St. Mary's University
School of Graduate Studies

Department of Computer Science

Developing Cyber Security Risk Assessment Framework for Railways Industry in Ethiopia

A Thesis Submitted to the Department of Computer Science of St. Mary's University in the Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

By

Eyuel Mulualem Bahiru

May 2019

St. Mary's University
School of Graduate Studies

Department of Computer Science

Developing Cyber Security Risk Assessment Framework for Railways Industry in Ethiopia

By

Eyuel Mulualem Bahiru

Panel of Examiners:

Advisor: Dr. Getahun Weldemariam Signature_______________Date_________

Internal Examiner: Dr. Asrat Beyene Signature_______________Date_________

External Examiner: Dr. Temtim Assefa Signature_______________Date_________

Table of Contents

Abstract vi

Declaration vi

Acknowledgments viii

List of Acronyms ix

Lists of Figures xi

Lists of Tables xii

Chapter One: 1

Introduction 1

1.1 Overview 1

1.2 Background of the Study 2

1.3 Statement of the Problem 3

1.4 Research Question 5

1.5 Objectives 6

1.5.1 General objective 6

1.5.2 Specific objective 6

1.6 Scope 6

1.7 Significance of the Research 6

1.8 Organization of the Study 7

Chapter Two: 8

Literature Review 8

2.1 Overview 8

2.2 Information Security 8

2.3 Cyber Security 8

2.4 Cyber Security in Railways Industry 9

2.4.1 Railways System Overview and Cyber Attack Incident 9

2.4.2 Safety and Security 11

2.4.3 Rail Security Requirements 12

2.5 Information, ICT and Cyber security 13

2.6 Risk Assessment 13

2.6.1 Risk Analysis 14

2.6.2 Risk Evaluation 14

2.7 Asset, Vulnerability, Threat and Attack 15

2.7.1 Asset 15

2.7.2 Vulnerability 15

2.7.3 Threat 17

2.7.4 Attacks 18

2.8 International Standards and Framework 19

2.8.1 Cyber Security Risk Assessment Standards and Framework 20

2.9 Review of Related Literature 23

Chapter Three: 29

Research Methodology 29

3.1 Overview 29

3.2 Research Design 29

3.2.1 Design Science Research Approach 30

3.3 Data Collection Method and Source 32

3.4 Sampling Technique 33

3.5 Data Analysis Method 33

Chapter Four: 35

Interpretation of the Data 35

4.1 Introduction 35

4.2 Ethiopia Railways Features as well Information, Safety and Security Requirements 35

4.3 Cyber Security Risk Assessment Framework & Standards Challenges and Organizational Difficulties 39

4.4 Extent/Level to which International Cyber Security Risk Assessment Frameworks and Standards Suitable for Ethiopia Railways 43

Chapter Five: 49

The Proposed Cyber Security Risk Assessment Framework 49

5.1 Introduction 49

5.2 National Cyber Security Risk Assessment 53

5.3 Proposed Cyber Security Risk Assessment Framework 54

Chapter Six: 68

Evaluation of the Proposed Framework 68

5.1 Descriptive Framework Evaluation Method 68

5.1.1 Cyber Incident Scenario 68

5.1.2 Analysis of Scenario against Proposed Framework 69

5.2 Panel of Experts Method 72

5.3 Summery 74

Chapter seven: 75

Conclusions, Recommendations and Future Works 75

7.1 Conclusions 75

7.2 Recommendations 76

7.3 Future Works 76

References 77

Appendix A: Interview Question and Answer 81

Appendix B: - Interview Questions____87

Appendix C: Strategic and Tactical Risk Assessment______________________________88

Abstract

Cybersecurity is very crucial for the railway's industry. The railway's organization should protect its asset from possible threats. An organization needs to assess cybersecurity risks primary to protect the assets. In order to conduct a cybersecurity risk assessment, a framework should be developed first.

The researcher identified and investigated the railway's industry problem in Ethiopia and the gap of previous cybersecurity risk assessment standards, guidelines and frameworks and come up with the solution. The general objective of this research is to develop an integrated cybersecurity risk assessment framework for the railway's industry in Ethiopia to improve the level of safety and security. The synthesized result of thematic data analysis and the relevant framework, standard, guidelines such as ISO27001, NIST SP 800-30, and critical mass cybersecurity requirement standard is used to develop cybersecurity risk assessment framework for railways industry in Ethiopia.

The national cybersecurity risk assessment process has3 main levels that are national, sectoral and organizational. The organizational level risk assessment process also has 3 main level that is strategic tactical/managerial and operational level. The organizational operational level has a total of 13 components that include cybersecurity strategic management awareness, organizational structure, established system context, purpose, scope, identify assets & intrusion detection, identify threats, identify vulnerability determine likelihood, determine impact, risk evaluation, communicate result and risk identification & evaluation update opportunity.

The design science approach is applied in this study to develop and evaluate the framework. To evaluate the framework the researcher used a descriptive approach which is scenario and panel of expert’s method. The data is collected from Ethiopian Railways Corporation and Information Network Security agency then thematic data analysis approach is applied to analyze and interpret the data.

Though two studies conducted on the financial sector in Ethiopia, the methodology to conduct this study and few CSRA process components (specific to the railway's industry in Ethiopia) makes this research different from the other two. Thus it provides the opportunity to extend the knowledge area. The result of this research can help improve organization cybersecurity risk assessment process.

Keywords: Cybersecurity, Risk Assessment, Cyber Security Risk Assessment, Cyber Security Risk Assessment Standards, framework and Guidelines, Cyber Security Risk Assessment Framework for Railway

Declaration

I, the undersigned, declare that this thesis is my original work, has not been presented for a degree in this or any other universities, and all sources of materials used for the thesis work have been duly acknowledged.

Name: Eyuel Mulualem Bahiru

Date: May 15, 2019

Signature: ____________________

Acknowledgments

First and foremost I am grateful to God, who kindly helped me to complete my thesis. Then I would like to express my special appreciation and thankfulness to my advisor, Dr. Getahun Weldemariam for his continuous support, patience, motivation, enthusiasm, and immense knowledge.

I would like to thank the expert and professionals at Ethiopia Railways Corporation and Information Network Security Agency for the invaluable assistance they have provided me during the process of information gathering, analysis, and evaluation. My research would not have been possible without their help. Special thanks go to my family, my beloved girlfriend, my best friends, and subordinates for their continuous support and encouragement with their best wishes towards my goal, without whose love, encouragement, and prayer I would not have finished this thesis.

Eyuel Mulualem Bahiru

List of Acronyms

AALRT	Addis Ababa Light Rail Transit
AC	Axel Counter
ATS	Automatic Train Supervision
BMIS	Business Model for Information Security
CBI	Computer-Based Interlocking
CC	Car-borne Controller
DMI	Driver Machine Interface
DOS	Denial-of-Service
ERC	Ethiopia Railways Corporation
ERTMS	European Railway Traffic Management System
FDRE	Federal Democratic Republic of Ethiopia
CSRA	Cyber Security Risk Assessment
ICT	Information Communication Technology
IEC	International Electro technical Commission
InfoSec	Information security
INSA	Information Network Security Agency
ISO	International Organization Standardization
IT	Information Technology
ITU	International Telecommunication Union
LEU	Line Side Electronic Unit
MSS	Maintenance Support System
NCSSC	National Cyber Security Standardization Committee
NISEAC	National Information Security Engineering Core Process
NISMC	National Information Security Management Center

NIST SP	National Institute of Standards and Technology
PESTLE	Political, Economic, Social, Technological, Legal Environmental
RTO	Rail Transport Operators
SCADA	Supervisory Control and Data Acquisition
SGOC	Strength, Gap, Opportunity and Challenge
SIL	Safety Integrity Level
TA	Thematic Analysis
TAC	Technical Assistance Center
TCP/IP	Transmission Control Protocol/ Internet Protocol

Lists of Figures

Figure 2.1 Railway System Scheme 9
Figure 2.2 Risk Assessment Process.. 21
Figure 3.1 Design science research process application in the study 31

Figure 5. 1 National Cyber Security Risk Assessment Layer... 53
Figure 5. 2 Cyber Security Risk Assessment Framework 55
Figure 5. 3 Addis Ababa Light Rail Transit System Architecture.................................... 60

Lists of Tables

Table: - 2.1 Vulnerability Severity and Exposure Rating 16
Table: - 2.2 Vulnerability Rating Combination 16
Table: - 2.3 Overall Vulnerability Ratings.. 17
Table 2.4 Threats 18
Table 2.5 the difference between standards and related studies 25
Table 4.1: Coding.. 36
Table 4.2: Searching for Themes 37
Table 4.3 Coding.. 39
Table 4.4: Searching for Themes 41
Table 4.5 Coding.. 43
Table 4.6: Searching for Themes 46
Table 5.1 Summarization of how the proposed integrated framework is derived from empirical data and pertinent standards.. 51
Table 5.2 Railways Layer 59
Table 6.1 Summary of Scenario Application in CSRA Framework.. 71

Chapter One:

Introduction

1.1 Overview

Information and Cybersecurity risk management is crucial for one organization to survive on the network. Security is the quality or state of being secured, to be free from danger. In other words, security can be defined as building protection against an opponent. Information security (InfoSec) is the protection of information and its critical elements, including the systems and hardware which use, store and transmit that information. Information security includes the broad areas of information security management, computer, and data security management, computer and data security, and network security. To protect information and its related systems, tools such as strategy, policy, awareness, and technologies are of vital importance.

Cyber Attacks are described by (Tatum, 2010), as "an attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission. Attacks of this type may be undetectable to the end user... or lead to such a total disruption of the network that none of the users can perform even the most rudimentary of tasks"[1].

Cyber-security is considered a growing political, economic and social threat, which is constantly evolving and challenging high-tech users globally. The way in which security is understood has developed rapidly over the last century, and this has had an influence on the recent risk-based security paradigm. ISO defined cybersecurity as the 'preservation of confidentiality, integrity, and availability of information in the cyberspace.

Risk assessment – the process of identifying, analyzing and evaluating risk – is the only way to ensure that the cyber security controls you choose are appropriate to the risks your organization faces. Without a risk assessment to inform your cyber security choices, its waste of time, effort and resources. A cybersecurity risk assessment identifies the various information assets that could be affected by a cyber-attack (such as hardware, systems, laptops, data, and intellectual property), and then identifies the various risks that could affect those assets.

As stated by Expert Joe Granneman "An information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment. These frameworks are basically a "blueprint" for building an information security program to manage risk and reduce vulnerabilities. Information security pros can utilize these frameworks to define and prioritize the tasks required to build security into an organization"[2].

The reasons many organization use information security frameworks are to assure people that their data is being handled and processed safely and reduce the opportunity for fraudulent use of data.

1.2 Background of the Study

As stated by MichałKozickiThe Ethiopian railway was built by the French to facilitate the transport of merchandise [3].

The railway connecting Ethiopia with Djibouti via Dire Dawa is a 780 km meter-gauge line opened in 1917. It is the only railway line that connects landlocked Ethiopia with Djibouti Port, a major cargo entry point, but decline due to a lack of maintenance and management.

Ethiopia is working on building a wide rail network. In response to this and thus understanding the strategic importance of railway infrastructure, the Federal Democratic Republic of Ethiopia established the Ethiopian Railways Corporation on 28 November 2007 by regulation 141/2007 of the Council of Ministers of the Federal Democratic Republic of Ethiopia. The regulation mandates ERC to develop railway infrastructure and provide passenger and freight rail transportation services in Ethiopia. Ethiopia Railways Corporation has developed railway projects on eight corridors in the country that have been identified as necessary to enhance both the social and economic needs.

The company launched a 756 Kilometers railway network construction project that links the capital city Addis Ababa to the port of Djibouti and 34 km Addis Ababa Light Rail Transit service that have 2 lines from Minilik square to Kallity and Ayat to Tor Hayiloch (that started operation in September 20, 2016 which is highly support the city's transport). Even if the lines are very limited it has a large and integrated system which might be vulnerable to cyber-attack and has a big national impact if cyber-attack and accident happened.

The Railways industry relies heavily on information technology and automation system. Our country railways system also relies on railways industry technology demand such as control train movement, power delivery to the network, supervisory control and data acquisition, management information system control signaling and communication system and infrastructure, operational planning and timetable.

The railway signaling system is a safety-critical system that lies in the core of railway infrastructure. Addis Ababa Light Rail and Addis Ababa Djibouti signaling system consists of (a) computer-based interlocking system: - it is real-time control system which uses computer technology to realize the interlocking process and it restrict relations among route, switch and signal light (b) Automatic train supervision: - is composed of equipment in control center, in stations and depots. Its function is to collect track occupation state, route state, train running state and signaling equipment failure state from wayside equipment and onboard automatic train protection (c) Automatic train control system: - it's composed of trackside and train onboard equipment such as LEU and beacons are trackside and Car-borne Controller (CC), Driver Machine Interface (DMI), Beacon Antenna, and Coded-odometer are onboard equipment. All of them are connected to the signaling network. Communication systems of Addis Ababa Light Rail are the backbone of all systems, it includes transmission, wireless radio, telephone systems, and surveillance camera.

Supervisory Control and Data Acquisition system is a computer communication based on the production process control and dispatch automation system, on-site equipment monitoring and control. It is not a simple control system, but more emphasis on the level of surveillance, it is based on the hardware platform to provide an interactive interface software.

1.3 Statement of the Problem

The advanced digital Railways technology is being constructed and implemented in our country. It provides transportation services to customers in Addis Ababa city and in the Addis Djibouti corridor. The railway's transport network is highly digital signaling, communication, management information system includes ticket management and railways construction management system. Supervisory Control and Data Acquisition system have a wide range of data flowing across the system. As more devices and control systems are connected through the network, more vulnerabilities will appear, increasing the potential for disruption to the assets.

To provide safe and efficient transportation service, organization (operator) needs to coordinate different systems, including railway signaling system, Communication system, Supervisory Control, and Data Acquisition system traction power system, passenger information system, and fare collection system. The growth dependency of such systems on ICT introduces cybersecurity risks[4].

The organization network, signaling systems (including wayside equipment: switch machine), transmission system, wireless radio communication system and management information system which is connected to an operation control center must be protected.

The hacking of the computer-based interlocking (CBI), a signaling system designed to prevent the setting up of conflicting routes would cause serious problems, including physical damage [5].In 2007, a 14-year-old Polish teenager in the city of Lodz studied the tram and track operations in his city and built a device similar to a TV remote control to change switch points on the tracks. Twelve people were sent to the hospital with injuries and four vehicles were derailed [6]. If someone (hackers) enter into this network it can access directly all the systems and train drivers along the line and they might give the wrong command to the equipment and personnel. If the organization doesn't protect all the asset that has a direct relation with cyber it may expose the organization to cyber risk.

Also the entire organization systems have connectivity through the internet for sharing system information for maintenance purpose such as Supervisory Control and Data Acquisition system, Communication and signaling system which may cause supplier relationship risk (the contractor which have the privilege to access the system remotely from some were else) could be a channel to cyber-attack to the systems. Besides the supplier relationship, the organization/management doesn't have enough cybersecurity awareness; and the company is in organizational/management risk.

As we understand the possible vulnerabilities in the organization and attack in different country rail systems, Ethiopian Railways Corporation might face the same possible attacks on its assets for the reason that our country railways system adopted similar railways technology like other countries which faced railways cyber-attack.

All the above discussion showed us that Ethiopia Railways technology is a composition of several integrated systems and identified possible risk area. The researcher has investigated the railway's system in our country and possible risk area for the reason that it helps the researcher to identify organizational problems related to cybersecurity and risk assessment.

Primarily, it's important to conduct a cybersecurity risk assessment of the railway's system to secure normal transport operation. In order to conduct a cybersecurity risk assessment, a framework suitable for the railway's industry should be developed first.

Regarding cybersecurity risk assessment standards and frameworks the researcher identified the following gaps:

- International and national standards such as ISO 27001, NIST SP 800-30 and critical mass cybersecurity requirement standard don't consider or cover railways features as well railways information, safety, and security requirements: it's not specific to railways organization.

International standards are developed based on generic and universal principles. They also claim that generic and universal guidelines do not pay attention to organizational differences. Such guideline does not address the organization's own and unique information security requirement but prescribes universal or general procedure [7].

