Risk, Crisis and Security Management (CC5052NI)

Course Work 1

Topic Chosen: Risk Management and Risk Control

Submitted By: Manish Giri
Student ID Number: 16034959

Submitted To: Lecturer: Saroj Lamichane
Submission Date: 1/8/2018

Marking Scheme

Items	***Marks Awarded***	***Feedback***
1) Technical content [Maximum 70 Marks]:		
Rationale and Objectives of the chosen topic [Maximum 15 Marks]:		
Abstract Content [Maximum 10 Marks]:		
Literature Review[Maximum 20 Marks]: NOTE: Relevance of the resources (i.e. in terms of useful of the resources referred to within the context of the topic), breadth and depth of the content reviewed.		
Identification of Issues (use of examples / case studies), Analysis and Reflection: [Maximum 25 Marks] NOTE: Identify issues relating to the techniques being reviewed, compare and analyse, and reflect on what you have learnt about these techniques by undertaking this task.		
2) Report Format[Maximum 15 Marks]: Overall structure – organisation of material; quality of documentation; and citing the correct reference(s) in appropriate sections of the report using a chosen referencing style. The report should have an abstract, introduction, main body, conclusions, references, face page, contents page and page number etc.		
3) Oral Presentation[Maximum 15 Marks]: NOTE: You should demonstrate good understanding of the technical contents of the report. The quality of slides and delivery aspects (speed, time control, etc.) will be assessed.		

Acknowledgement

I would like to express my special thanks of gratitude to my teacher Mr. Saroj Lamichane gave me the golden opportunity to do this wonderful project on the topic Risk Management and Control, which also helped me in doing a lot of Research and I came to know about so many new things I am really thankful to them.

Abstract

This course work was assgined to us by the college which requires us to prepare a report on one of the given topic. The module Risk, Crisis and Security Management was handled by our module leader Mr.Saroj Lamichanne.

This report contains the basic of the concept of Risk Management/Risk control. This report covers the risk management approaches and risk implementation strategies that were taught by our tutor as well as relevant case studies related to the topic. Personal reviews and Analysis on the topic are also included.

Table of Contents

Table of Figures

1. Introduction

1.1 Overview

Risk Management is the process of identifying, assessing and controlling threats for a particular company or organization. It is a techniques that utilizes findings from risks assessments which involves identifying potential risk factors in a firm's operation, such as technical and non-technical aspects of business, financial policies and other policies which may impact the well-being of the firm.

1.2 Aims and Objectives

This report briefly explains about the risk management/risk control. In this report we will get the detailed knowledge about the history of risk management, preventive measures to avoid potential risks which can easily harm an organization and we will also know how important risk management today is. We will learn about the effects of bad management of risk and we will also know the ways to secure the data and information of an organization. We will also do the case study of the topic risk management/risk control.

1.3 Problem Statements

The uncertain economic times of the past few years have had a major effect on how companies operate these days. Companies that used to operate smoothly with the help of forecasts and projections now refrain from making business judgements that are set in stone. Now, companies have a renewed focus: to manage risk.

2. Background

2.1 Risk And Its History

The concept of risk management was started after 1955. Since the early 1970s, the concept of financial risk management evolved considerably. Risk Management has become less limited to market insurance coverage, which is known as a competing protection tool that complements several other risk management activities. After the Second World War, huge number of companies carrying diversified portfolios of physical assets began to develop self-insurance against risks which they covered effectively as insurers for many small risks. (Dionne, 2013)

2.2 Risk Management Approaches

2.2.1 Risk Identification

The process of determining risks that could potentially prevent the program, enterprise or investment from achieving its objectives is called risk identification.

In an organization, the project team should review the program scope, cost estimates , schedule, technical maturity, key performance parameters, performance challenges, stakeholder expectations vs. current plan, external and internal dependencies, implementation challenges, integration, interoperability, supportability, supply-chain vulnerabilities, ability to handle threats, cost deviations test event expectations, safety, security and more. (The MITRE Institute, n.d.)

2.2.2 Risk Management

Risk is the chance of something happening that will have an impact upon objectives. Risk is often specified in terms of events and consequences that may flow from them.

