health authorities prior to or at the outset of any significant supply disruption or emergency. Early communication on drug supply challenges, preferably before supply disruptions occur, will maximize the assistance the health authorities may be able to provide to mitigate or prevent a drug shortage."[16]

Business Significance

The commercial relevance of a product should be evaluated from both the standpoint of the company's overall revenue position and the market share of the product. If a product is crucial to a company's revenue stream, there may be little financial room for even a single day of product supply interruption. On the other end of the range, a product might only be produced once or twice a year and sold in very small quantities. A supply gap for a low-volume product might not significantly affect patients or the business, aside from failure-to-provide charges that could be included in supply agreements. However, even an absence of a small-volume product can create significant challenges for patients who may rely on it, which could then generate business challenge for a company if the health care provider or patient reaction to the absence of product generates unfavorable publicity and impacts the overall reputation of the company.

"A market share analysis is an important activity to complete when determining business significance. It should include an analysis of how much market share the company holds for the product, as well as how interconnected the competing suppliers may be to the manufacturing nodes. Generally, if the market for a specific product is divided across at least three manufacturers"[17] a supply disruption from one manufacturer may not make a significant difference to the overall market. However, if the market share is divided

[14] ISPE Drug Shortages Initiative Core Team. "ISPE Offers Platforms to Progress Continuity of Supply of 'Essential' Medicines" (2020) <https://ispe.org/pharmaceutical-engineering/ispeak/ispe-offers-platforms-progress-continuity-supply-essential> accessed 3rd February 2023.

[15] Tomeo, D., K. Hirshfield, and D. L. Hustead. "Engage with Health Authorities to Mitigate & Prevent Drug Shortages." Pharmaceutical Engineering 40, no. 4 (2020): 36–41 <https://ispe.org/pharmaceutical-engineering/july-august-2020/engage-health-authorities-mitigate-prevent-drug> accessed 7th February 2023.

[16] Persaud, N., M. Jiang, R. Shaikh, et al. "Comparison of Essential Medicines Lists in 137 Countries." Bulletin of the World Health Organization 97 (2019):394—404C. doi:10.2471/BLT.18.222448.

[17] World Health Organization. "Medicines Shortages." WHO Drug Information 20, no. 2 (2016): 180–185 <https://www.who.int/medicines/publications/druginformation/WHO_DI_30-2_Medicines.pdf?ua=1> accessed 2nd February 2023.

unevenly and the manufacturer experiencing the supply disruption contributes significantly to the overall industry-wide inventory, the disruption may drive an industry-wide shortage and competitors may have insufficient capacity to increase manufacturing to address the supply gap. Additionally, a product may be a higher priority if any risks to supply would likely impact multiple suppliers (e.g., all companies use the same raw material supplier), and very quickly create an industry-wide gap.

Lastly, connections between products, either within the portfolio of one company (i.e., one MAH holder) or connections with a partner company, may need to be considered when establishing the business significance for each product. One product may be interdependent with other products due to marketing, regulatory quality, or manufacturing supply requirements or strategies. Depending on the nature of the connection, a product that may otherwise be of lower priority may become more significant because interruption in its supply may impact other products the company markets or the company’s partnerships with other companies.

Risk Assessment

An organization requires performing a risk assessment to determine potential risks and opportunities and address them accordingly. According to ISO 31000, **Risk management** process is a “systematic application of management policies, procedures and practices to the tasks of communication, consultation, establishing the context, identifying, analyzing, evaluating, treating, monitoring and reviewing risk”.

The Risk Assessment consists in the identification of hazards, analysis and evaluation of risks associated with exposure to those hazards Risk assessment defines with three fundamental questions.

a) Risk Identification address what might go wrong.
b) Risk Analysis, to analyze the risk involved.
c) Risk evaluation, comparing the risk identification and analyze the risk against the criteria.

Any potential risk identified shall be assessed qualitatively and quantitatively. The Risk assessment shall be done in a cross functional committee to read upto a common rating.

- Qualitatively: The risk shall be categorized into “High” “Medium” and “Low”
- Quantitatively: The risk shall be provided with numerical value “1” “2” “3” “4” “5”.

Sr.No.	Risk Identification No.	Risk Description	Quantitative Score	Qualitative Score	Remarks
1.	R001/2023				
2.	R002/2023				
3.	R003/2023				
4.					
5.					