Regarding Ethiopian Railways Corporation the researcher identified the following problem:

- The framework they have used at present doesn't meet national cybersecurity requirement standard. ERC/Temporary cybersecurity risk assessment adopted and used the NIST SP 800-30. INSA issued national cybersecurity requirement standard based on our country context, the framework includes national information security policy, national cybersecurity strategy, national cybersecurity governance system and national cybersecurity regulation framework[8]. According to the standard risk assessment process should be based on national cybersecurity risk assessment methodology and it should comprise strategic, tactical (managerial) and operational risk assessment which is based on operation related clauses of ISO 27001 standard[8].

The aim of this study is, therefore, to enhance existing frameworks by investigating and incorporating the unique railway's features as well as information and cybersecurity requirements of ERC. The finding from empirical data and the gaps of international standards are used to develop a new integrated cybersecurity risk assessment framework. It will help improve the knowledge and understanding of the cyber security and risk assessment domain and the actual framework can be used as a guide to address some of the current limitations in the railways Corporation risk assessment process.

1.4 Research Question

The following research questions are formulated to address the research problem:

- What are the existing features as well as information, safety and security requirements of Ethiopian Railways?
- What is the existing challenge in cybersecurity risk assessment in Ethiopian Railways?
- To what extent are international cybersecurity risk assessment frameworks and standards suitable for Ethiopia Railways?
- What cybersecurity risk assessment framework can best address the existing challenges and difficulties?

1.5 Objectives

1.5.1 General objective

The general objective of this research is to develop an integrated cybersecurity risk assessment framework for the railway's industry in Ethiopia to improve the level of safety and security.

1.5.2 Specific objective

- To understand the existing status and level of cybersecurity risk assessment being practiced in Ethiopia Railways Corporation.
- To identify and evaluate the relevance of the existing cybersecurity risk assessment standards and frameworks being applied nationally and internationally to the Ethiopian Railway industry.
- To identify gaps in the existing cybersecurity risk assessment frameworks in Ethiopia in the railway industry.
- To propose a cybersecurity risk assessment framework relevant to the context of Ethiopia Railways Corporation
- To validate the framework.

1.6 Scope

Considering the objective of the study, the scope of the research focus was on developing cybersecurity risks assessment framework for the railway's sector in Ethiopia which comprises Addis Ababa Djibouti railways and Addis Ababa light rail transit. Ethiopia Railways Corporation is a responsible organization for constructing railways infrastructure and operate. The cybersecurity risk assessment focused on the overall railway system that could have a major national impact.

1.7 Significance of the Research

The implementation of advanced technology for Ethiopian railways system is ongoing for the last three years. The railway's infrastructure has a complexity of the integrated system. Most of the systems share information, data and different command each other through the network, this may expose the organization to cyber risk. The development of the cyber security risk assessment framework will help the organization to assess risks: identify assets, threat, and vulnerability, determine likelihood and impact. In addition to this, the framework will be an input for developing a security plan and countermeasures (policy and procedure).

1.8 Organization of the Study

The research report is organized into six chapters: Chapter one focused on the background of the study, problem statement, research question, objectives, scope, significant of the study and organization of the study. In Chapter two, the results of a review of a range of literature captured concerning information security, cyber security including cybersecurity in Railways, risk assessment, information communication technology, international standards and framework, related research papers conducted in Ethiopia and knowledge gap. In chapter three, details of the methodology followed to achieve results were outlined. It includes the study research design, data collection method, and source, sampling technique, data analysis. Chapter four explains interpreting the data, finding and discussion. Chapter five contained the development of an integrating cybersecurity risk assessment framework. Chapter six evaluates the proposed integrated framework. Chapter seven presented conclusion, recommendations and future work of the study.

Chapter Two:

Literature Review

2.1 Overview

This section presents a review of related researches in Ethiopia, international cybersecurity risk assessment standards and framework, international cybersecurity risk management standards, and framework. It also covered major concepts pertaining to cyber security, cyber security in railways, risk assessment, cybersecurity risk assessment.

2.2 Information Security

In general, security is the quality or state of being secure — to be free from danger. In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective. A successful organization have multiple layers of security in place to protect its operation: Physical security, to protect physical items, objects, or areas from unauthorized access and misuse; Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations; Communications security, to protect communications media, technology, and content; Network security, to protect networking components, connections, and contents; Information security, to protect the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission [9].

Information security ensures that within the enterprise, information is protected against disclosure to unauthorized users. Confidentiality means preserving authorized restrictions on access and disclosure, including means for improper modification. Integrity means guarding against improper information modification or destruction, and includes ensuring and non-access when required. Availability means ensuring timely and reliable access to and use of information [10].

2.3 Cyber Security

The term ‘cybersecurity’ was widely adopted during the year 2000 with the ‘clean-up’ of the millennium software bug. The different organization has their own definition of cybersecurity.

ISO defined cybersecurity as the ‘preservation of confidentiality, integrity and availability of information in the Cyberspace as well as ITU also defined cybersecurity broadly as:The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment [11].

2.4 Cyber Security in Railways Industry

2.4.1 Railways System Overview and Cyber Attack Incident

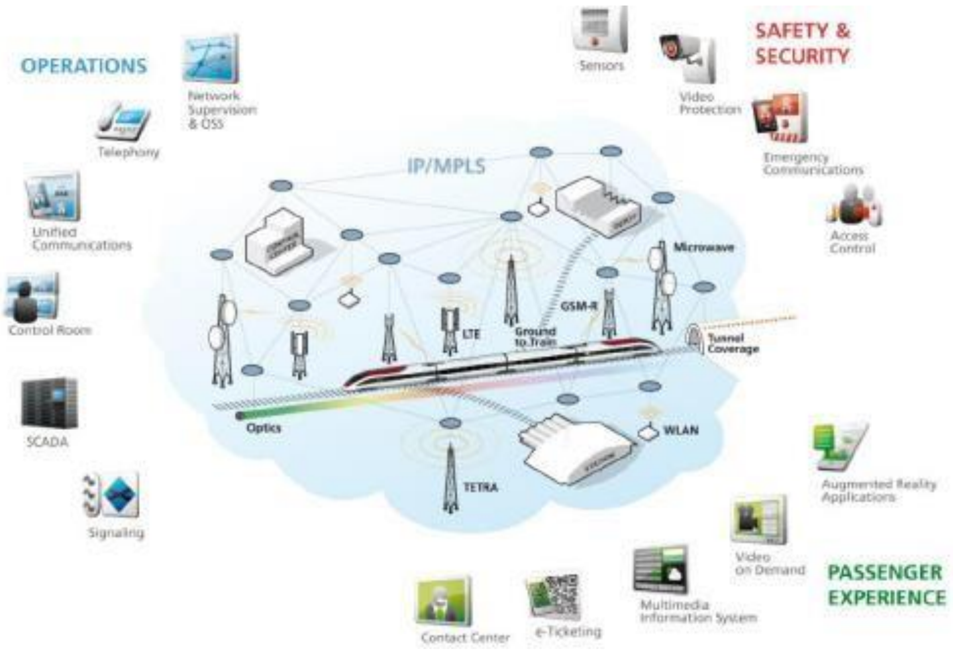


Figure 2.1Railway System Scheme

There are several differences between a rail transportation system and a single manufacturing site[12]:

- **Distance** - A rail system covers vast distances, and each segment of the rail system has to communicate with its adjacent segments and with the operations control center (and backup operations control center). Transit agencies are expert at the physical security aspects of their systems. Cybersecurity adds a new dimension to the security program. In addition, a rail system includes self-contained equipment rooms located along the tracks, known variously as signal bungalows and waysides.
- **Communication** - A transit agency needs to communicate with maintenance crews on or near the track; with engineers/drivers (if applicable); between the train set and the wayside; and between and among the control and signal devices, such as signals,

road crossing gates, track circuits, various maintenance and detection devices, passenger information displays, emergency information displays, advertising displays, and others.

- **Power** - A transit system often has its own traction power stations for electricity. There are power feeds from local utilities that need to be coordinated. Power is distributed via catenaries or third rail. Additional power is required to run all other equipment, including lighting, communications, and signals. There are differences between a railway electrical system and most other commercial systems; the most common difference is the use of floating ground.
- **People** - The purpose of a transportation system is to move people. They are the precious cargo of the system, and they expect and need to be delivered safely. Transit systems have many large, public areas, including entrances, exits, platforms, waiting for areas and amenities (toilets, cafes, etc.) that must allow everyone access. There are other areas that need to be restricted, such as equipment and power rooms, tracks, signaling systems, employee areas and so on.
- ➢ **Access to property**- Transportation system assets, on the other hand, is out in public. Physical security exists—much of it to keep the public from dangerous areas, such as power sources, third rails, overhead wiring, the path of trains and so on—but it is impossible to keep determined individuals away from the transportation system's assets.

Railway system such as signaling systems, communication system, management information system and Supervisory Control and Data Acquisition system have become more and more software and IT-based.

Cybersecurity is an increasingly important topic, especially for railways. Every railway operator faces the massive challenge of protecting its own infrastructure. In most cases, heterogeneous IT technologies and software solutions are used and result in wide-ranging, disparate data sets. The protection of such environments is complex and multi-dimensional. It is exacerbated by the enormous quantity of data resulting from an ever-increasing number of devices, processes, and services. From an information security perspective, one of the primary concerns for every manager is reducing the risk of potential data losses and ensuring smooth, stable railway operations [13].

Railways are classified as critical infrastructures, and the signaling, communication, Supervisory Control, and Data Acquisition system technology is becoming more and more dependent upon ICT systems. If something goes wrong, it may have massive consequences:

- Trains stop (emergency braking, system failures)
- Negative economic effects and loss of trust

- In the worst case, accident casualties

In order to be able to offer excellent rail service, rail operators make widespread use of information technologies and automated computer systems. These systems are under a constant and increasing threat. The protective measures against cyber-attacks in the railway sector are not yet fully developed. There is often a lack of awareness with respect to new risks. Railways in particular, with their highly developed security philosophies, do not take the risks into account because they are convinced of the high level of security of their systems. This is, however, the result of a misunderstanding: Security in the railway industry is operational safety. But cybersecurity is about protecting information systems against theft or damage, ergo defending them against external and internal attacks and risks, in particular as a result of criminality. That is a significant difference. Protecting railway operators against the consequences of cyber-attacks is a key task[13].

Examples from the past prove that real attacks are not just theory:

1. CSX railway virus attack in 2003, the “So big virus” struck CSX’s Jacksonville, Florida, headquarters, bringing down signaling, dispatch and other related systems. Amtrak trains operating in CSX’s territory were also affected. Trains were delayed from between four to six hours. Another web news account related that the virus struck at 1:15 in the morning and most affected computers were fixed by 7:15 a.m. However, CSX had said it would take up to 24 hours to completely recover. Consequences were losses from the freight and passenger delays, as well as confusion and extra computer cleanup from the virus.
2. Polish tram hack: - In 2007, a 14-year-old Polish teenager in the city of Lodz studied the tram and track operations in his city and built a device similar to a TV remote control to change switch points on the tracks. Twelve people were sent to the hospital with injuries and four vehicles were derailed.
3. In 2008, a teenager wreaked havoc by derailing four tram-trains in Lodz, Poland using an adapted TV remote. There were a number of injuries.
4. In 2011, hackers remotely attacked computers in the north-western USA, stopping railway signals for two days.
5. In 2015, North Korea was suspected of hacking a subway operator in Seoul, South Korea over the course of several months.

2.4.2 Safety and Security

Safety is at the core of rail activity. It’s the total responsibility of the railway's companies, infrastructure and undertakings since the beginning of the rail, whereas security is often a shared responsibility with authorities.

Safety is the state of being "safe”. The condition of being protected against physical, social, occupational, psychological, or other types or consequences of failure, damage, error, harm or any other event which could be considered as non-desirable. Safety is protection against accidental events, but these can come from internal causes (faults, errors, omissions…) and external causes (for example 3rd parties at level crossings or natural disasters and climate events)[12].

Security as a state or condition is resistance to harm. From an objective perspective, it is a system or structure's actual (conceptual, and never fully known) degree of resistance to harm. Security is protection against intentional damage (delinquency, terrorism, cyber-attacks)[1].

2.4.3 Rail Security Requirements

The following sets of requirements for ensuring information security are needed for equipment performing train and shunting control functions (Railway Automation and devices) and they're associated critically important facilities (processes) [12]:

1. Requirements for personnel and other people involved in the operation of Railway.
2. Physical protection requirements.
3. Access management requirements.
4. Requirements for data storage devices.
5. Software requirements.
6. Intrusion detection requirements.
7. Information security incidents response requirements.
8. Reliability requirements.

During formulating the requirements, it is necessary to consider the following points:

- Hardware and software of the railway automation and telemechanic systems and data security hardware and software are allowed to be supplied to the object only if they have unexpired documents according to their technical documentation, and confirming their compliance with the requirements established in the technical documentation;
- Information transmission lines and local area networks that are part of the railway automation and telemechanic systems should be designed in accordance with the established norms of technological design. During the construction of these lines and networks, any deviations from the design documentation are prohibited;
- Radio equipment used within railway automation and telemechanic systems must be registered in accordance with the established procedures;
- All technical means and facilities must not have any damage.

2.5 Information, ICT and Cybersecurity

Information security, computer security and information assurance all these three terms are often used interchangeably, even if they address slightly different viewpoints.

Information security' focuses on data regardless of the form the data may take: electronic, print or other forms. 'Computer security' usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Information assurance' is a superset of information security, and deals with the underlying principles of assessing what information should be protected[11].

In general, ICT security is more directly associated with the technical origins of computer security and is directly related to 'information security principles' including the confidentiality, integrity, and availability of information resident on a particular computer system. ICT security, therefore, extends beyond devices that are connected to the internet to include computer systems that are not connected to any internet.

There is no agreed definition of 'internet security'. Within a technical context, internet security 'is concerned with protecting internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet security also ensures the availability and reliability of internet services. What internet security probably does not include is non-internet relevant technical issues, including those that address the various 'internets' which are not connected to the World Wide Web. These, however, are covered by the term 'network security'. Network security is particularly important for critical infrastructures that are often not directly connected to the internet [11].

2.6 Risk Assessment

The need to conduct vulnerability and risk assessments is being driven by these new laws and mandates. Organizations must now be information security conscious and must develop and implement proper security controls based on the results of their internal risk assessment and vulnerability assessment. By conducting a risk assessment and vulnerability assessment, an organization can uncover known weaknesses and vulnerabilities in its existing IT infrastructure, prioritize the impact of these vulnerabilities based on the value and importance of affected IT and data assets, and then implement the proper security controls and security countermeasures to mitigate those identified weaknesses. This risk mitigation results in increased security and less probability of a threat or vulnerability impacting an organization's production environment.

Risk assessment is composed of risk analysis and risk evaluation. It provides a systematic way for the organization to obtain a comprehensive view of existing information security risks and their consequences, and the countermeasures to deal with them. Since assessment process includes the risks associated with all kinds of platforms, operating systems, application programs, networks, people, and processes, as well as the interdependencies between them, it is a challenging process and in most cases, organizations require outside help to perform it properly. Note that mistakes in risk assessment can be dangerous and costly. Underestimating the risks can leave the organization vulnerable to severe threats, whereas by over estimating them, some useful IT services and technologies might be withdrawn[14].

2.6.1 Risk Analysis

Risk analysis identifies the organization's valuable information assets and their vulnerabilities, reveals threats that may take advantage of those vulnerabilities and put the organization at some sort of risk, and, finally, estimates the possible damage and potential losses resulting from those risks [14]. We discuss the risk analysis steps in detail below:

1. Resource Identification and Valuation: Identifying and evaluating information assets/resources is a critical first step in risk analysis. In general, information assets are either tangible or intangible and are assets which are valuable to the organization.
2. Risk Identification: The objective of this step is to identify all possible risks to the assets. Thus, the vulnerabilities of each valuable resource and the threats that might take advantage of them are identified, and then the relationship between vulnerability and threats is defined as a risk.
3. Risk Measurement: In this step, the organization needs to choose a model to measure risk. Risk model specifies the relationship among risk factors which include resource value, vulnerability effect, threat impact, threat likelihood, and so on. Based on the chosen model, the risk value for each incident scenario is measured. In the process of risk assessment, it is also important to identify existing/planned safeguards. Failing to consider all of these safeguards will result in an inaccurate risk assessment report, which will generate unnecessary costs for the organization and also put the business in danger because of risk overestimation

2.6.2 Risk Evaluation

Risk evaluation is the process of rating risk exposures on a scale and against accepted risk criteria to determine the significance of each risk. Then we need to determine the proper steps to manage the risks and address them appropriately. In this phase, the identified risks need to be prioritized based on their relative probability of occurrence and their legal, regulatory, financial, or reputational impact to the organization in order to make decisions on their treatment[14]. There are four ways to address a particular risk:

1. Accept: The organization understands the risk and its consequences and consciously decides to accept it.
2. Avoid: The activity that is exposing the organization to one or more risks is avoided altogether.
3. Transfer: All or part of the responsibilities and liabilities associated with a particular activity and the related risk are shifted to another party.
4. Mitigate: The risk and its consequences are controlled and limited in some way, reducing

2.7Asset, Vulnerability, Threat, and Attack

2.7.1 Asset

An asset is the direct or indirect target of an event. Assets are generally something of value including; applications, databases, software, hardware, buildings, people and infrastructures. The asset is what needs protection from the event.