Risk management is a management process that is taken before the occurrence of the (risk) event. The result of risk management is a collection of recommendations for a risk prevention/mitigation plan, and, preferably, an associated implementation of the plan. (Tech Target, n.d.)

2.2.3 Cost Benefit Analysis (CBA)

Cost benefit analysis is a systematic approach to estimating the strengths and weaknesses of alternatives and used to determine options that provide the best approach to achieve benefits while preserving savings.

To determine if an investment/decision is sound (justification/feasibility) – verifying whether its benefits outweigh the costs, and by how much is one of the main purpose of CBA.

CBA = ALE (prior) – ALE (post) – ACS

ALE (prior to control) is the annualized loss expectancy of the risk before the implementation of the control. ALE (post control) is the ALE examined after the control has been in place for a period of time. ACS is the Annual Cost of the Safeguard. (Investopedia, n.d.)

2.2.3 Feasibility Studies

To determine the viability of a business venture in a specific area or sector of business is called feasibility study.

By conducting a proper feasibility study, the target audience can be clearly identified along with their purchasing power. It provides in-depth details about the business to determine if and how it can succeed, and it serves as a valuable tool for developing a winning business plan. (Investopedia, n.d.)

2.3 Implementation of Risk Control Strategies

Some of the techniques which should be implemented in order to reduce the risks which may harm the organization are as follows. (Tutsplus, n.d.)

2.3.1 Avoidance

- Avoidance should be implemented in-order to control the financial consequences of threatening events and protect an information asset and accept the loss when it occurs.
- A risk avoidance attempts to minimize vulnerabilities which can pose a threat.
- For example, let us suppose a factory and the chemical used to manufacture the goods is dangerous for the workers then to avoid this risk, the owner finds a safe substitute chemical to protect the workers. (Tutsplus, n.d.)

2.3.2 Transference

- Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.

- This may be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations purchasing insurance, or by implement in service contracts with providers. (Tutsplus, n.d.)

2.3.3 Mitigation

Mitigation is the control approach that attempts to reduce, by means of planning and preparation, the damage caused by the exploitation of vulnerability. This approach includes three types of plans:

- Incident Response Plan (IRP)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)

Mitigation depends upon the ability to detect and respond to an attack as quickly as possible. (Tutsplus, n.d.)

2.3.4 Acceptance

It indicates that the organization is willing to accept the level of risk associated with a given activity or process. Generally, but not always, this means that the outcome of the risk assessment is within tolerance. There may be times when the risk level is not within tolerance but the organization will still choose to accept the risk because all other alternatives are unacceptable (Tutsplus, n.d.)

2.4 Implementation of CIA and AAA

Confidentiality, integrity and availability which is also known as the CIA triad, is a model designed to guide policies for information security within an organization. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Authentication, authorization, and accounting is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. (Buhlz_I, 2017)

2.5 Risk Elimination

It is better to control risk , there are some of the methods which can be implemented in order to prevent risk of loss of data and information of an organization.

- Purge data policy
- Monitoring BYOD program
- Securing Networks
- Updating software's with all patches and updates (Rouse, 2011)

3. Case Studies

3.1 A Case Study of Robust Risk Management : Medical Devices

3.1.1 Summary

This case study presents an example of a robust risk management program, based on ISO14971, for a Continuous Positive Airway Pressure (CPAP) medical device used to treat Obstructive Sleep Apnea (OSA) is discussed below.. The main elements of this risk management process, i.e. risk analysis, risk evaluation, risk control and postproduction information, are generally documented in a risk management file. This risk management file is required to get FDA approval to market a medical device (prior to product launch). (Hegde, 2011)

An overview of risk management activities (13 stepsoutlined in ISO14971 standard), performed in the different phases of the risk management process (i.e. risk analysis, risk evaluation, risk control and post-production information phase), is represented graphically below.