Business Impact Analysis

It defines requirements for an organization to find out two things. That is:

1. Effectiveness of the recovery plan
2. Recovery time objectives are requirements for the successful recovery process.

Business Continuity Plan

There are several kinds of business continuity plans. These are:

1. Incident response plan
2. Recovery plan

Risk Treatment

Risk control includes decision making to reduce and/or accept risks. The purpose of risk control is to reduce the risk to an acceptable level. The amount of effort used for risk control should be proportional to the significance of the risk. Decision makers might use different processes, including benefit-cost analysis, for understanding the optimal level of risk control. Risk control might focus on the following questions:

- Is the risk above an acceptable level?
- What can be done to reduce or eliminate risks?
- What is the appropriate balance among benefits, risks and resources?
- Are new risks introduced as a result of the identified risks being controlled?

Risk reduction focuses on processes for mitigation or avoidance of quality risk when it exceeds a specified (acceptable) level. Risk reduction might include actions taken to mitigate the severity and probability of harm. Processes that improve the detectability of hazards and quality risks might also be used as part of a risk control strategy. The implementation of risk reduction measures can introduce new risks into the system or increase the significance of other existing risks. Hence, it might be appropriate to revisit the risk assessment to identify and evaluate any possible change in risk after implementing a risk reduction process.

Risk acceptance is a decision to accept risk. Risk acceptance can be a formal decision to accept the residual risk or it can be a passive decision in which residual risks are not specified. For some types of harms, even the best quality risk management practices might not entirely eliminate risk. In these circumstances, it might be agreed that an appropriate quality risk management strategy has been applied and that quality risk is reduced to a specified (acceptable) level. This (specified) acceptable level will depend on many parameters and should be decided on a case-by-case basis.