Before addressing security threats, attack and vulnerabilities the assets that have value for the organization and have a big impact on the organization and country should be identified. An asset is anything that has value to the organization and is necessary for achieving its objectives. An information system is a composition of hardware, software, network, people and facilities.

2.7.2 Vulnerability

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks. Weaknesses can be in system hardware or software, policies, and procedures used in the systems and system users themselves. Hardware vulnerabilities are very difficult to identify and also difficult to fix even if the vulnerability were identified due to hardware compatibility and interoperability and also the effort it takes to be fixed. Software vulnerabilities can be found in operating systems, application software, and control software like communication protocols and devices drives. There are a number of factors that lead to software design flaws, including human factors and software complexity[15]. Technical vulnerabilities usually happen due to human weaknesses.

Vulnerability Analysis

The purpose of vulnerability analysis is to take what was identified in the gathering of information and test to determine the current exposure, whether current safeguards are sufficient in terms of confidentiality, integrity or availability. It will also give an indication as to whether the proposed safeguards will be sufficient [16].

The specific vulnerabilities can be graded according to the level of risk that they pose to the organization, both internally and externally. A low rating can be applied to those vulnerabilities that are low in severity and low in an exposure. Vulnerabilities would receive a high rating if the severity was high and the exposure was high. The following tables from the Threat and Risk Assessment Working guide illustrate this grading system[16].

Table: - 2.1 Vulnerability Severity and Exposure Rating

Severity	Rating	Exposure
Minor severity: Vulnerability requires significant resources to exploit, with little potential for loss	1	**Minor exposure:** Effect of vulnerability tightly contained. Does not increase the probability of additional vulnerabilities being exploited
Moderate severity: Vulnerability requires significant resources to exploit, with significant potential for loss. Or, vulnerability requires little resources to exploit, moderate potential for loss.	2	**Moderate exposure:** Vulnerability can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited.
High severity: Vulnerability requires few resources to exploit, with significant potential for loss.	3	**High exposure:** Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited.

Table: - 2.2 Vulnerability Rating Combination

Severity Rating		Exposure Rating	
	1	2	3

1	1	2	3
2	2	3	4
3	3	4	5

Table: - 2.3 Overall Vulnerability Ratings

Rating	Description
1	Minor exposure, minor severity.
2	Minor exposure, moderate severity; or moderate exposure, minor severity.
3	Highly exposed, minor severity; or minor exposure, high severity; or moderate exposure, moderate severity
4	Highly exposed, moderate severity; or, moderate exposure, high severity.
5	Highly exposed, high severity.

2.7.3 Threat

Threats can be seen as events, sources, actions or inactions that could lead to the loss or harm of organization assets. It can be very difficult to identify all threats given the scope of assets, location, industry segment as well as the state of current events in the market.

Threat assessment

Threats are described as anything that would contribute to the tampering, destruction or interruption of any service or item of value. These threats can be split into Human and Nonhuman elements. For example.

Table 2.4 Threats

Human	Non- Human
• Hackers • Theft (electronically and physically) • Non-technical staff (financial/accounting) • Accidental • Inadequately trained IT staff • Backup operators • Technicians, Electricians	• Flood • Lightning strike • Plumbing • Viruses • Fire • Electrical • Air (dust) • Heat control

Threats that are identified must be looked at in relation to the business environment and what effect they will have on the organization. Threats go hand in hand with vulnerabilities and can be graded in a similar manner, measured in terms of motivation and capability.

2.7.4 Attacks

Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources, and motivation is called attack cost. Attack actors are people who are a threat to the digital world. They could be hackers, criminals, or even governments [15].

Common cyber-attack types are:

1. Physical attacks: This sort of attack tampers with hardware components.
2. Reconnaissance attacks – unauthorized discovery and mapping of systems, services, or vulnerabilities.
3. Denial-of-service (DoS): This kind of attack is an attempt to make a machine or network resource unavailable to its intended users.
4. Access attacks – unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access attack: the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to IP-connected devices.

5. Cyber-crimes: The Internet and smart objects are used to exploit users and data for materialistic gains, such as intellectual property theft, identity theft, and fraud.
6. Destructive attacks: Space is used to create large-scale disruption and destruction of life and property. Examples of destructive attacks are terrorism and revenge attacks.

Supervisory Control and Data Acquisition (SCADA) Attacks: Like any other TCP/IP systems, the SCADA system is vulnerable to many cyber-attacks. The system can be attacked in any of the following ways:

1. Using denial-of-service to shut down the system.
2. Using Trojans or viruses to take control of the system.

2.8 International Standards and Framework

The purpose of the Framework is to create a common approach for addressing cybersecurity within the member organizations, to achieve an appropriate maturity level of cybersecurity controls within the member organizations and ensure cybersecurity risks are properly managed throughout the member organizations [17].

The International Organization for Standardization (ISO) defines a standard as “a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context[18]” Numerous standards have been developed for cybersecurity to help organizations better manage security risk, implement security controls that meet legal and regulatory requirements.

Based on the above statement we can say that a country must organize (prepare) cybersecurity standards to meet its own country legal and regulatory requirement. In addition to this cybersecurity standard must prepare (proven) by a recognized body that provides common rule and guideline to the country. The Federal Democratic Republic of Ethiopia established Information Network Security Agency by regulation of the council of ministry of FDRE. INSA has published critical mass cybersecurity requirement standard version 1.0 on September 2009 E.C. As stated on critical mass cybersecurity requirement standard, the framework includes national information security policy, national cybersecurity strategy, national cybersecurity governance system and national cybersecurity regulation framework[8]. We can say that this standard meet Ethiopia legal and regulatory requirement.

Critical mass cybersecurity requirement standard is issued in order to enable organizations to realize the security of their information and information system. The standard enables the organization to create significant and unstoppable cyber security capability and process, i.e. a critical mass of cybersecurity, which will continuously build cybersecurity capabilities and established cybersecurity process in order to effectively manage their cybersecurity risks. This standard is issued by INSA pursuant to article 13 of INSA re-establishment proclamation execution council of ministers regulation no. 320/2014 [8]. This standard has the section which is clearly explained detail about what process need to follow to organize our country's cybersecurity risk assessment.

The many US and international organizations and businesses have adopted the National Institute of Standards and Technology (NIST) Special Publications as standards, even though those documents are published as guidelines for use by US Federal agencies. But this standard and others not suitable for our country context. Ethiopia critical mass cybersecurity requirement standard stated cybersecurity risk assessment framework should be strategic, tactical and operational level [8]. According to critical mass cybersecurity requirement standard, it's better to develop a cybersecurity risk assessment framework based on our country context.

2.8.1 Cyber Security Risk Assessment Standards and Framework

1. Critical Mass Cyber Security Requirement Standard

A secured cyber has a crucial impact on peace, development, and democracy of a country. The organization should understand that cybersecurity is an integral part of national interest and national security and, therefore, an integral part of their organization mission [8].

This critical mass cyber security standard has two main parts which are the foundation, guidelines for the development of the standard and main part of the standard requirement. Cybersecurity risk assessment process is one of the main parts of the standard requirement.

On this requirement standard clearly stated that "The risk assessment process should be based on national cybersecurity risk assessment methodology, the risk assessment should comprise of strategic, tactical (managerial) and operational (technical) assessment". Also, this requirement standard has cybersecurity strategic management model which have 3 dimensions: perspective (contains capability building, process, stakeholders), level (strategic, tactical and operational) and analysis dimension.

Analysis dimension explained in detail how strategic, tactical and operational level can be analyzed. The strategic level can be analyzed using SGOC (strength, gap, opportunity, and challenge) with PESTLE (political, economic, social, technological, legal, and environmental) in it. The tactical level can be analyzed using BMIS (governance, process, people, technology and the six dynamic interconnections that is governance, architecture, culture, emergence, enabling & support and human factor). The operational level can be analyzed using operational related clause of ISO27001 (operation, support, and relevant clauses).

The limitation/ gap of the standard is:

- The risk assessment process at the organization operational level doesn't consider or cover railways features as well information, safety, and security requirements. Also, it doesn't consider/solve a specific organizational problem related to the cyber security issue.

2. National Institute of Standards and Technology Special Publication 800-39 (NIST SP800-30)

National Institute of Standards and Technology (NIST) Special Publication 800-39 described risk assessment is one of the fundamental components of an organizational risk management process. The purpose of risk assessments is to inform decision-makers and support risk responses by identifying: (a) relevant threats to organizations or threats directed through organizations against other organizations; (b) vulnerabilities both internal and external to organizations; (c) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (d) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

The risk assessment process is composed of four steps: (a) prepare for the assessment; (b) conduct the assessment; (c) communicate assessment results, and (d) maintain the assessment. Each step is divided into a set of tasks.

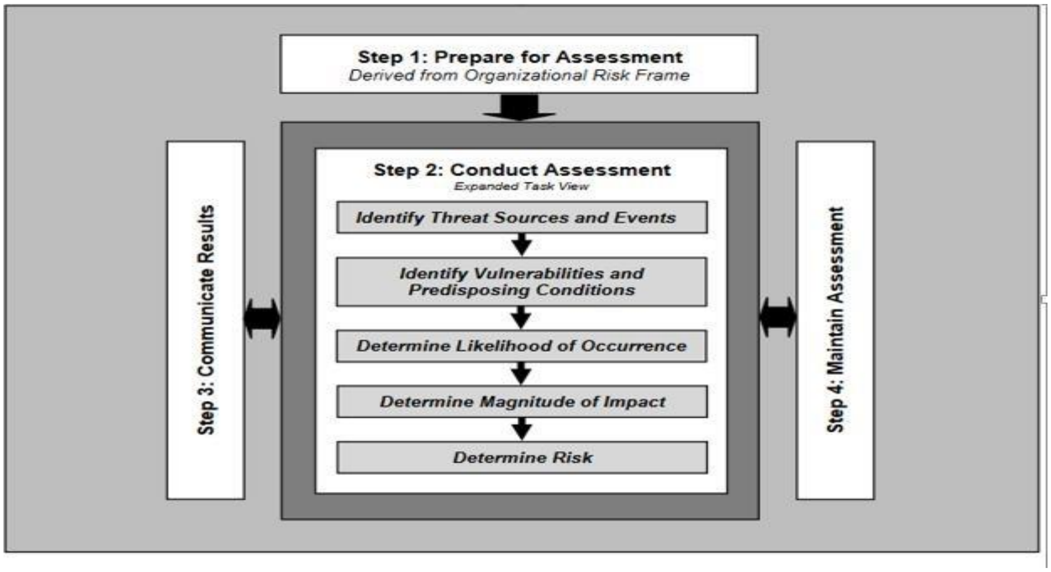

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Figure 2.2 Risk Assessment Process

The first step in the risk assessment process is to prepare for the assessment. The objective of this step is to establish a context for the risk assessment. According to NIST preparing risk assessment includes identify the purpose of the assessment, identify the scope of the assessment, identify the assumptions and constraints associated with the assessment, identify the sources of information to be used as inputs to the assessment and identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

The second step in the risk assessment process is to conduct the assessment. Theobjective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. This step also includes identify threat sources, identify threat events, identify vulnerabilities, determine the likelihood, determine the adverse impacts and determine risks.

The third step is to Communicate risk assessment results to organizational decision makers to support risk responses. Organizations can communicate risk assessment results in a variety of ways (e.g., executive briefings, risk assessment reports, dashboards).

The fourth step in the risk assessment process is to maintain the assessment. Theobjective of this step is to keep current, the specific knowledge of the risk organizations incur. The results of risk assessments inform risk management decisions and guide risk responses.

The limitation/ gap of the standard is:

- Risk assessment process not specific to the railways industry. Prepare for the assessment and maintain risk assessment steps not considering or cover railways features as well information, safety, and security requirements.
- Risk assessment process not considering strategic and tactical level risk assessment.

3. **International Standard Organization (ISO 27005)**

According to ISO 27005 Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment[19].

Risk assessment consists of the following activities:

a. Risk Identification
b. Risk analysis
c. Risk evaluation

The limitation/ gap of the standard is:

- Risk assessment process not specific to the railways industry. Context establishment and monitoring & review step not considering or cover railways features as well information, safety, and security requirements.
- Risk assessment process not considering strategic and tactical level risk assessment.

2.9 Review of Related Literature

As far as my investigation there are no research studies conducted in Ethiopia on cybersecurity risk assessment framework for the railways industry but there are two studies which are conducted on the financial sector in Ethiopia. Because of the following two aspects, this study is different from the study which is conducted in the financial sector:

- Methodology to conduct the study.
- Cybersecurity risk assessment process components. The study which is conducted in financial sector misses' important specific components to railways industry in Ethiopia such as cybersecurity strategic management awareness, establish system context, intrusion detection, and risk identification & evaluation update components.

However, the researcher identified rail cybersecurity standards prepared by other countries and studies published as journal articles. The following section explained in detail.

1. **The Risk Assessment of European Railway Traffic Management System (ERTMS)-Based Railway systems from a Cyber Security Perspective: methodology and Lessons Learned.**

This paper presents a high-level cybersecurity risk assessment of a national European railway traffic management system implementation. The researcher main concern was train movements rather than information, so their primary concern is integrity, then availability, and finally confidentiality. The put integrity, availability, and confidentiality as railways security requirements.

Loss of integrity could result in accidents or collisions, whereas loss of availability would bring the railway system to a halt. Loss of confidentiality is less of an immediate threat but might result in the leak of sensitive operational information. Reliability is also important since an unreliable train service will result in a loss of public confidence in the railway operators[20].

The main risk assessment steps are:

- The first step of risk assessment was to establish the system context and agree on the scope and motivation for the assessment with stakeholders. The major system assets and services were identified in order to ensure that the risk assessment was focused on high impact scenarios. Potential threat sources were identified and attack capabilities and impact levels were defined.
- The next step was to perform a preliminary risk analysis, identifying potential hazards and consequences, and relevant vulnerabilities and causes, together with any intrinsic mitigations and controls.

- The final step was to summarize the results of the risk analysis, identify areas of uncertainty, possible mitigations, and controls, and present the results of the risk assessment.

The limitation/ gap of the study is:

- Risk assessment process misses important international and national standard components such as strategic and tactical level risk assessment, determine likelihood, maintain risk assessment or monitoring and review components.
- Risk assessment process not considering railways industry in Ethiopia, it can't solve organizational problems related to cybersecurity risk assessment issues such as cybersecurity strategic management awareness, organizational structure, risk identification & evaluation update opportunity.

2. Cyber Security and Digital Railways: Risk and System Assessments Methodology and Capability

This paper mainly focuses on cybersecurity risk assessment and system assessment. The researcher uses 8 risk assessment stages:

Step 1 – Establish system context and scope of the assessment

Step 2 – Identify potential threat types

Step 3 – Refine and focus system models

Step 4 – Preliminary risk analysis

Step 5 – Identify specific attack scenarios

Step 6 – Focused risk analysis

Step 7 – Finalize risk assessment

Step 8 – Report results

The limitation/ gap of the study is:

- Risk assessment process misses important international and national standard components such as strategic and tactical level risk assessment, identify the asset, identify vulnerability & maintain risk assessment or monitoring and review components.
- Risk assessment process not considering railways industry in Ethiopia, it can't solve organizational problems related to cybersecurity risk assessment issues such as cybersecurity strategic management awareness, organizational structure, risk identification & evaluation update opportunity.

3. Rail Cyber Security: Australian Standard

This Rail cyber security standard specifies the requirements for Rail Transport Operators (RTO) for managing cyber security risk on the Australian Railway Network. Rail cybersecurity risk assessment and management requirement is one part of the standard.