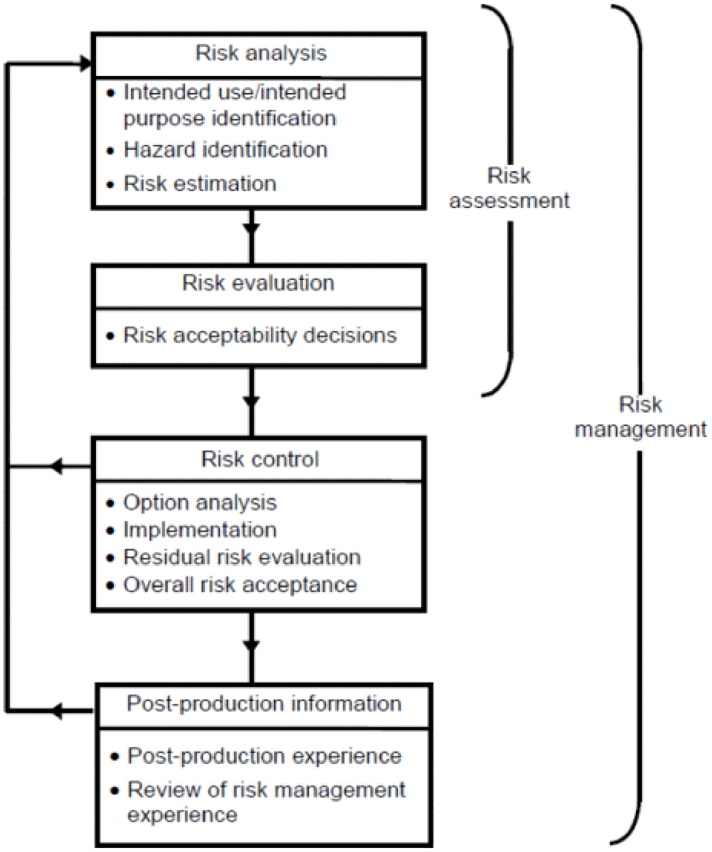

Risk analysis
• Intended use/intended purpose identification
• Hazard identification
• Risk estimation
Risk evaluation
• Risk acceptability decisions
Risk control
• Option analysis
• Implementation
• Residual risk evaluation
• Overall risk acceptance
Post-production information
• Post-production experience
• Review of risk management experience
Risk assessment
Risk management

Figure 1 13 stepsoutlined in ISO14971 standard

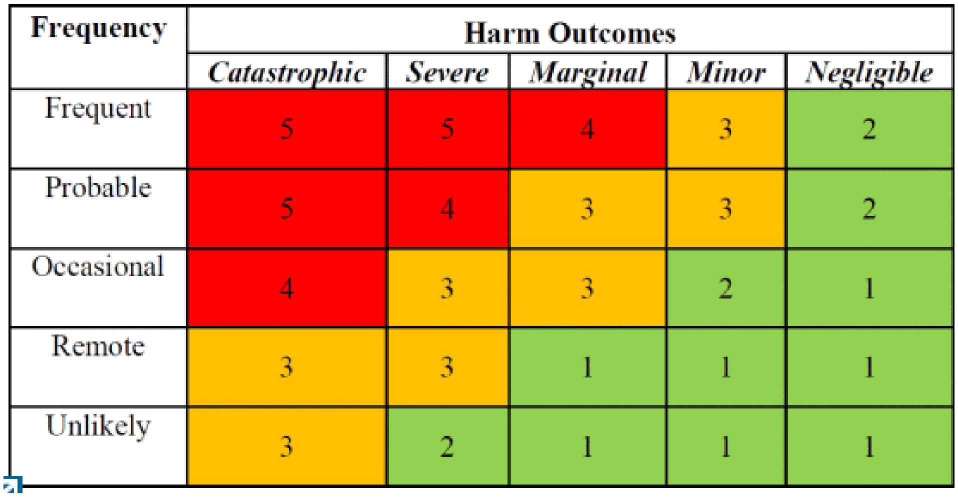
3.1.2 Risk Management Program (based on ISO14971)

The first task in the risk management program was to write a risk management plan that spanned the life of the product from the design and development phase to the disposal phase. The plan included: (Hegde, 2011)

- Risk acceptability criteria for determining acceptable risk
- The scope of the planned risk management activities, and the life-cycle phases for which each element of the plan was applicable
- Assignment of responsibilities and authorities
- Requirements for review of the risk management activities
- Verification activities for risk control measures
- Activities related to collection and review of relevant production and post-production information

3.1.3 Risk Acceptability Criteria

The figure below is an example of the risk acceptability criteria used in this program. Descriptions, definitions, criteria and acceptability explanations are located directly below the figure.