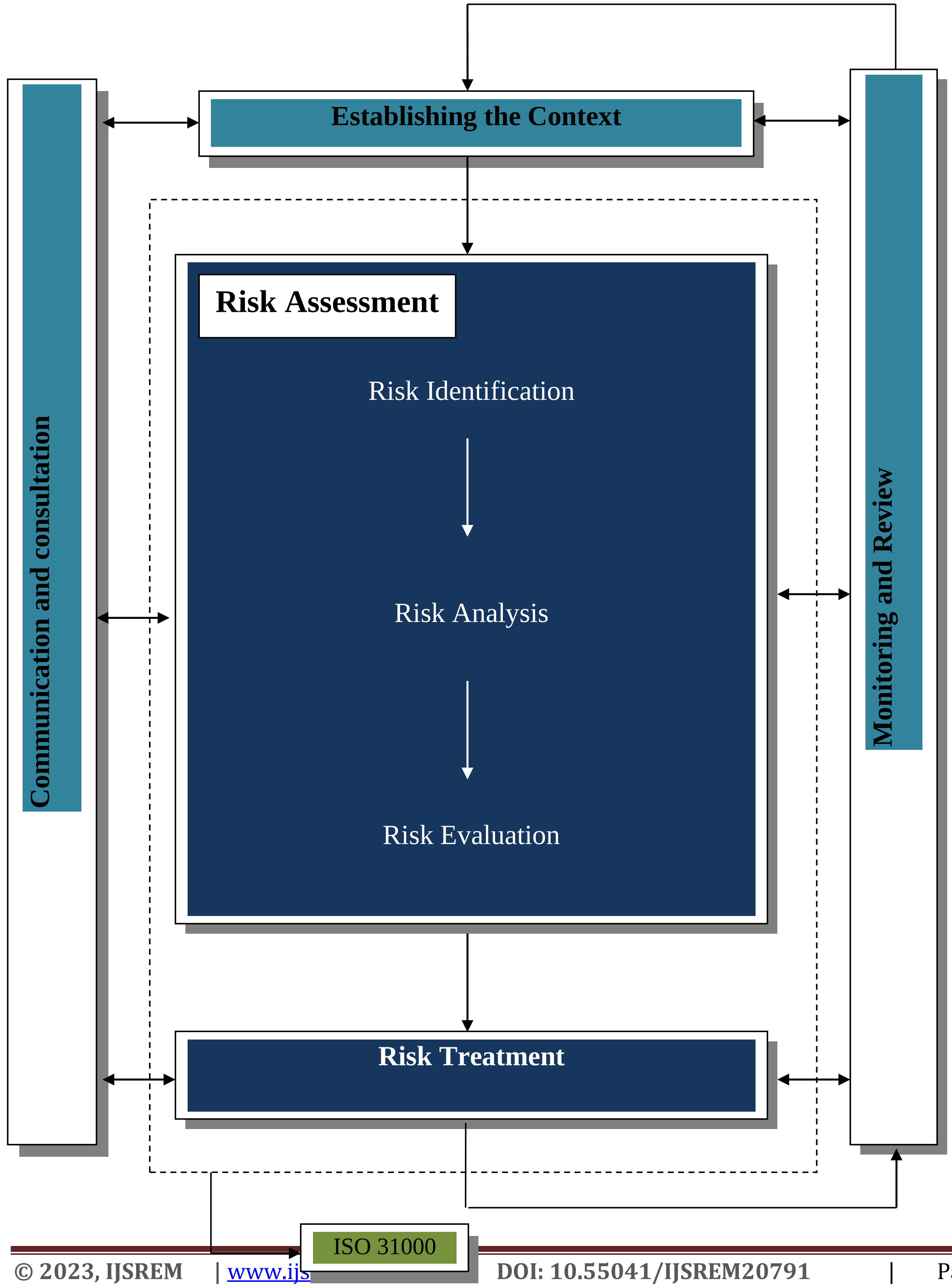
Risk Transfer

Risk transfer refers to a risk management technique in which risk is transferred to a third party. In other words, risk transfer involves one party assuming the liabilities of another party. Purchasing insurance is a common example of transferring risk from an individual or entity to an insurance company.

Methods of Risk Transfer

1. **Insurance policy** - As outlined above, purchasing insurance is a common method of transferring risk. When an individual or entity is purchasing insurance, they are shifting financial risks to the insurance company. Insurance companies typically charge a fee – an insurance premium – for accepting such risks.
2. **Indemnification clause in contracts** - Contracts can also be used to help an individual or entity transfer risk. Contracts can include an indemnification clause – a clause that ensures potential losses will be compensated by the opposing party. In simplest terms, an indemnification clause is a clause in which the parties involved in the contract commit to compensating each other for any harm, liability, or loss arising out of the contract.

Risk Identification No.	**Risk Score**	**Corrective action**	**Preventive action**	**Responsibility**	**Remark**
R001/2023					
R002/2023					
R003/2023					


Establishing the Context
Communication and consultation
Monitoring and Review
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
ISO 31000

Training & Awareness

A business continuity plan prepares the business for an unexpected incident or crisis. It requires providing necessary training to employees so that they know how to save their lives during an incident. It also instructs the organization to execute mock drills and develop recovery plans.

Risk communication is the sharing of information about risk and risk management between the decision makers and others. Parties can communicate at any stage of the risk management process. The output/result of the quality risk management process should be appropriately communicated and documented. Communications might include those among interested parties; e.g., regulators and industry, industry and the patient, within a company, industry or regulatory authority, etc. The included information might relate to the existence, nature, form, probability, severity, acceptability, control, treatment, detectability or other aspects of risks to quality. Communication need not be carried out for each and every risk acceptance. Between the industry and regulatory authorities, communication concerning quality risk management decisions might be effected through existing channels as specified in regulations and guidances.

Internal Audit

An organization must conduct an internal audit to identify the weak areas and shortcomings. An internal audit allows organizations to achieve the desired outcomes and eliminate factors that might cause unintended results.

Corrective Actions

After conducting an internal audit, the organization must implement corrective actions to eliminate shortcomings and mitigate factors that cause undesired outcomes.

Conclusion

This article summarizes key stages and decision points for successful business continuity planning to mitigate and prevent pharmaceutical organization from disaster, and the foundational concepts described are aligned with ISO 31000, Enterprise Risk Management. The approach was developed from across academic experience and has benefited from preliminary learnings from the Internship. It will be reviewed and updated, if required, based on further learnings emerging from industry interactions and regulatory feedback.

The circumstances surrounding COVID-19 are no different from other incidents in that they each bring particular difficulties and chances for improvement. One of the many effects of the COVID-19 pandemic has been that businesses have had to rely more heavily on business continuity planning in order to be more adaptable and narrow their attention on ways to guarantee ongoing delivery of essential medications. It will be crucial to know which business continuity strategies were successful and which failed once we have overcome these challenging circumstances. In order to improve the overall effectiveness of the supply chain, it will be crucial to determine whether manufacturing or commercial practises created during the pandemic may be implemented regularly. Exciting new directions and enduring solutions for preventing and mitigating drug shortages may be achieved, and this constant evolution in the business continuity planning space should always be embraced. The researcher is open to proposals for best practices to improve pharmaceutical organizations' business continuity in the case of an actual or potential disaster.