This standard prepared based on the country legal and regulatory requirements. As stated on this standard "Rail transport operation shall develop and document an understanding of their cybersecurity threat context, which includes identifying threat source, the system architecture of the system, organizational structure and interface relevant to cyber security, and legal and regulatory requirements"[21].

Australian rail cyber security standard used NIST SP800-30 revision 1 guide for conducting risk assessments as a normative reference and the standard recommends risk assessment process of NIST SP800-30.

The limitation/ gap of the standard is:

- ➢ Risk assessment process not specific to the railways industry. Prepare for the assessment and maintain risk assessment steps not considering or cover railways features as well information, safety, and security requirements.
- ➢ Risk assessment process not considering strategic and tactical level risk assessment.

Table 2.5 the difference between standards and related studies

No	**Identified Risk Assessment process in international, national standards and related studies**	**Standards**				**Related Studies**	
		IS27O01	NISTSP800-300	National (Ethiopia)Cyber Security Requirement Standard	Australian Standard-Rail cybersecurity	Risk Assessment of ERTMS	Cyber Security and Digital Railways-Risk Assessment
1	Organizational strategic risk assessment	Not included	Not included	Included	Not included	Not included	Not included

2	Organizational Tactical risk assessment	Not included	Not included	Included	Not included	Not included	Not included
3	Organizational Operational risk assessment	Included	Included	Included	Included	Included	Included
	Step 1 Prepare for the assessment	Context establishment	Recommend to drive from organization risk frame	Context establishment	Recommend to drive from organization frame (adopted from NIST)	-Context establishment -Scope -motivation for the assessment	-Context establishment -Scope
	Step 2 Conduct risk assessment -Identify asset -Identify threat -Identify vulnerability -Determine likelihood -Determine impact -Risk evaluation	Included	Included	Included	Included	-Identify asset -Identify threat -Attack capability -Identify vulnerability -Determine impact -Mitigation, control -Summarize the result	-Identify threat -Risk analysis (Includes likelihood and impact and) -identify specific attack scenario -Summarize the result

	Step 3 Communicate the result	Included	Included	Included	Included	Not Included	-Report result
	Step 4 Maintain risk assessment	Monitoring and review	Included	Monitoring and review	Included	Not Included	Not Included

As we understand from the above table the national cybersecurity requirement standard (organization operational level risk assessment) and Australian rail cyber security standard recommend ISO27001 and NIST SP800-30 respectively.

International standards which are ISO 27001 and NIST SP 800-30 not specific to railways organization (do not address railways features as well safety & security needs). It's based on generic and universal guidelines.

Related studies which conducted on railways industry in other countries use a few components of the international standard risk assessment process.

Finally, the researcher summarized the gaps/limitation as follows:

1. The international standards don't consider or cover railways features such as layers and safety integrity level (discussed in chapter 5)
2. The international standards don't include specifically organizational critical problem related to awareness of top management and staffs(discussed in chapter 5)
3. The international standards don't consider or cover railways information, safety and security requirements such as intrusion detection (discussed in chapter 5)
4. Related studies which conducted on railways industry misses important international and national (Ethiopia) standard components such as strategic and tactical level risk assessment, identify asset, identify vulnerability & maintain risk assessment or monitoring and review (cyber security and digital railways- risk assessment), determine likelihood, maintain risk assessment or monitoring and review (risk assessment of ERTMS).
5. Related studies which conducted on railways industry misses' important Ethiopian Railways Corporation context (problems) components such as cybersecurity strategic management awareness, organizational structure, risk identification & evaluation update opportunity.

Finally, railways industry in Ethiopia should have well developed integrated cybersecurity risk assessment framework by considering national cybersecurity requirement standard, international standards, railways features, organizational critical problem, railways information, and safety and security requirements.

Chapter Three:

Research Methodology

3.1 Overview

This chapter discusses the procedure and methods used in carrying out the study. Design science research approach is conducted to accomplish the objective of the study. In this chapter research design approach, data collection and source, sampling technique, data analysis and interpreting the data will be discussed in detail.

3.2 Research Design

Research design is an action plan for getting from here to there, where there may be defined as the initial set of questions to be answered, and there is some set of conclusions (answers) about these questions. Between "here" and "there" may be found a number of major steps, including the collection and analysis of relevant data. As a summary definition, another textbook has described a research design as a plan that guides the investigator in the process of collecting, analyzing, and interpreting observations [22].

Another way of thinking about a research design is as a "blueprint' of research, dealing with at least four problems: what questions to study, what data are relevant, what data to collect, and how to analyze the results. The researcher used a design science research approach to improve the previous research and give suggestion for a problem solution on the existing theory. According to Pierce design research is sometimes called improvement research and this designation emphasizes the problem-solving/performance-improving nature of the activity. Suggestion for a problem solution is addictively drawn from the existing knowledge/theory base for the problem area [23].

Subsequently, the objective of the research is developing a cybersecurity risk assessment framework. Design science research approach is suitable for such kind of study because it is evidenced by many studies that the output of the design science approach is an artifact, construct, model and methods. The output of this study is also a model or framework. The following statement will strength this:

1. Design science creates and evaluates IT artifacts intended to solve identified organizational problems. Information technology artifacts are broadly defined as constructs (vocabulary and symbols), models (abstractions and representations),

methods (algorithms and practices), and instantiations (implemented and prototype systems) [24].

2. Design science knowledge is manifested in the form of artifacts—constructs, models, frameworks (Real or conceptual guides to serve as support or guide), architectures, design principles, methods, and/or instantiations—and design theories[23].
3. The utilitarian concern of construct and models, consider the research in an expert system where knowledge is modeled as a set of production rules or frame [25].
4. Design science research in the IS field is not limited to IT artifacts in the form of computer-based systems. Artifacts or solution technologies may include IS development methods, tools, and techniques, IS security and risk management practices and IS planning and management methods [26].

3.2.1 Design Science Research Approach

Design Science research approach in the Information Systems is a discipline in which new knowledge is produced by the construction and evaluation of artifacts such as software, composite systems of software, users and use processes and IS-related organizational methodologies and interventions [4], models, frameworks, theories [5]. The fundamental principle of design-science research is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact [24].

According to Denning (1997), design science is fundamentally a problem-solving paradigm which seeks to create innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, management and use of information systems can be effectively and efficiently accomplished. To effectively and efficiently design and manage a proposed risk assessment framework for information and cybersecurity, a design science paradigm was used.

The design science research paradigm is proactive with respect to technology as it focuses on creating and evaluating innovative IT artifacts that enable organizations to address important information-related tasks. The artifacts that are designed using this methodology are tested in a rigorous manner to solve complex, real-world problems, make research contributions that extend the boundaries of what is already known and communicate the results to appropriate audiences [24].

The authors agree on design science research method should consist of six main activities in nominal sequence. The following design science research approach process was applied in this study [27].

1. Problem identification and motivation.
2. Define the objectives for a solution.
3. Design and development, create the artifact.
4. Demonstration.

5. Evaluation
6. Communication

1. Problem Identification:

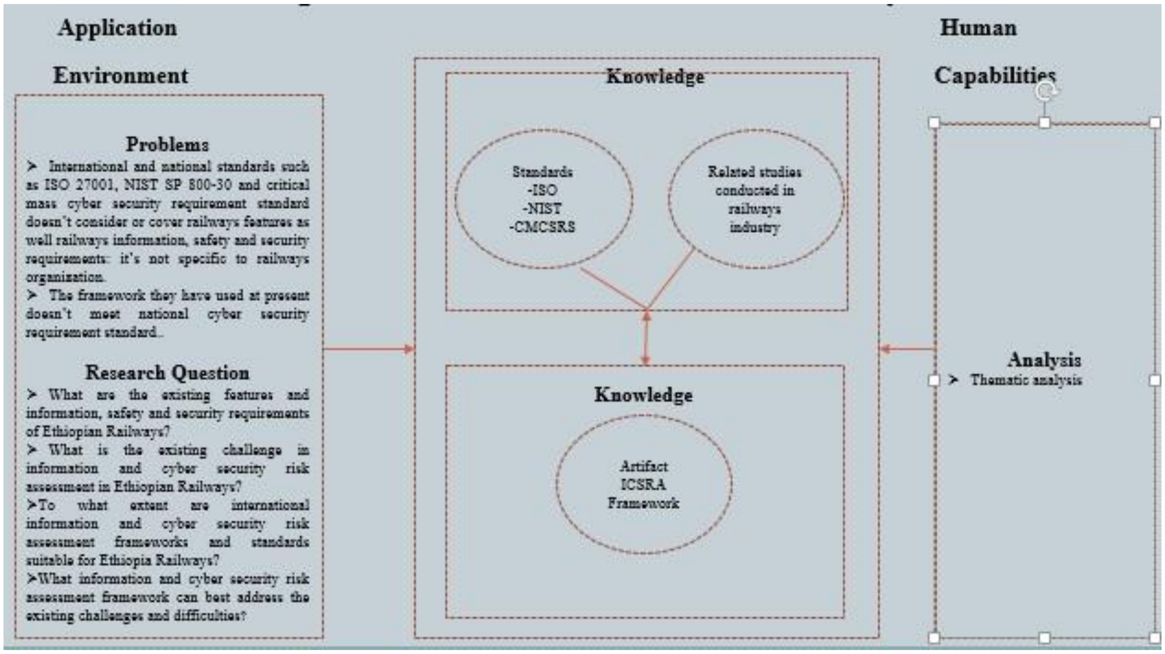
Ethiopia railways technology is a composition of several integrated systems such as signaling, communication, SCADA, management information and ticketing system. The researcher investigated the organization (ERC) is implemented cybersecurity risk assessment platform that is NIST SP 800-30. Though the organization adopted international risk assessment frameworks, it doesn't meet railway organization specific features as well information security need, not solve problems related to cybersecurity issues and not meet national cybersecurity requirement standard. So that the new cybersecurity risk assessment framework solution is considered national cybersecurity requirement standard, specific to the railways, railways feature and railways information security requirement.

2. The objective of the Solutions

The objective was to develop an integrated cybersecurity risk assessment framework for the railways industry in Ethiopia to improve the level of safety and security. The components in the framework enable the organization to assess risks in depth and it helps them to strong organizational safety and security.

3. Design and Development (Construct the Framework)

Based on the design science research process, the artifact (framework) was constructed. Application environment which is ERC and human capability has a contribution to the knowledge area which is the artifact, related standards, and related studies.



Problems

➤ International and national standards such as ISO 27001, NIST SP 800-30 and critical mass cyber security requirement standard doesn't consider or cover railways features as well railways information, safety and security requirements: it's not specific to railways organization.

➤ The framework they have used at present doesn't meet national cyber security requirement standard.

Research Question

➤ What are the existing features and information, safety and security requirements of Ethiopian Railways?

➤ What is the existing challenge in information and cyber security risk assessment in Ethiopian Railways?

➤To what extent are international information and cyber security risk assessment frameworks and standards suitable for Ethiopia Railways?

➤What information and cyber security risk assessment framework can best address the existing challenges and difficulties?

Figure 3.1 Design science research process application in the study

Qualitative data collection technique is used to collect the relevant data. The finding through thematic analysis is used to develop the framework. The framework is the artifact that supports Ethiopia Railways Corporation to assess organizational cybersecurity risks. The structure of the framework has a total of 13 components that conducts cybersecurity awareness program, cybersecurity department/risk assessment unit, established system context, purpose, scope, identify assets & intrusion detection, identify threats, identify vulnerability, determine likelihood, determine impact, risk evaluation, communicate result and risk identification & evaluation update opportunity.

4. Demonstration

After developing or constructing the framework, the researcher delivered to the user organization (ERC). The researcher used the framework with organization information technology, safety, and security department employee and received feedback that the framework is easy to use, specific to railways (solves the organizational problem). Finally, the researcher understands or recognize the framework is suitable for the organization.

5. Evaluation

Once the framework is constructed, the researcher uses a descriptive approach which is a scenario to evaluate the artifact's utility. The use of scenario in this study is purposeful because it can help to inform the corporation on the possibilities that may occur cyber incident and help the organization to be ready to protect its assets from a threat by doing risk assessment primary. The use of scenarios in design science is an acceptable and effective evaluation approach. Design evaluation methods as follows [24].

Scenarios are useful to describe the chain of the possibility of events and how the artifact may factor into those events. Also, the researcher uses a panel of expert's method to evaluate. Evaluation of the framework will be discussed in detail in chapter six.

6. Communication

The research was communicated through various publication mediums including the thesis. The work also is presented to Ethiopian Railways Corporation and INSA experts in the form of presentation.

3.3 Data Collection Method and Source

To understand cyber security risk assessment the data is collected from Ethiopian Railways Corporation and Information Network Security Agency. In this study, qualitative data collection technique is used to collect the relevant data. Once a theory or hypothesis is framed from the literature it can be used as initial guidance for data collection and data analysis.

For collecting data both primary and secondary data source has been used. Semi-structured interview method (in-depth) is used to get information about information and cybersecurity risk assessment standard, guideline and framework (see Appendix A and B). Because they provides valuable information from the context of participants (and stakeholder) experiences and use of pre-determined questions provide uniformity. In addition to this observation and document analysis have been used to get the relevant data.

The interview, observation, and document analysis focused on two business units such as Addis Ababa- Djibouti and Addis Ababa light rail transit. The respondents were selected based on their roles and position that have a direct relation with information technology, cyber security, safety and security, risk assessment and management which is information technology leaders, safety and security leaders, risk assessment team and INSA cybersecurity risk assessment unit.

Secondary data source like ERC safety and security procedures and policies that have been used to get information about cybersecurity risk assessment framework and safety and security majors for Railways industry.

3.4 Sampling Technique

In this study non-probability, purposive sampling technique has been used to select the respondent from railways organization and INSA that help the researcher understand the problem and the research question, theory, and framework. Purposive or judgmental sampling is a strategy in which particular settings persons or events are selected deliberately in order to provide important information that cannot be obtained from other choices [28].

The population for the study consisted of IT, safety and security, risk assessment professionals from Ethiopian Railways Corporation and INSA. The sample for the study was made up of professionals selected from Addis Ababa- Djibouti and Addis Ababa light rail transit, INSA risk assessment unit.

The total number of interviewees participated was 8 (sample size is eight). Current guidelines for thematic analysis are varied, ranging from around 2 to over 400 and itis unclear how to choose a value from the space in between[29].

3.5 Data Analysis Method

The selected data analysis method for this research is inductive thematic analysis because

- It’s suitable for qualitative data. Thematic analysis is frequently used to analyze qualitative data [29].

- The researcher wants to identify themes that are important points regarding the research data and shows a pattern or meaning related to data sets. An inductive analysis means that the recognized themes are strongly made related to the data [30]. TA is an approach for extraction of meanings and concepts from data and includes pinpointing, examining, and recording patterns or themes [31]. TA is a method for detection, analysis and reporting the themes in data [30].

The inductive approach is associated with qualitative data, whereas deductive approaches are more commonly associated with quantitative data. Once collected the required data the researcher follows the required steps to analyses the data. The main steps are presents as follows based on thematic analysis phases [30]:

1. Familiarization of the data: In this phase, the researcher read carefully to understand the collected data. It is necessary to read the whole set of data, before coding, in order to obtain an overall understanding.

2. Generate initial coding: In this phase, the researcher organized the data into the significant group and gave initial codes to the data. Create a preliminary list of ideas related to the data. Organize your data into significance groups and give the initial codes to the data[32]. The researcher also used margin note methods for writing codes. According to Javadi, Mostefa “Different methods for writing codes. For example, some software’s have been designed for this purpose and margin notes with different color”[30].

3. Searching for themes: In this phase, the researcher combined similar codes and formulated themes. The theme is the outcome of coding. The code is the label referred to special parts of the data that contribute to a theme [33].

4. Defining and naming themes: In this phase, the researcher name, describe each theme and how it related to the research question.

The frameworks, standards, guidelines and related studies that identified by literature review and the findings of the thematic analysis will be used to develop a cybersecurity risk assessment framework for Railways industry in Ethiopia.

Chapter Four:

Interpretation of the Data

4.1 Introduction

The data was collected from Ethiopia Railways Corporation and INSA. The total number of interviewees participated was 8. Six interviewees were involved from ERC (two from the IT department, 2 safety and security departments and the other 2 are from other departments) and two of them from INSA cybersecurity risk assessment unit.