Frequency	**Harm Outcomes**				
	Catastrophic	***Severe***	***Marginal***	***Minor***	***Negligible***
Frequent	5	5	4	3	2
Probable	5	4	3	3	2
Occasional	4	3	3	2	1
Remote	3	3	1	1	1
Unlikely	3	2	1	1	1

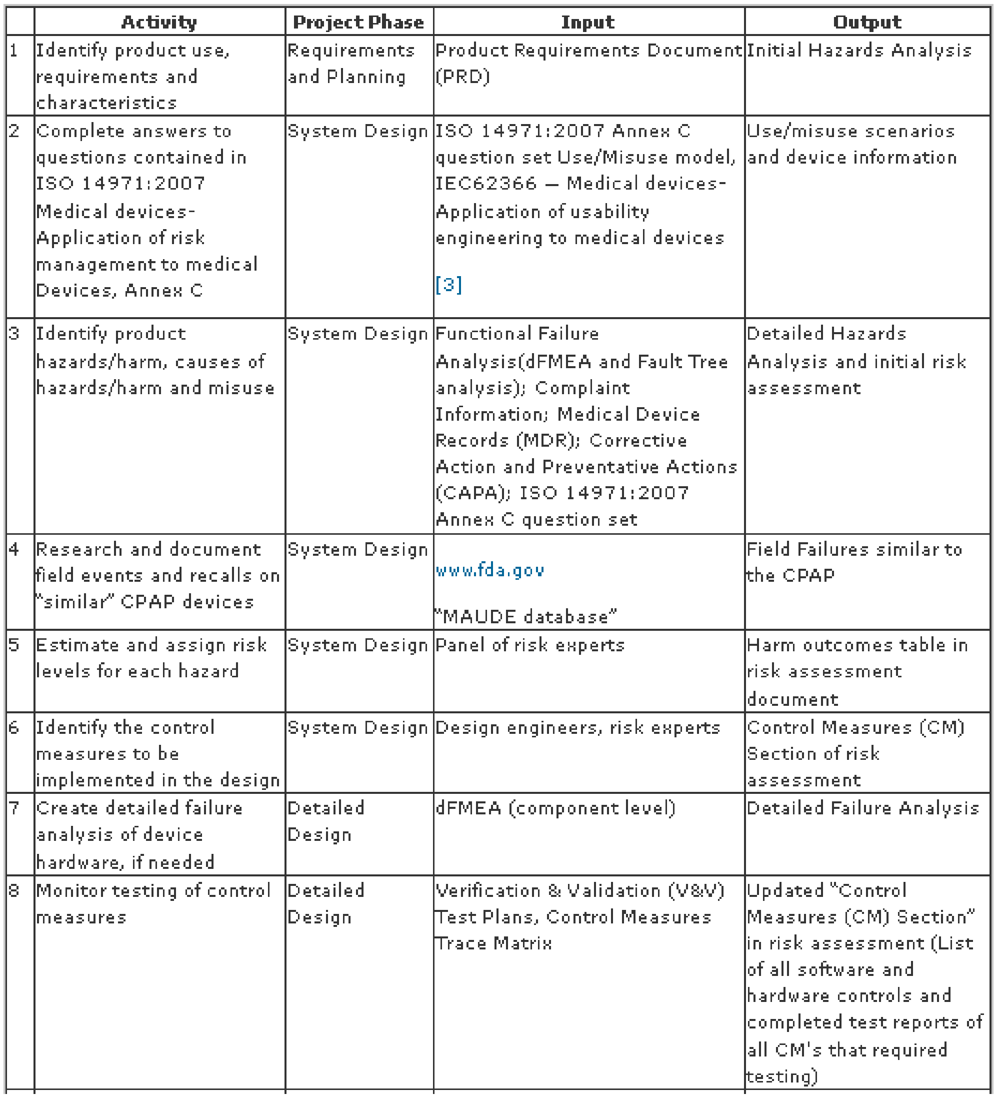
Figure 2 Risk Acceptability Criteria

Criterias:

1. Risk can be accepted by project team even in the absence of control measures
2. Risk can be accepted by project team upon verification of implementation of control measures
3. Risk can be accepted with the approval of top management needed on the basis of risk benefit justification