Suggestions

- "Risk Management in the Pharmaceutical Industry: An Integrated Approach using ISO 22301 and ISO 31000 Standards" - This research paper can explore the benefits of integrating ISO 22301 and ISO 31000 standards for risk management in a pharmaceutical organization. It can provide a detailed analysis of the implementation process, challenges faced, and lessons learned from the integration of these standards.
- "Enhancing Business Continuity in Pharmaceutical Organizations: A Comparative Study of ISO 22301 and ISO 31000 Standards" - This research paper can compare and contrast the effectiveness of ISO 22301 and ISO 31000 standards in enhancing business continuity in a pharmaceutical organization. It can provide insights into the strengths and weaknesses of these standards and suggest best practices for their implementation.
- "Impact of ISO 22301 and ISO 31000 Standards on Pharmaceutical Organizations: A Case Study Analysis" - This research paper can present a case study analysis of a pharmaceutical organization

that has implemented ISO 22301 and ISO 31000 standards. It can examine the impact of these standards on the organization's risk management, business continuity, and overall performance, and provide recommendations for other organizations looking to implement these standards.

Future Scope:

- Further research can be conducted to explore the potential of integrating other ISO standards with ISO 22301 and ISO 31000 for enhanced risk management and business continuity in pharmaceutical organizations.
- A comparative study of the effectiveness of ISO 22301 and ISO 31000 standards in pharmaceutical organizations across different geographical regions can be conducted to identify regional differences and similarities in their implementation and impact.
- Research can be conducted to examine the role of emerging technologies such as artificial intelligence, blockchain, and Internet of Things (IoT) in enhancing risk management and business continuity in pharmaceutical organizations implementing ISO 22301 and ISO 31000 standards.

BIBLIOGRAPHY

BOOKS/E-BOOKS

- Chen Thomas M., "Information Security and Risk Management" Southern Methodist University, USA "Encyclopedia of Multimedia Technology and Networking" (2009) page 668 2nd ed., Idea Group Publishing
- Snedaker Susan, "Business Continuity & Disaster Recovery" Syngress Publishing, Inc "Risk Assessment" < https://b-ok.asia/book/486981/3b5df9> accessed on 29th October
- Snedaker Susan, "Business Continuity & Disaster Recovery" Syngress Publishing, Inc "Business Continuity & Disaster Recovery" < https://b-ok.asia/book/486981/3b5df9> accessed on 29th October
- W. Michael and W. Lawrence, "The Disaster Recovery Handbook" Amacom (2018) <http://www.amacombooks.org/go/DisasterRecovery3E> accessed on 29th October 2022.

RESEARCH PAPERS AND ARTICLES

- Anir Hanane, F. Mounia and K. Meryem, "Towards an approach for Integrating Business Continuity Management into Enterprise Architecture" International Journal of Computer Science & Information Technology (IJCSIT) (2019) <https://aircconline.com/ijcsit/V11N2/11219ijcsit01.pdf> accessed on 22nd October 2022
- B. Saiful, N.S. Ganthan and S. Bharanidharan, "Business Impact Analysis Ontology for Information Technology Continuity Management" (2014) <https://www.academia.edu/40371152/Business_Impact_Analysis_Ontology_for_Information_Technology_Continuity_Management > accessed on 25th October 2022
- Ko Andrea, "Risks Evaluation and IT Audit Aspects of Business Intelligence Solutions" Academia (2014) <https://www.academia.edu/10744178/Risks_Evaluation_and_IT_Audit_Aspects_of_Business_Intelligence_Solutions> accessed on 26th October 2022

- M. Flys I, M.S Sviderok “Project Approach to Activity Management of the Land Artillery Unit in a Combined Battle” Science Review, (2018) <https://doi.org/10.31435/rsglobal_sr/01072018/5920> accessed on 21st October 2022
- M. Urbaniak, "Risk factors affecting relations with suppliers" LogForum (2018) <http://doi.org/10.17270/J.LOG.2019.333> accessed on 21st October 2022
- Viacheslav Lebedinets, Olena Romelashvili and Serhiy Stepanenko, “Status of the Problem of Falsified Pharmaceutical Products on the World and National Pharmaceutical Markets” (2018), Science Review, <https://doi.org/10.31435/RSGLOBAL_SR/01072018/5922> accessed on 21st October 2022

WEBSITES

- IBEF (India Brand Equity Foundation), “Indian Pharmaceutical Industry” Aug 2022 <https://www.ibef.org/industry/pharmaceutical-india> accessed on 29th October 2022
- Jain Sudarshan, secretary general, Indian Pharmaceutical Alliance (IPA), Business Standard September 2022, <https://www.business-standard.com/article/companies/indian-pharma-industry> accessed on 28th October 2022
- TuneEngineering, "Business Continuity in Pharma: the role of Risk Management" 4TE Team (2022) <https://blog.4tuneengineering.com/business-continuity-in-pharma-the-role-of-risk-management/> accessed on 6th November 2022
- World Health Organization, "WHO guidance for business continuity planning" (2022) <https://apps.who.int/iris/bitstream/handle/10665/324850/WHO-WHE-CPI-2018.60-eng.pdf> accessed on 6th November 2022