This section describes the main finding through thematic analysis (TA). TA is an approach for extraction of meanings and concepts from data and includes pinpointing, examining, and recording patterns or themes[31].TA is a method for detection, analysis and reporting the themes in data[30]. Thematic Analysis is capable to detect and identify, e.g. factors or variables that influence an issue generated by the participants. Therefore, the participants' interpretations are significant in terms of giving the most appropriate explanations for their behaviors, actions, and thoughts[34]. The discussions are based on the following aspect to address the research question:

- ➢ Ethiopia Railways features as well as information, safety, and security requirements.
- ➢ Cybersecurity risk assessment framework & standard challenges and organizational difficulties.
- ➢ Extent/level to which international cybersecurity risk assessment frameworks and standards suitable for Ethiopia Railways.

4.2 Ethiopia Railways Features as well Information, Safety and Security Requirements

The data collected from interviewees are analyzed and discussed here based on the interview questions and answer (see Appendix A).

What are organizational/railways features as well as information, safety, and security requirements? The coding, themes, defining and naming explanation are presented as follows:

1. Coding: After reading the interview data many times, coding is performed based on repeated and very important words relevant to the research question. Repeatedly mentioned words and relevant to research questions are as follows:

Table 4.1: Coding

No	Codes	Words relevant to railways features as well as information, safety, and security requirements	Frequency of the words that appear in the responses (out of 6 respondents)
1	Code 1	Identification and Authentication of user	3
2	Code 2	Authorization	3
3	Code 3	Integrity and confidentiality	2
4	Code 4	Threat detection	4
5	Code 5	Attack detection	4
6	Code 6	Fail safe	2
7	Code 7	System failure and output is always safe	2
8	Code 8	ATS system	3
9	Code 9	SCADA system	3
10	Code 10	CBI system	4
11	Code 11	ATP system	3
12	Code 12	Wayside equipment	3
13	Code 13	Operation staff	3
14	Code 14	Supporting staff	2

2. Searching for Themes: Once coding is completed, merging of two or more similar codes in one theme was performed. As Braun & Clarke explain, there are no hard and fast rules about what makes a theme. A theme is characterized by its significance[35]. As examined in the above table some of the codes are clearly fitted: they are similar to each other. The themes are formulated by collecting these similar codes which are presented as follows:

Table 4.2: Searching for Themes

No	Codes	Themes
1	Identification Authentication Access privilege, Authorization Recording and registration Integrity and Confidentiality	Access control and management
2	Automatic train control system (ATS) SCADA Computer-based interlocking (CBI) Onboard signaling system (ATP) Wayside equipment	Layers of the railway's system
3	Fail-safe System failure and output is always safe	System reliability
4	Threat detection Attack detection	Intrusion detection
5	Operation staff Supporting staff	Personnel

3. Define and Naming Themes: This is the final refinement of the themes and the aim is to ‘identify the ‘essence’ of what each theme is about’[35]. This phase answered the following topics:

I. What is the theme saying?

- Access management theme describes who the user is who is granted the privilege and authorized to access the railway's system. All the activities on the system need to be recorded and registered. Integrity (railways systems technological software should have settings to block unwanted programs from running and unauthorized data storage devices from connecting to the system).
- Layers of railways system theme are described which layers (e.g. business, control, safety, communication, and line side) the organization assets are classified and levels of safety that the layers categorized. Based on the rail network (from outdoor equipment, onboard (train) equipment and indoor equipment) the order of the layers:
    - Line side (outdoor equipment’s)
    - Safety (onboard equipment’s)
    - Communication, control, and business (indoor equipment’s)
- System reliability theme describes the trustworthiness of the railway's system safety in case of failure (failsafe & system failure and output is always safe means the system guarantee the safety with the highest reliability in a critical situation when a fault occurs. Example is mentioned Appendix A).
- Intrusion detection theme is described as the tools for detecting and alerting railways personnel about threat information.
- Personnel theme is described by peoples who involves in the operation of railways.

II. How do they interact, relate to the main theme and which research question do the themes relate with?

Access management, system reliability, intrusion detection, and personal themes are railways information security requirements. Requirements for personnel, Physical protection requirements, Access management requirements, Requirements for data storage devices, Software requirements, Intrusion detection requirements, and Reliability requirements are information security requirements needed for equipment performing train and shunting control functions (Railway Automation and devices) and they're associated critically important facilities[12].

Layers of the system theme described railways system features. This theme is described in the established system context (see section 4.3).
This theme answer the following research question:

- What are the existing features and information, safety and security requirements of Ethiopian Railways?

4.3 Cyber Security Risk Assessment Framework & Standards Challenges and Organizational Difficulties

The data collected from interviewees are analyzed and discussed here based on the interview questions (see Appendix A).

Does the corporation have any cybersecurity risk assessment framework, standards and guideline to conduct cybersecurity risk assessment? If yes describe them. What are the strength and gap of the framework? What are the challenges facing the corporation while using this framework and recommendation to improve the framework? What is the difficulty in the organization related to cybersecurity and recommendation to solve this problem? The coding, themes, defining and naming explanation are presented as follows:

1. Coding: After reading the interview data many times, coding is performed based on repeated and very important words relevant to the research question. Repeatedly mentioned words and relevant to research questions are presented as follows:

Table 4.3 Coding

No	Codes	Words relevant to framework the organization using currently, strength, gap, challenges, organizational difficulties, recommendation to improve the framework and recommendation to solve difficulties.	Frequency of the words that appear in the responses (out of 6 respondents)
1	Code 1	NIST SP800-30	6
2	Code 2	Difficult to understand	4
3	Code 3	Difficult to use Recommended easy to use	3
4	Code 4	Generic (not explained in detail step 1 of risk assessment which is prepared for risk assessment and step 4 which is maintained risk assessment).	4

		Recommended that the standard should be specific to railways industry	
5	Code 5	Risk assessment detail process not focused on railways industry Recommended that risk assessment process should be focus railways industry in detail	5
6	Code 6	The organization doesn't have a cybersecurity strategy Recommended that the organization should have a cybersecurity strategy	5
7	Code 7	The organization doesn't have a cybersecurity policy Recommended that the organization should have a cybersecurity policy	5
8	Code 8	The organization doesn't have an annual plan and budget for a cybersecurity program Recommended that the organization should have a detail plan and budget	3
9	Code 9	The organization doesn't have a cybersecurity department Recommended that the organization should have a cybersecurity department	6
10	Code 10	The organization doesn't have a permanent cybersecurity risk assessment unit Recommended that the organization should have a permanent cybersecurity unit	3
11	Code 11	The organization doesn't have cybersecurity permanent responsible person Recommended that the organization should have cybersecurity permanent responsible person	2

12	Code 12	Doesn’t describe to what extent/covered risk assessment process conducted	5
13	Code 13	Doesn’t describe which railways systems area should be assessed	3
14	Code 14	Doesn’t describe how long risk assessment result will be used	4
15	Code 15	Doesn’t describe the aim of this program Doesn’t describe the objective of risk assessment	4

2. Searching for Themes: Once coding is completed merging of two or more similar codes in one theme was performed. As Braun & Clarke explain, there are no hard and fast rules about what makes a theme. A theme is characterized by its significance[35]. As examined in the above table some of the codes are clearly fitted: they are similar to each other. Collected these similar codes and put in themes is demonstrated as follows:

Table 4.4: Searching for Themes

No	Codes	Themes
1	-Difficult to understand -Difficult to use -Easy to use -Risk assessment detail process - Focus and specific to the railways industry in detail	Established system context
2	-Cybersecurity strategy -Cybersecurity policy -Annual plan and budget for a cybersecurity program	Cybersecurity strategic management awareness
3	-Cyber security department -Permanent cyber security risk assessment unit	Organizational structure

	-Permanent responsible person	
4	-The extent of coverage for the risk assessment process - Railways systems area to be assessed -For how long risk assessment result will be used	Scope and Time
5	-The objective of risk assessment	Purpose

3. Define and Naming Themes: This phase answered the following topics:

I. What is the theme saying?

- Established system context theme describes the railway's system, assets, and layers with its safety level. The theme concept is all about specific railways system.
- Cybersecurity strategic management awareness theme is described top management and staffs awareness for cyber security culture& risk as well cybersecurity strategy and policy.
- Organizational structure theme is described organization cyber security structure and responsibility.
- Scope and time theme is described extent of the risk assessment process (business units, railways system and for how long).
- Purpose theme defines the objective of cybersecurity risk assessment process.

II. How do they interact, relate to the main theme and which research question the themes related?

All themes are derived from the organization and the themes are railways industry context. They are specific to the organization. These themes are answers to the following research question:

- What is the existing challenge in cybersecurity risk assessment in Ethiopian Railways?
- What cybersecurity risk assessment framework be developed that can best to address the existing challenges and difficulties?

4.4Extent/Level to which International Cyber Security Risk Assessment Frameworks and Standards Suitable for Ethiopia Railways

The data collected from interviewees are analyzed and discussed here based on the interview questions (see Appendix A).

Does the corporation have any cybersecurity risk assessment framework, standards and guideline to conduct cybersecurity risk assessment? If yes, to what extent the framework is suitable for Ethiopia Railways? The coding, themes, defining and naming explanation as follows:

1. Coding: After reading the interview data several times, coding is performed based on repeated and very important words relevant to the research question. Repeatedly mentioned words, phrases, and statements which are relevant to research questions are presented as follows:

Table 4.5 Coding

No	Codes	Words relevant to what extent the framework is suitable for Ethiopia Railways	Frequency of the words that appear in the responses (out of 6 respondents)
1	Code 1	Interlocking system, automatic train supervision system, automatic train control system, supervisory control, and data acquisition system	5
2	Code 2	Financial information, employee information, design documents, trainmasters operation daily record, operation control center records, maintenance records, and service level agreement document with a contractor	5
3	Code 3	Workflows and procedure manuals	5
4	Code 4	Internetworking and communication devices, wayside signaling and commination equipment's, train, optical fiber cables, e operation maintenance client software, e sight ICT unified network management system	5

5	Code 5	Operation staffs, users and support staffs	5
6	Code 6	Hackers	5
7	Code 7	Intruders	5
8	Code 8	Attackers	5
9	Code 9	Fire	5
10	Code 10	Flood	5
11	Code 11	Earth quake	5
12	Code 12	System weakness	5
13	Code 13	Physical weakness	5
14	Code 14	Document weakness	5
15	Code 15	Process weakness	5
16	Code 16	Awareness weakness	5
17	Code 17	Very low	5
18	Code 18	Very high	5
19	Code 19	High	5
20	Code 20	Low	5

21	Code 21	0-100 scale	5
22	Code 22	Low or non-existing	5
23	Code 23	High or critical	5
24	Code 24	Injury	5
25	Code 25	Death	5
26	Code 26	Disruption of railways operation	5
27	Code 27	Economic lose	5
28	Code 28	Decision making	5
29	Code 29	Risk analysis	5
30	Code 30	Determine impact vs determine likelihood	5
31	Code 31	Reporting method	5
32	Code 32	Elements of result/report	5
33	Code 33	Risk identification, evaluation, and update opportunity	5
34	Code 34	How many times the risk assessment process should be updated	5

2. Searching for Themes: Once coding is completed merging of two or more similar codes in one theme was performed. As examined in the above table some of the codes are clearly fitted: they are similar to each other. Collecting these similar codes and put in themes is done as follows:

Table 4.6: Searching for Themes

No	Codes	Themes
1	- Interlocking system, automatic train supervision system, automatic train control system, supervisory control, and data acquisition system -Financial information, employee information, design documents, trainmasters operation daily record, operation control center records, maintenance records, and service level agreement document with the contractor - Workflows and procedure manuals -Internetworking and communication devices, wayside signaling and commination equipment's, train, optical fiber cables, e operation maintenance client software, e sight ICT unified network management system - Operation staffs, users and support staffs	Assets
2	-Hackers - Intruders -Attackers - Fire - Flood - Earthquake	Threat
3	- System weakness - Physical weakness - Document weakness - Process weakness	Vulnerability

	- Awareness weakness	
4	- Very low - Very high - High -Low -0-100	Likelihood
5	- Low or non-existing -High or critical -Injury -Death - Disruption of railways operation - Economic loss	Impact
6	- Decision making - Risk analysis - Determine impact vs determine the likelihood	Risk evaluation
7	- Reporting method - Elements of result/report	Communicate result
8	- Risk identification, evaluation, and update opportunity - Risk assessment process update	Risk identification, evaluation, and update

3. Define and Naming Themes: This phase answered the following topics:

I. What is the theme saying?

- Asset theme describes anything that has value to the organization and is necessary for achieving its objectives.
- Threat theme is about anything that could have a potential impact on organizational assets.

- Vulnerability theme is all about the weakness in defense.
- Likelihood theme tells about the chance that threat event happen.
- Impact theme describes the consequence of possible cyber-attack.
- Risk evaluation theme is about to determine the likelihood of occurrence and determining impact.
- Communicate result theme states about communicating operational results to organizational decision makers to support risk response.
- Risk identification & evaluation update theme is described in what situation the organization should update the risk assessment result.

II. How do they interact, relate to the main theme and which research question the themes related?

All themes are processes of international standard risk assessment. All these themes belong to risk identification, risk analysis, risk evaluation, communicate result and maintain risk assessment steps.

These themes are answers to the following research question:

- To what extent are international cybersecurity risk assessment frameworks and standards suitable for Ethiopia Railways?

Chapter Five:

The Proposed Cyber Security Risk Assessment Framework

5.1 Introduction

The research objective addressed in this chapter is the development of an integrated cybersecurity risk assessment framework for the railway's industry based on the findings derived from data collected through interview and observation. The literature/documents reviewed in the area of national cybersecurity requirement standard, NIST SP 800-30, ISO 27001 and related studies in the railway's industry contributed to the development of the framework. It enhances the existing framework/risk assessment process.

National cybersecurity requirement standard recommends organizations in Ethiopia to follow the risk assessment process which is stated/described in the document. The structure has 3 main levels that are national, sectoral and organizational layers. The entire purpose of the study is to amend the national cybersecurity risk assessment process at the organizational level.

The proposed framework components/parameters that are derived from collected data and their relationship with the national standard and international standard is presented as follows:

1. Cybersecurity strategic management awareness

Strategic management parameter is derived from the data collected through interview. The standards which are discussed in the chapter of the related work does not include the specific parameters relevant for Ethiopian Railway's Industry's context. One of the missing parameters in prior standards but found by the study is Cybersecurity strategic management awareness in Ethiopian Railways Corporation. It is believed that it will have various significances. For instance:-

- It will support the organization to have a cybersecurity culture.
- It will help to create awareness for the top management and staffs about cyber risks.
- It will help the organization to recognize &prepare cybersecurity strategy and policies.

2. The organizational structure established system context, purpose, and scope &time

ISO27001 puts the parameters as a generic term like context establishment, NIST SP800-30 also used a generic term like preparing for the assessment. In addition, related studies identified in this paper study didn't include organizational structure, purpose, and scope & time parameters. The findings derived from data collected through interview indicated and supported that all the parameters are key components to prepare for organizational risk assessment.

3. Identify asset, identify the threat, identify vulnerability, determine likelihood, determine impact, risk evaluation, communicate the result and monitoring and review International standards put this parameter in terms of risk identification, risk analysis, risk evaluation, communicate the result and monitoring and review. The researcher finding derived from data collected through interview indicated and supported that all the parameters are key components to conduct a risk assessment (all parameters exist in the international standards and there is no new finding).

4. Identify intrusion detection (together with identify asset parameter)

Intrusion detection is one of railways organization information security requirement. Requirements for personnel, physical protection requirements, access management requirements, requirements for data storage devices, software requirements, intrusion detection requirements, and reliability requirements are information security requirements needed for equipment performing train and shunting control functions (Railway Automation and devices) and they're associated critically important facilities[1].

Based on the finding derived from data collected through the interview the researcher identified the above requirements as unique organizational information security need but six requirements out of seven can be assessed by existing risk assessment parameters. But to strengthen railways organization cybersecurity, it's better to asses/identify intrusion detection align with asset identification.

Even if international standards categorized all type of organization software's/tools inside asset parameter, it is better to focus intrusion detection tools separately (aligned with asset identification parameter) to strengthen railways organization cybersecurity because the finding shows us intrusion detection requirement is one of organizational information security need and international standards doesn't consider these unique information securities need separately. The following statement from literature strengthens the claim.

International standards do not pay attention to organizational differences. Such guideline does not address the organization's own and unique, information security need, but prescribe universal or general procedure" [7].