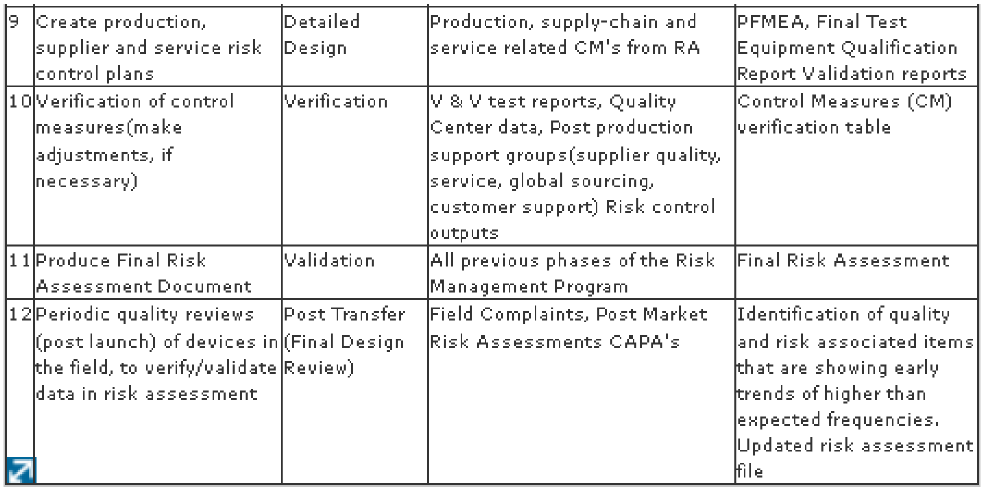
3.1.4 Risk Management Activities

A list of risk management related activities (based on 13 steps outlined in ISO14971) that were performed in the different phases of the CPAP device development project is given below in .These activities were useful in identifying hazards, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls during the entire life cycle of the product. (Hegde, 2011)



	Activity	Project Phase	Input	Output
1	Identify product use, requirements and characteristics	Requirements and Planning	Product Requirements Document (PRD)	Initial Hazards Analysis
2	Complete answers to questions contained in ISO 14971:2007 Medical devices- Application of risk management to medical Devices, Annex C	System Design	ISO 14971:2007 Annex C question set Use/Misuse model, IEC62366 — Medical devices- Application of usability engineering to medical devices [3]	Use/misuse scenarios and device information
3	Identify product hazards/harm, causes of hazards/harm and misuse	System Design	Functional Failure Analysis(dFMEA and Fault Tree analysis); Complaint Information; Medical Device Records (MDR); Corrective Action and Preventative Actions (CAPA); ISO 14971:2007 Annex C question set	Detailed Hazards Analysis and initial risk assessment
4	Research and document field events and recalls on "similar" CPAP devices	System Design	www.fda.gov "MAUDE database"	Field Failures similar to the CPAP
5	Estimate and assign risk levels for each hazard	System Design	Panel of risk experts	Harm outcomes table in risk assessment document
6	Identify the control measures to be implemented in the design	System Design	Design engineers, risk experts	Control Measures (CM) Section of risk assessment
7	Create detailed failure analysis of device hardware, if needed	Detailed Design	dFMEA (component level)	Detailed Failure Analysis
8	Monitor testing of control measures	Detailed Design	Verification & Validation (V&V) Test Plans, Control Measures Trace Matrix	Updated "Control Measures (CM) Section" in risk assessment (List of all software and hardware controls and completed test reports of all CM's that required testing)