Table 5.1 Summarization of how the proposed integrated framework is derived from empirical data and pertinent standards

Questioner	Code (important words) generated from Questioner	Theme (parameter) generated from code		The research question answered by the theme	Proposed framework parameter
		Themes derived from empirical data	**Themes derived from international standards & supported by empirical data**		
What are organizational/railways features as well as information, safety, and security requirements?	-Automatic train control system (ATS) -SCADA -Computer-based interlocking (CBI) -Onboard signaling system (ATP) -Wayside equipment -Threat detection -Attack detection	-Layers of the railway's system -Intrusion detection		What are the existing features as well as information, safety and security requirements of Ethiopian Railways?	-Part of establishing system context -Presented with asset identification parameter
Does the corporation has any cyber security risk assessment framework, standards and guideline to conduct cyber security risk assessment? If yes describe them. What are the strength and	Refer table 4.3	-Established system context - Cybersecurity strategic management awareness		-What is the existing challenge in cybersecurity risk assessment in Ethiopian Railways? -What cybersecurity risk assessment framework be developed that can best to address the existing challenges and difficulties?	-Established system context -Cybersecurity strategic management awareness - Organizational structure

gap of the framework? What are the challenges facing the corporation while using this framework and recommendation to improve the framework? What is the difficulty in the organization related to cybersecurity and recommendation to solve this problem?		-Organizational structure -Scope -Purpose			-Scope& Time -Purpose
Does the corporation have any cybersecurity risk assessment framework, standards and guideline to conduct cybersecurity risk assessment? If yes, to what extent the framework is suitable for Ethiopia Railways?	Refer table 4.5	Supported by empirical data	- Assets - Threat - Vulnerability - Likelihood -Impact -Risk evaluation -Communicate result -Maintain risk assessment	To what extent are international cybersecurity risk assessment frameworks and standards suitable for Ethiopia Railways?	-Identify asset -Identify threat -Identify vulnerability -Determine the likelihood -Determine the impact -Risk evaluation -Communicate result -Risk identification & evaluation update

5.2 National Cyber Security Risk Assessment

The structure of the national cybersecurity risk assessment process has 3 main layers that are national, sectorial/Transportation sector and organizational/Ethiopian Railways Corporation.

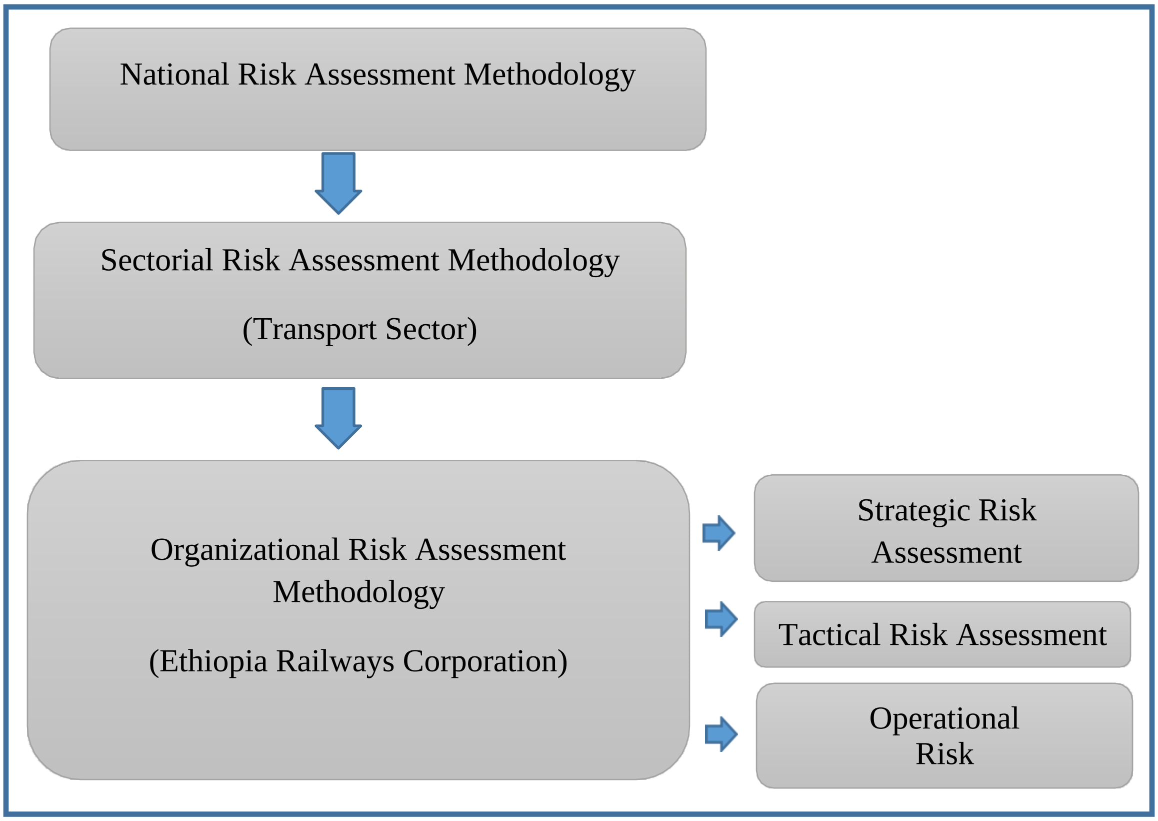

National Risk Assessment Methodology
Sectorial Risk Assessment Methodology
(Transport Sector)
Organizational Risk Assessment Methodology
(Ethiopia Railways Corporation)
Strategic Risk Assessment
Tactical Risk Assessment
Operational Risk

Figure 5. 1 National Cyber Security Risk Assessment Layer

National Cybersecurity requirement standard illustrated as risk assessment process should be based on national cybersecurity risk assessment methodology. One of the finding through an interview with the employee of INSA is that the national cybersecurity risk assessment methodology is being prepared and not implemented yet.

Sectorial risk assessment methodology includes strategic, tactical (managerial) and operational (technical) risk assessment profile. The strategic risk assessment of the sector should focus on sectorial strategic risk. The strategic risk assessment can be analyzed using SGOC (strength, gap, opportunity, and challenge) with PESTEL (political, economic, social, technological, legal and environmental) in it. The tactical/ managerial risk assessment is based on BMIS (governance, process, people, technology and the six dynamic interconnections that is governance, architecture, culture, emergence, enabling & support and human factor) [8].

The organizational level risk assessment process also has 3 main level that is strategic, tactical/managerial and operational level.

5.3 Proposed Cyber Security Risk Assessment Framework

The organizational level risk assessment process also has 3 main level that is strategic, tactical/managerial and operational level.

Strategic & tactical risk assessment process are properly represented in the national cybersecurity requirement standard. Besides the researcher haven't identified any new aspect from the gathered data and recommend to adopt the national strategic & tactical risk assessment methodology. But the researcher organized/customized these process and discussed in detail regarding Ethiopia Railways Corporation. See Appendix C [8]. The detail discussion only focuses on an organization's operational level risk assessment process which is the area in which the study made a contribution.

As it is indicated in the statement of the problem and chapter 4 of this study the main area of the contribution of this research is in the organization's operational risk assessment process since the existing national and international standards haven't considered this layer which involves highly contextual issues. The study derived key parameters to be included in the newly proposed framework from the empirical study conducted. This section, therefore, presents a discussion on the proposed framework for an organization's operational risk assessment level.

The operational risk assessment is focused on organizational technical risk. This risk assessment should be based on the organizational strategic risk assessment, organizational managerial risk assessment, and national technical risk profile.

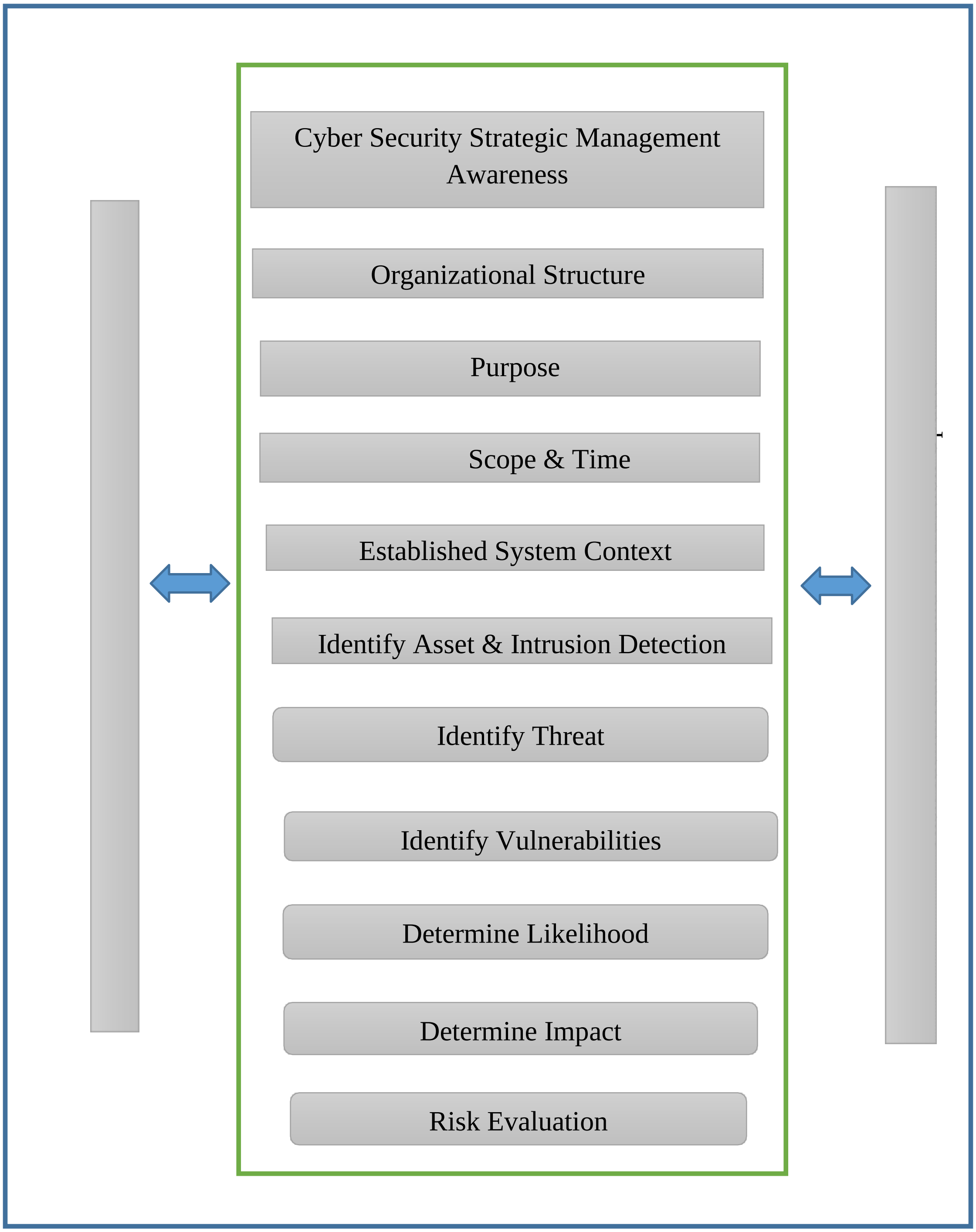


Figure 5. 2 Cyber Security Risk Assessment Framework

1. Cyber Security Strategic Management Awareness

Conducting awareness about a cybersecurity-related issue such as strategy & policy to the leader (top management) and staffs is very crucial. It will support to have cyber security culture in the organization and helps the leader to focus on cyber risk, to implement employee awareness training and initiate to conduct a risk assessment.

Building awareness into the organization culture, it increases the ability to address cyber risk. Leadership involvement is critical for cybersecurity organization. Leaders are significant to guaranty cyber secure culture in the organization and implementing employee awareness training:-these programs build an understanding of risks, and—most importantly—provide specific steps for mitigating them[36].

Principle

First, a cyber-security awareness program should be defined and conducted for all management members, staffs and stakeholders of Ethiopian Railways Corporation.

Objective

The main purpose is to create a cyber-security risk-aware culture where the management members and staff make effective risk-based decisions which protect the organization's assets. Besides it will help railways organization top management, middle management, front management, engineers, experts, technicians, and stakeholders to have knowledge on cybersecurity, cyber risks and impact of cyber-attack on the railway's organization as well as the country.

Considerations

- ➢ The cybersecurity awareness programs should be defined, approved and conducted to promote cyber security awareness and to create a positive cyber security culture.
- ➢ A cybersecurity awareness program should be defined and conducted for:
  a. Management members of Ethiopian Railways Corporation;
  b. The staff of Ethiopian Railways Corporation;
  c. Stakeholders of Ethiopian Railways Corporation. The cybersecurity awareness program should target cyber security behaviors to address the different target groups through multiple channels.
- ➢ The activities of the cybersecurity awareness program should be conducted periodically and throughout the year.
- ➢ The cybersecurity awareness program should at a minimum include:

a. An explanation of cybersecurity actions;
b. The roles and responsibilities regarding cyber security;
c. Information on relevant emerging cybersecurity events and cyber threats.

- The cybersecurity awareness program should be evaluated to:
    a. Measure the effectiveness of the awareness activities;
    b. Formulate recommendations to improve the cybersecurity awareness program.

2. Organizational Structure

Ethiopia Railways Corporation should establish cybersecurity department in the organization structure. To conduct cybersecurity risk assessment the organizational risk assessment unit should be organized under cyber security department. This department should have authority over cybersecurity matters in the organization.

The main purpose of organizing cybersecurity department is to create capability building in the organization and to conduct cybersecurity tasks of the organization including risk assessment. The following statement from literature strengthens the above claim.

The objective of capacity building is to create competent institutional structure and security governance that continuously build human capability & assures the execution of organization cybersecurity program[8]. Cybersecurity risk assessment is one of a cyber security program.

The director of this department should be a member of ERC top management team. The organization should have a representative in the highest level of management who fully engages in the cybersecurity program of the organization. This person should lead the cyber department and security committee of the organization [8].

3. Purpose

Identify the purpose of the risk assessment in the railway's organization in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.

- ERC should specify the method and procedure for hazard/ risk identification, risk evaluation, and control.
- Based on risk assessment result ERC should prepare risk control/risk management procedure.

4. Scope& Time

The risk assessment process should apply in both business unit of Ethiopian Railways Corporation, namely:

- Addis Ababa Light Rail Transit Service;
- Addis Ababa Djibouti Railways.

The main focus of risk assessment in the railway's organization should be on the signaling system and communication system that could have a major national impact, namely:

- Attacks that result in unsafe train movements, which could cause a train accident with considerable loss of life;
- Attacks that result in loss of service, which could lead to major transport disruptions.

The scope should also include the entire railway's system that has a direct or indirect relation with information and cybersecurity.

- Signaling system
- Communication system
- SCADA
- Ticketing system
- Operational issue
- Process
- People

Ethiopia Railways Corporation should determine for how long the results of particular risk assessments can be used:

- Organization hazard identification and risk evaluation & control procedures document recommend the process shall be organized at least once a year.
- National cybersecurity requirement standard recommends the process should be updated every 3 months.

5. Established System Context

Ethiopian Railways system is designed based on information technology and automation system. Our country railways system also relies on railways industry technology demand such as control train movement, power delivery to the network, supervisory control and data acquisition, management information system, signaling, and communication system and infrastructure, operational planning and timetable.