Figure 3 Risk Management Activities



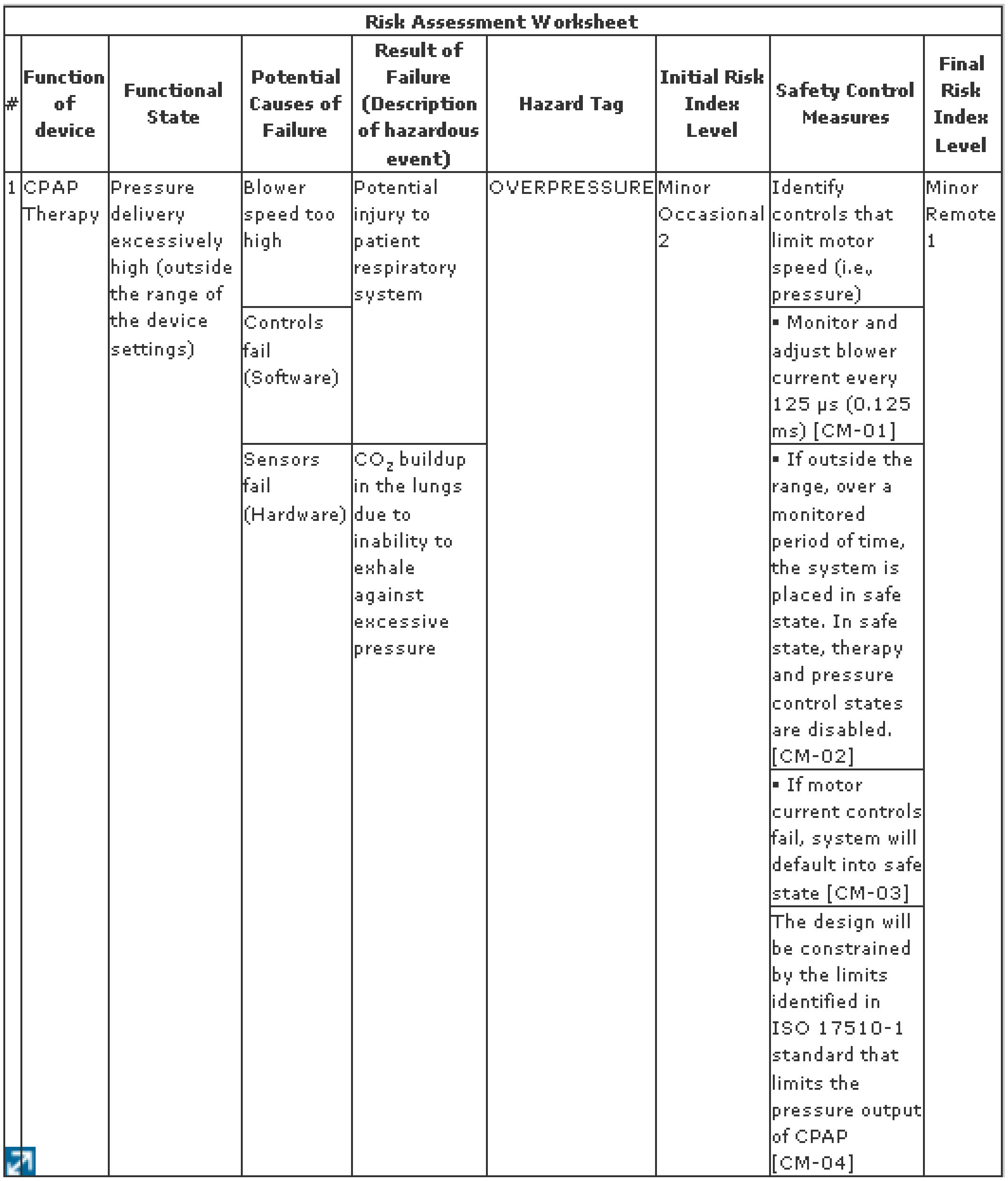
9	Create production, supplier and service risk control plans	Detailed Design	Production, supply-chain and service related CM's from RA	PFMEA, Final Test Equipment Qualification Report Validation reports
10	Verification of control measures(make adjustments, if necessary)	Verification	V & V test reports, Quality Center data, Post production support groups(supplier quality, service, global sourcing, customer support) Risk control outputs	Control Measures (CM) verification table
11	Produce Final Risk Assessment Document	Validation	All previous phases of the Risk Management Program	Final Risk Assessment
12	Periodic quality reviews (post launch) of devices in the field, to verify/validate data in risk assessment	Post Transfer (Final Design Review)	Field Complaints, Post Market Risk Assessments CAPA's	Identification of quality and risk associated items that are showing early trends of higher than expected frequencies. Updated risk assessment file

Figure 4 Risk Management Activities

3.1.5 Risk Management File

The risk management file, submitted to the FDA, included the risk management plan, the initial hazard analysis, use/misuse model, detailed hazard analysis, dFMEA, risk assessment, control measures trace matrix, control measures verification report, production-supplier-service risk control plans, post market risk assessment plan and a final risk report. . (Hegde, 2011)

The risk assessment worksheet template, used in this program, is given in table below :



Risk Assessment Worksheet

#	Function of device	Functional State	Potential Causes of Failure	Result of Failure (Description of hazardous event)	Hazard Tag	Initial Risk Index Level	Safety Control Measures	Final Risk Index Level
1	CPAP Therapy	Pressure delivery excessively high (outside the range of the device settings)	Blower speed too high	Potential injury to patient respiratory system	OVERPRESSURE	Minor Occasional 2	Identify controls that limit motor speed (i.e., pressure)	Minor Remote 1
			Controls fail (Software)				▪ Monitor and adjust blower current every 125 μs (0.125 ms) [CM-01]	
			Sensors fail (Hardware)	CO_2 buildup in the lungs due to inability to exhale against excessive pressure			▪ If outside the range, over a monitored period of time, the system is placed in safe state. In safe state, therapy and pressure control states are disabled. [CM-02]	
							▪ If motor current controls fail, system will default into safe state [CM-03]	
							The design will be constrained by the limits identified in ISO 17510-1 standard that limits the pressure output of CPAP [CM-04]	

Figure 5 Risk Management File

3.2 Case Review

Using the risk management process outlined in ISO14971 standard as a guideline to manage risk can ensure the design and deployment of a safe product, with an acceptable level of risk. The concepts, processes and risk management activities discussed in this paper can be applied to non-medical fields as well.

4. Conclusion

By breaking down all reality said above thus obviously the scope of risks that association might be uncovered has been investigated. Distinctive risks which association may confront have been presented and in particular actualized hazard administration process have been analyzed in detail. This report gives an outline of the risk administration process which ought to be inserted in the operations and risk management of each association.

4.1 Personal Reflection

Understanding how to not only find by correctly use my found sources for my papers improved my efficiency of writing dramatically because I did not have to spend a great amount of time figuring out how to correctly apply and use the information from my sources in my papers without having to worry about plagiarizing someone else's work.

4.2 Social and Ethical Issues

Administration of risk inside social work rehearse is basic to guarantee the conveyance of protected, successful and innovative practice. Investigation of literature in regards to hypothesis and routine with regards to the risk administration and moral issues in social work and expert experience enable us to recognize the most widely recognized dangers confronting contemporary social specialists and risk administration. (Reamer, 2013)

4.3 Recommendation

Six recommendations that boards can take in order to create a more Risk Intelligent governance. These recommendations are:

- Determine board's risk oversight responsibility
- Enhance Risk Intelligence throughout the organization
- Determine risk appetite
- Align managements strategic risk identification and mitigation with strategy
- Evaluate the entities risk governance maturity.
- Communicate risk process and issues to stakeholder

5. References

Bibliography

Buhlz_I, 2017. [Online] Available at: https://acloud.guru/forums/aws-certified-developer-associate/discussion/-KTdRPtz4PF2rLHO1_tD/what-is-cia-and-aaa-models-ingress-vs-egress-filtering-and-which-aws-services-an.

Dionne, G., 2013. [Online] Available at: https://www.cirrelt.ca/DocumentsTravail/CIRRELT-2013-17.pdf.

Hegde, V., 2011. *IEEE*. [Online] Available at: http://0-ieeexplore.ieee.org.emu.londonmet.ac.uk/document/5754492/.

Investopedia, n.d. [Online] Available at: https://www.investopedia.com/terms/c/cost-benefitanalysis.asp.

Investopedia, n.d. [Online] Available at: https://www.investopedia.com/terms/f/feasibility-study.asp.

Reamer, F.G., 2013. *academic.oup.com*. [Online] Available at: https://academic.oup.com/sw/article-abstract/58/2/163/1940392.

Rouse, M., 2011. [Online] Available at: http://searchcompliance.techtarget.com/definition/risk-avoidance.

Tech Target, n.d. [Online] Available at: http://searchcompliance.techtarget.com/definition/risk-management.

The MITRE Institute, n.d. [Online] Available at: https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-identification.

Tutsplus, n.d. [Online] Available at: https://business.tutsplus.com/tutorials/effective-risk-management-strategies--cms-22887.