The following discussions with network rail, I demonstrated the critical railway system as a series of layers. Based on the rail network (from outdoor equipment, onboard (train) equipment and indoor equipment) the layers hierarchy is:

- Line side (outdoor equipment's)
- Safety (onboard equipment's)
- Communication, control, and business (indoor equipment's)

Table 5.2 summarizes the functionality provided by each layer and the required safety integrity level (SIL)

Table 5.2 Railways Layer

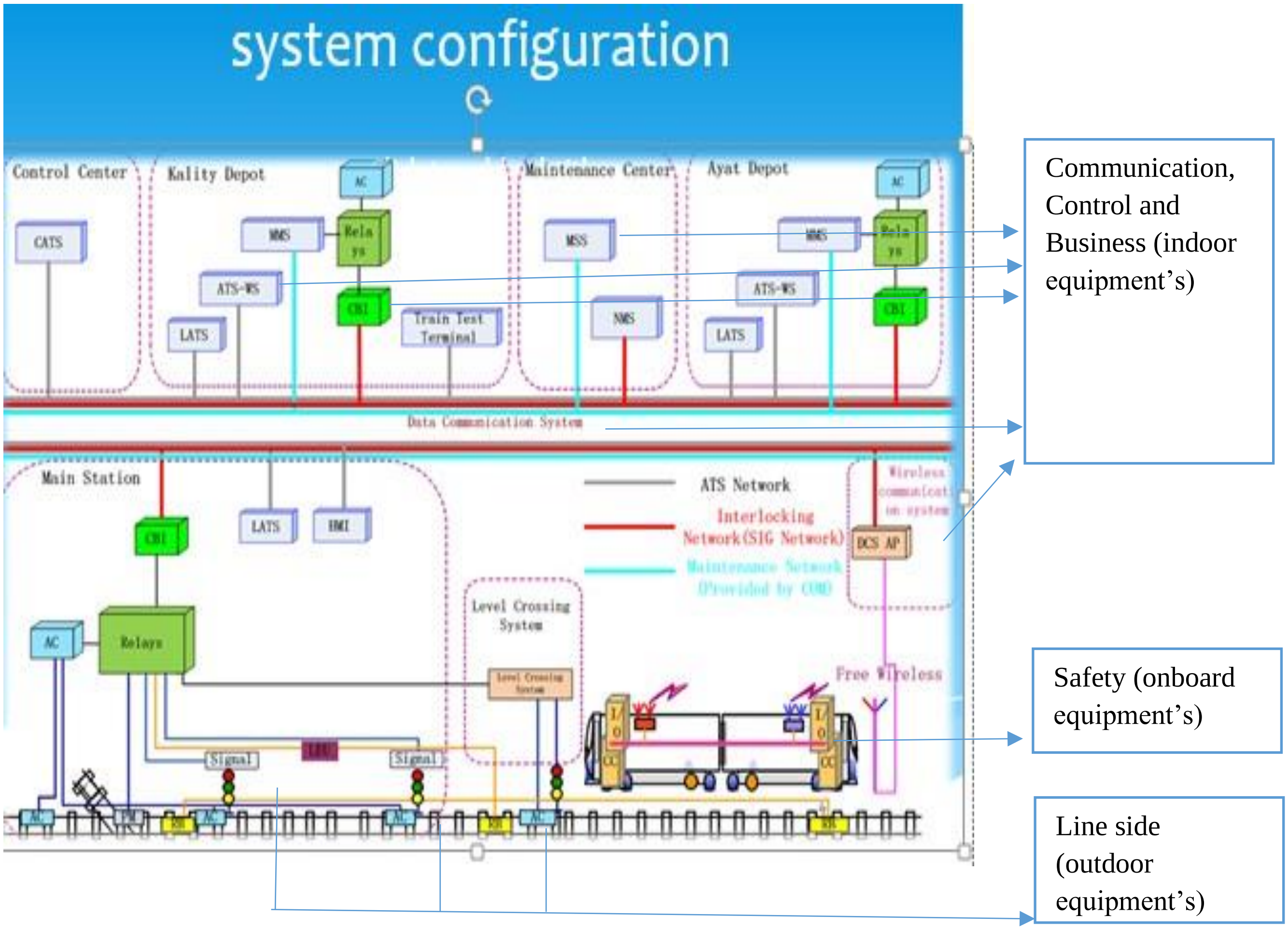
Layers	**Safety Integrity Level[20]**	**Functionality**
Line side	SIL 4	➢ Axle counters (AC) ➢ Beacon, switch machine
Safety	SIL 4	➢ Onboard signaling system (ATP)
Communication	SIL 0	➢ Transmission system ➢ Data communication system ➢ Wireless communication system
Control	SIL 2	➢ ATS ➢ A central train control system ➢ SCADA ➢ Computer-based interlocking (CBI)
Business	SIL 0	➢ Time table ➢ Maintenance support system

A safety integrity level (SIL) is defined in IEC 61508-4 as "a discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems, where level 4 has the highest level of safety integrity and level 0 has the lowest" [37].

Integrity levels are selected by associating each level with a given severity as follows: [38].

- SIL 1 - represents the integrity required to avoid relatively minor incidents and is likely to be satisfied by a certain degree of fault tolerant design using guidelines that follow good practice.
- SIL 2 - represents the integrity to avoid more serious, but limited, incidents some of which may result in serious injury or death to one or more persons.
- SIL 3 - represents the integrity required to avoid serious incidents involving a number of fatalities and/or serious injuries.
- SIL 4 - represents the integrity level required to avoid disastrous accidents.

Fig 5.3 provides a high-level overview of the architecture of the Addis Ababa Light Rail Transit system. The diagram illustrates the main interactions between the various layers and system components, and the criticality of each layer (SIL 0, SIL 2, and SIL 4).



Communication, Control and Business (indoor equipment's)

Safety (onboard equipment's)

Line side (outdoor equipment's)

Figure 5. 3Addis Ababa Light Rail Transit System Architecture

6. Identify Asset& Intrusion Detection

Identify Asset

Ethiopia Railways Corporation should identify all type of assets based on layers mentioned in the establish system context section:

- Mission critical system such as interlocking system, automatic train supervision system, automatic train control system, supervisory control, and data acquisition system.

- Information assets such as financial information, employee information, design documents, trainmasters operation daily record, operation control center records, maintenance records, and service level agreement document with the contractor.
- A process such as inter and intra department workflows and procedure manuals
- Hardware, software, networks such as internetworking and communication devices, wayside signaling and commination equipment's, train, optical fiber cables, e operation maintenance client software, e sight ICT unified network management system and others.
- People such as operation staffs, users and support staffs.

An asset is anything that has value to the organization and is necessary for achieving its objectives. A business asset describes information, processes, capabilities, and skills inherent to the business and core mission of the organization, having value for it. An information system asset is a component of the IS supporting business assets like a database where information is stored. An information system is a composition of hardware, software, network, people and facilities [39].

Organizations must identify critical assets in this phase of the process. Identifying which assets are critical can be subjective based on the individual or group conducting the assessment. It is the responsibility of the information security professional to evaluate assets based on their criticality when compared to the overall list of assets [40].

Intrusion Detection

Intrusion detection is one of the railway's information security requirements. Ethiopian Railways Corporation should include/consider in the risk assessment process. The organization should identify tools for detecting and alerting users about information threats.

Moreover, the following information should be registered:

- Information on detected network traffic anomalies.
- Type of detected threats, date and time of threats detection.
- IP addresses of the source and object of the threats.
- Port number of the source and object of the threats.
- Detected threats priority level.

7. I<span>de</span>**ntify Threat**

Ethiopia Railways Corporation should compile a list of threats that could potentially have an impact on organizational assets. Compile a list of threats requires that the organization have the extensive railway's industry knowledge and the assistance of trained professionals who are capable of accurate forecasting.

Threat Source

After the identified threat, the railway organization should identify the threat source. The threat-source can be internal or external.

Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats. Organizations identify threat sources of concern and determine the characteristics associated with those threat sources. For adversarial threat sources, assess the capabilities, intentions, and targeting associated with the threat sources. For non-adversarial threat sources, assess the potential range of effects from the threat sources [41].

Deliberate threat sources can be broken in the following categories: [21]

A. Internal actors (staff, contractors and service providers)

- Operational Staff
- IT and OT Engineering Staff
- Contractors and Service Providers
- Supply-chain Partners
- Staff, not otherwise classified.

B. External actors

- Cyber terrorists
- Issue-motivated groups
- Former staff and contractors
- Cybercrime groups
- Nation-state actors
- General Hackers.

Besides, the organization should identify Non-human threats like a natural disaster (fire, flood, and earthquake)

Threat Event

Ethiopian Railways Corporation should determine which type of threat events are to be considered during risk assessments and the level of detail needed to describe such events.

Descriptions of threat events can be expressed in highly general terms (e.g., phishing, distributed denial-of-service), in more descriptive terms using tactics, techniques, and procedures, or in highly specific terms (e.g., the names of specific information systems, technologies, organizations, roles, or locations). In addition, organizations consider: (i) what representative set of threat events can serve as a starting point for the identification of the specific threat events in the risk assessment; and (ii) what degree of confirmation is needed for threat events to be considered relevant for purposes of the risk assessment [41].

Threat Action

When a threat assessment is developed, it is important to consider likely and possible modes of action. The technical act of hacking will be a component of these threats. Often the actual group performing the technical breach can be commissioned by the primary threat i.e. a hackers-for-hire. This can be because of technical capability or to maintain a certain degree of deniability. It is common for the threat actors to be a complex combination of actions. For example, a terror group could use a kinetic attack to disable control system while using hacking to identify vulnerable points to attack, to gain access to controlled areas, disable monitoring systems, or attack services required to run the railway such as power reticulation [21].

8. Identify Vulnerability

Vulnerabilities are contributing factors that make assets capable of being leveraged by threat sources. The existence of a vulnerability is an essential piece of the measurement when calculating the probability of an event occurring. Vulnerability assessment can be even more difficult in some cases than threat identification because it requires that organizations know the specific weaknesses of their assets [40].

Ethiopian Railways Corporation should identify the weakness of the entire railway's system that could be the gate of threats. Identify the weakness of

- Communication and signaling system
- Network.
- Policy and procedure.
- Architecture and design.
- Configuration and maintenance.
- Physical intrusion.
- Lack of training and awareness.

9. Determine the Likelihood

The railway's organization should determine the likelihood that threat events of concern result in bad impact by considering the characteristics of the treat sources, the vulnerabilities and the organization countermeasure implemented or planned to slow the progress of threat events.

Organizations employ a three-step process to determine the overall likelihood of threat events [41].

- First, organizations assess the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events).

- Second, organizations assess the likelihood that threat events once initiated or occurring, will result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation.
- Finally, organizations assess the overall likelihood as a combination of the likelihood of initiation/occurrence and likelihood of resulting in adverse impact

Once determining the likelihood of occurrence:

- The railway's organization should assign a qualitative or quantitative value to each threat in order to compare one event to another. A range of likelihood of threat events can range from 0-100 on a scale or very low to very high.

10. Determine Impact

- Ethiopia Railways Corporation should identify and assess the consequence of possible cyber-attack first.
- Then, impact assessment can be assigned a quantitative or qualitative rating based on the comparison of impacts. The comparison is calculated based on the impact that has the potential to cause dangerous disasters such as injury or death of railways travelers, disruption to efficient railways operation, reputation damage, and misinformation to public, stakeholders, suppliers and economic loss.

The impact must be measurable, but can be based on quantitative data and qualitative data depending on the threat and the asset. Quantitative risk assessments deal with estimating the loss from a monetary perspective using calculations such as the Single Loss Expectancy, Annualized Rate of Occurrence and Annualized Loss Expectancy. In order to use this method, there must be numbers associated with loss. Qualitative risk assessment, on the other hand, is not as easy to calculate therefore organizations must use relative values to assign to the potential impact of an event. Levels typical range from low or nonexistent to high or critical and even though it is not quantitative using real numbers an event of critical impact could still result in a significant financial loss [40].

In calculating the impact of a threat/hazard, an organization should consider not only the legal, economic and reputational impact of the immediate event but also the impact on the broader industry and the public’s confidence in transport systems [21].

11. Risk Evaluation

Once determine the likelihood of occurrence and determining impact the railway's organization should evaluate the risk. On this step level of risks should be compared against risk evaluation and risk acceptance.

- Ethiopia Railways Corporation should make a decision about the future based on the understanding of risk obtained by risk analysis (the chance that threat event occurs and the impact such as injury or death of railways travelers, disruption to efficient railways operation).

- Then, the decision should include whether an activity should be undertaken and priority for risk treatment considering the estimated level of risk.

Risk evaluation criteria used to make a decision should be consistent with the defined external and internal information security risk management context and take into account the objective of the organization and stakeholders. The decision as taken in the risk evaluation activity mainly based on an acceptable level of risk. However, consequence, likelihood, and the degree of confidence in the risk identification and analysis should be considered as well [42].

Risk evaluation consideration should include:

- Information security properties
- The importance of the business process or activity supported by a particular asset or set of asset

12. Communicate Result

The railway's organization should communicate operational results to organizational decision makers which are to leaders to support risk response. In addition to this, the communication should include a sectoral level that is the transport sector.

Ethiopian Railways Corporation should communicate risk assessment results in a variety of ways:

- Briefings (meeting) to management members.
- Preparing risk assessment reports
- Using dashboards.

The essential elements of information that organizations can use to communicate the results of risk assessments include an executive summary, the main body containing detailed risk assessment results and supporting appendices [41].

Elements or contents of the result:

Executive Summary

- List the date of the risk assessment.
- Summarize the purpose of the risk assessment.
- Describe the scope of the risk assessment.
- State whether this is an initial or subsequent risk assessment. If a subsequent risk assessment, state the circumstances that prompted the update and include a reference to the previous Risk Assessment Report.

- Describe the overall level of risk (e.g., Very Low, Low, Moderate, High, or Very High).
- List the number of risks identified for each level of risk (e.g., Very Low, Low, Moderate, High, or Very High).

Body of the Report

- Describe the purpose of the risk assessment, including questions to be answered by the assessment. Identify assumptions and constraints.
- Describe risk tolerance inputs to the risk assessment (including the range of consequences to be considered).
- Identify and describe the risk model and analytic approach.
- Provide a rationale for any risk-related decisions during the risk assessment process.
- Describe the uncertainties within the risk assessment process and how those uncertainties influence decisions.
- If the risk assessment includes organizational missions/business functions, describe the missions/functions.
- If the risk assessment includes organizational information systems, describe the systems (e.g., missions/business functions the system is supporting, information flows to/from the systems, and dependencies on other systems, shared services, or common infrastructures).
- Summarize risk assessment results (e.g., using tables or graphs), in a form that enables decision makers to quickly understand the risk (e.g., number of threat events for different combinations of likelihood and impact, the relative proportion of threat events at different risk levels).
- Identify the time frame for which the risk assessment is valid (i.e., time frame for which the assessment is intended to support decisions).
- List the risks due to adversarial threats.
- List the risks due to non-adversarial threats.

Appendices

- List references and sources of information.
- List the team or individuals conducting the risk assessment including contact information.

List risk assessment details and any supporting evidence, as needed to understand and enable reuse of results.

13. Risk Identification and Evaluation Update

The railway's organization should update the risk assessment process. There is two recommendation on this parameter:

- ERC hazard identification and risk evaluation & control procedures document recommend the process shall be organized at least once a year.
- National cybersecurity requirement standard recommends the process should be updated every 3 months.

Organizational risk identification, evaluation, and update opportunity should be:

- When the management area or business activity has a change.
- Before the new line is put into operation.
- Before new activities with an effect on operation safety or service quality appears.
- When relevant laws, legal regulations, standard, and other requirements change.
- Before newly purchased equipment related to safety is put into use.
- Before new, renovation and expansion projects involving traveling, passenger transportation, physical and fire safety and major changes of traveling and maintenance methods are implemented.
- After major safety hazards are discovered in the safety inspection process.
- When safety and security requirements of ERC is changed.

Chapter Six:

Evaluation of the Proposed Framework

This chapter considers the descriptive framework evaluation method and panel discussion of the expert's method to evaluate the proposed cybersecurity risk assessment framework.

5.1 Descriptive Framework Evaluation Method

This framework allows the corporation to assess cyber risks to the context of railways industry and it can solve problems of the organization risk assessment process. A designed artifact is complete and effective when it satisfies the requirements and constraints of the problem it was meant to solve[24]. The next section will discuss the methodology used to evaluate the framework, cyber incident scenario in the corporation, analysis of scenario against the proposed framework.

A descriptive approach which is scenarios was undertaken to evaluate the framework usefulness. The use of scenario in this study is purposeful because it can help to inform the corporation on the possibilities that may occur cyber incident and help the organization to be ready to protect its assets from a threat by doing risk assessment primary. The use of scenarios in design science is an acceptable and effective evaluation approach. Design evaluation methods as follows [24]:

Also, the use of scenarios in design science has been applied in similar studies. Scenarios have also been used in other IS research areas of simulation and experimentation to demonstrate the characteristics and benefits of defined models [43].

5.1.1 Cyber Incident Scenario

Since the beginning of the operation, Ethiopian Railways Corporation is assisted by (technical assistance such as maintenance) external supplier which is Chinese companies. As stated in the statement of the problem one of the risk areas of the organization is supplier relationship risk. The entire organization systems have connectivity through the internet for sharing system information for maintenance purpose such as Supervisory Control and Data Acquisition system, communication and signaling system which may cause supplier relationship risk (the contractor which have the privilege to access the system remotely from somewhere else).

The incident that happens within these 3 years are explained as follows:

1. September 2017 the power in all mainline station cannot monitor remotely from the operation control center. The power department engineers login the SCADA (Supervisory Control and Data Acquisition) system to maintain the problem. They identified (log file) that before a minute someone login the system and changed the system configuration. Because of this, the operation control center can't monitor power equipment's in every station. This SCADA system is accessible remotely from Chengdu, China. The supplier denied that they didn't login the system at that time.

2. Supplier X is a communication system supplier for the corporation. They have TAC (technical assistance center) in Egypt for all of Africa countries. In 2018 two times transmission system interruption occurred because of this all wayside equipment's not communicate each other and it disrupts normal operation. At this time signaling and communication department engineers identified that someone login the system remotely for an unknown purpose.

Finally, after they identified these two cyber incidents power and communication department report the situation to the leaders. The leaders gave a direction to the victim departments to not to allow remote access to the system. Later critical system failure happened, the suppliers came to the site and maintained the system.

5.1.2 Analysis of Scenario against Proposed Framework

The framework is intended to help guide Ethiopian Railways Corporation in identifying key elements to consider in assessing cybersecurity risks and allows the corporation to prepare protection method of its infrastructure against threats. Therefore the use of scenario helps in identified the consideration based on the framework main pillars that is organization operational risk assessment (the pillars such as cybersecurity strategic management awareness, organizational structure, established system context, purpose, scope, identify assets& intrusion detection, identify threats, identify vulnerability, determine likelihood, determine impact, risk evaluation, communicate result and risk identification & evaluation update opportunity). The parameters/pillars of cybersecurity risk assessment framework are further discussed which highlight the interrelation of each area:

1. Cybersecurity strategic management awareness

The scenario showed that the cybersecurity culture of the organization. Due to the staff & management carelessness/ Luck of awareness the organization hasn't conduct cybersecurity awareness program to the stakeholder in order to create positive cyber security culture (because of these the stakeholder login to the system without communicating ERC staffs). Also the scenario showed that the organization doesn't build awareness to the staffs to increase the ability to address cyber risk (due to this the staffs & management doesn't address technical countermeasure like intrusion detection tools and operational countermeasure like strategy & policy: only the management suggest the departments block them not to log in the system).

2. Organizational structure

The scenario showed that ERC's skill full institutional structure who follows/conduct cybersecurity tasks and the team who have the authority over cybersecurity matter (the scenario presented there is no responsible division, person who will follow this kind of cyber incident in the organization: even if some engineers from these departments are part of temporary risk assessment unit, they doesn't investigate the situation furthermore. Simply they identified the problem and report to the leader)

3. Purpose

The scenario showed that the objective of finding out/discover the cause of operation interruption and immediate control method but they don't set a procedure or method to identify the event/risk and doesn't set permanent control method.

4. Scope

The scenario showed that the extent to discover the cyber incident that is business unit is identified (Addis Ababa Light Rail Transit Service) and the system is identified (SCADA & communication system).

5. Established system context

Established system context are those system layers affected by the incident & safety integrity level required to the system. Control layer (indoor equipment's with SIL 2) and communication layer (indoor equipment's with SIL 0) is the one impacted by the attack.

6. Identify asset & intrusion detection

The critical assets are those valuable assets that will cause rail operation interruption. The asset impacted by the cyber incident on the scenario includes server, software, operation staffs, and wayside equipment. The systems by itself have remote login registration (log file) that register date, time and port number.

7. Identify threat

The scenario showed that the threat/ cyber incident that harms ERC assets. Stakeholder/supplier is the first suspected threat to the incident.

8. Determine vulnerability

The scenario showed that critical assets of the organization have weakness and they are vulnerable to the system supplier

9. Determine the likelihood

Likelihood determines the occurrence of a threat to the organization asset. System supplier relation (remote access for maintenance) is one of the gates to cyber-attack and the likelihood of occurrence is high.

10. Determine the impact

The scenario presented the impact of the incident. Disruption to efficient rail operation is the impact and the impact is critical.

11. Risk evaluation

The scenario showed that the likelihood of system supplier threat is high as well the impact is critical (operation interruption). Based on these top management decide/make the decision not to allow them remote access.

12. Communicate the result

Department engineers report the incident/ situation to the management.

13. Risk identification & evaluation update

The scenario showed that risk assessment update opportunity. ERC get the opportunity to update risk assessment due to this incident but not conducted.

Table 6.1 shows the main parameters/pillars of information and cybersecurity risk assessment framework and scenario application summarization as follow:

Table 6.1 Summary of Scenario Application in CSRA Framework

CSRA Framework Pillars		**Scenario Application**
Prepare for the risk assessment	Cybersecurity strategic management awareness	-ERC cybersecurity culture -ERC cybersecurity awareness: the ability to address cyber risks
	Organizational structure	-Skill full institutional structure - A team who have the authority over cybersecurity matter

	Purpose	To find out/discover the cause of operation interruption and immediate control method
	Scope	- Addis Ababa Light Rail Transit Service - SCADA and Communication system
	Established System Context	- Control layer (indoor equipments with SIL 2) - The communication layer (indoor equipments with SIL 0)
Conduct risk assessment	Identify Asset & Intrusion Detection	-Hardware + software (system), wayside equipment's and operational staff -Check log file
	Identify Threat	External (stakeholder)
	Identify Vulnerabilities	Policy, procedure (includes safety & security procedure) and system (not alerting during security breach)
	Determine likelihood	High (because the supplier can access the system at any time, they have the authorization to login the system for maintenance purpose
	Determine Impact	-Disruption to efficient railways operation - high or critical
	Risk evaluation	Based likelihood & impact the organization doesn't make decision yet
Communicate result		The team (engineers) report the situation (result) to management members
Maintain risk assessment	Risk Identification & Evaluation Update	Update opportunity

5.2 Panel of Experts Method

In addition to the descriptive/ scenario evaluation method the researcher conduct panel discussion in the railway's corporation meeting room. The researcher presented the main part of the study and the professionals who participated in the presentation ask questions and give opinions about the constructed cybersecurity risk assessment framework. The reason for the evaluation process is to make sure to what extent the proposed cybersecurity risk assessment framework is functionally implemented and suitable for Ethiopian Railways Corporation.

Professionals who have knowledge and experience in the area of safety & security, information & cybersecurity have participated in the evaluation process of the panel discussion. The total number of professionals participated in the panel discussion was 8. Six professionals involved from ERC (two from the IT department, 2 safety and security departments and the other 2 are from other departments) and two of them from INSA cybersecurity risk assessment unit. They evaluated the proposed cybersecurity risk assessment framework based on the following concepts.

ERC Context/specific

Once the presentation completed the professional explained that the proposed framework is covered/considered railways features as well information security requirements, the solution for problems & challenge ERC faced related to cybersecurity and also consider organizational safety and security procedure. As an indication they put the following points:

- The proposed framework shows critical organizational systems layers with the necessary safety integrity level.
- The proposed framework shows organizational cybersecurity knowledge gap such as well-organized cybersecurity culture (policy, strategy), organizational structure. Finally, they mentioned the proposed framework put the solution with detail procedure.
- They appreciated that maintain risk assessment step considering ERC Hazard identification and risk evaluation & control procedures document.
- The experts believed that the proposed framework is trying to address temporary cybersecurity risk assessment team challenges during the previous organizational risk assessment engagement.

The proposed framework tries to consider a few unique railways information security requirements like intrusion detection but they questioned why & how intrusion detection requirement is considered as unique ERC information security requirement. After the discussion, they convinced and they agree to include in the framework. (The answer was regarding the question: one of the major organization problem identified through the study is supplier relationship risk which is mentioned in the above scenario. If we can’t give special attention to this problem the organization is at risk: identify intrusion detection tools in the organization and need to make a decision).

Experts from INSA appreciated the proposed framework considered the railways sector in Ethiopia and adopted the national cybersecurity risk assessment requirement at strategic & tactical level but they suggested that such like of study should consider sectorial level risk assessment/ transport sector in the future because ERC strategic & tactical level risk assessment should consider transport sector strategic, tactical and operational risk profile.

Research questions clarity & data analysis

The experts described that the clarity of research question & aspects to address the research questions in the data analysis is clear to recognize the status & level of cybersecurity risk assessment in Ethiopia railways industry. They appreciated & accepted that the way the study links/related the code generated from the questioner, the theme generated from code, research questions answered by the theme and the proposed framework is clearly explained on the study. But they questioned why all themes (like access management, system reliability, and personal themes) illustrated in the data analysis part is used by the framework and the researcher explained about it and convinced them. (Regarding the explanation: access management, system reliability, and personal themes are well explained in the international standard parameters which included in the framework)

Lastly, they concluded that the proposed framework is suitable for the railway's industry in Ethiopia and requested to have the framework.

5.3 Summary

Based on the above two evaluation method the researcher believed that the cyber security risk assessment framework is suitable and specific to the railway’s industry in Ethiopia. It is useful as it provides a platform to assess organizational cybersecurity risks. The pillars of the framework are shown to be an effective lens in viewing a scenario of cyberincident and risk assessment process.

Chapter seven:

Conclusions, Recommendations and Future Works

This chapter is dedicated to the presentation of the conclusion, recommendation and future work regarding the proposed cybersecurity risk assessment framework for the railway's industry in Ethiopia.

7.1 Conclusions

The thesis review the current state of cybersecurity risk assessment process, guideline, standards in Ethiopia and other international standards. From the review of such guidelines, standards, related studies and empirical data the researcher come up with an approach (framework development) that will enhance existing cybersecurity risk assessment frameworks.

This research articulated the current railway organization's cybersecurity risk assessment problems in Ethiopia and discussed the need for the development of an enhanced framework by taking into account the organization context. The general objective of this research was to develop an integrated cybersecurity risk assessment framework for the railway's industry in Ethiopia to improve the level of safety and security.

The proposed framework has a total of 13components that includes cybersecurity strategic management awareness, organizational structure, established system context, purpose, scope, identify assets & intrusion detection, identify threats, identify vulnerability, determine likelihood, determine impact, risk evaluation, communicate result and risk identification & evaluation update opportunity. The design science approach is applied in this study to develop and evaluate the framework. To evaluate the framework the researcher used a descriptive approach which is scenario and panel of expert's method.

The research question was answered in the data analysis and interpretation section. Thematic data analysis approach was applied to analyze and interpret the data. The researcher codes the interviewee answer first, then conducting formulation of themes and finally define the themes accordingly.

Finally, an integrated and organization's operational level cybersecurity framework was proposed which has contributed both to the theory and practice. The utilization of advanced cybersecurity risk assessment framework is an important contribution to the railway industry in Ethiopia. Additionally, there are no research studies conducted in cybersecurity risk assessment for the railway's industry in Ethiopia thus it provides the opportunity to extend the knowledge area. The result of this research can help improve organization cybersecurity risk assessment process.

7.2 Recommendations

A cybersecurity program is very important for the corporation. Cybersecurity risk assessment process is one part of a cybersecurity program. The railway's organization top management should give special focus for the cybersecurity program in the corporation. Even if the corporation formulated temporary cybersecurity risk assessment team, it needs to be improved. The researcher recommends to formulate a permanent cybersecurity department, create and conduct cybersecurity awareness program to the employee, expertise should be hired at each level, and training should be conducted by external body INSA. Besides, the corporation and its employee should have a cybersecurity culture in order to protect the organization asset and ensure safe rail operation.

Finally, based on the output of risk assessment the organization should organize a risk management process.

7.3 Future Works

As we discussed in chapter five the limitation of the study was the researcher haven't identified/ found any new aspect at organizational strategic & tactical risk assessment process from the gathered data. While conducting the study the researcher identified future works as follow:

- Railways strategic and tactical risk assessment process.
- Railways cybersecurity risk management process.

References

[1] “Cyber Attack: Exploiting the User - There are so many ways,” p. 88.

[2] “https://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security”.

[3] J. Granneman, “IT security frameworks and standards: Choosing the right one”.

[4] M. Kozicki, “The history of railway in Ethiopia and its role in the economic and social development of this country,” p. 28.

[5] B. Chen et al., “Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective,” in Computer Safety, Reliability, and Security, vol. 9338, F. Koornneef and C. van Gulijk, Eds. Cham: Springer International Publishing, 2015, pp. 277–290.

[6] S. Gordeychik, “Modern railroad systems vulnerable to cyber-attacks,” Jan. 2016.

[7] “Securing Control and Communications,” 2010.

[8] “International Organization for Standardization/International Electro technical Commission,” 5th ed. 2004.

[9] “Critical mass cyber security requirement standard,” p. 107, 2009.

[10] M. Siponen and R. Willison, “Information security management standards: Problems and solutions,” Inf. Manage., vol. 46, no. 5, pp. 267–270, Jun. 2009.

[11] “Introduction to Information Security,” p. 37.

[12] Information Systems Audit and Control Association, COBIT 5 for information security. 2012.

[13] “National cyber security framework manual,” p. 231, 2012.

[14] “Cyber security in the railways sector,” p. 68, 2017.

[15] “Cybersecurity For Rail:Not A Single-Shot Approach, Applying the NIST

approach to rail transportation," p. 10.

[16] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," Comput. Secure, vol. 57, pp. 14–30, Mar. 2016.

[17] M. Abomhara, Department of Information and Communication Technology, University of Agder, Norway, G. M. Kien, and Department of Information and Communication Technology, University of Agder, Norway, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," J. Cyber Secure. Mobile, vol. 4, no. 1, pp. 65–88, 2015.

[18] J. Bayne, "An Overview of Threat and Risk Assessment," p. 9, 2002.

[19] "Cyber Security Framework Saudi Arabian Monetary Authority," vol. 1, p. 56.

[20] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012.

[21] R. Bloomfield, M. Bendele, P. Bishop, R. Stroud, and S. Tonks, "The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned," in Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification, vol. 9707, T. Lecomte, R. Pinger, and A. Romanovsky, Eds. Cham: Springer International Publishing, 2016, pp. 3–19.

[22] "Rail Cyber Security: Austeralian Standard," p. 35, 2018.

[23] K. Yin, "Case study research design abd methods" 2nd ed. vol. 5.

[24] A. Vaishnavi, "Design science research in information-systems," p. 66.

[25] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," p. 32.

[26] S. T. March and G. F. Smith, “Design and natural science research on information technology,” Decis. Support Syst., vol. 15, no. 4, pp. 251–266, Dec. 1995.

[27] J. R. Venable, “The Role of Theory and Theorising in Design Science Research,” p. 18.

[28] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” J. Manag. Inf. Syst., vol. 24, no. 3, pp. 45–77, Dec. 2007.

[29] J. Maxwell, “Designing a Qualitative Study,” in The SAGE Handbook of Applied Social Research Methods, 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2009, pp. 214–253.

[30] M. Javadi and K. Zarea, “Understanding Thematic Analysis and its Pitfall,” J. Client Care, vol. 1, no. 1, 2016.

[31] T. Nathalia, “Exploring the influence of country-of-origin information to Generation Y's perception towards international fashion brands,” p. 24.

[32] V. Clarke, “Teaching thematic analysis: Overcoming challenges and developing”.

[33] J. Saldaña, The coding manual for qualitative researchers. Los Angeles, Calif: Sage, 2009.

[34] M. Ibrahim, “THEMATIC ANALYSIS: A CRITICAL REVIEW OF ITS PROCESS AND EVALUATION,” vol. 1, no. 1, p. 9, 2012.

[35] V. Braun and V. Clarke, “Using thematic analysis in psychology,” Qual. Res. Psychol., vol. 3, no. 2, pp. 77–101, Jan. 2006.

[36] “Cyber security is everyone's job," vol. 1, p.6, October 2018. .

[37] “Functional safety of electrical/electronic/ programmable electronic safety-related systems,” 1997.

[38] M. Charlwood, S. T. Cp. MInstP, and N. Worsell, “A methodology for the

assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines," p. 82.

[39] N. Mayer, "An integrated conceptual model for information system security risk management and enterprise architecture management based on TOGAF," p. 361, 2016.

[40] M. Haythorn, "Information Security Risk Assessment Methods, Frameworks and Guidelines," p. 18.

[41] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012.

[42] "Information technology-security techniques-information security risk management," 2011.

[43] R. Warren, D. E. Diller, A. Leung, W. Ferguson, and J. L. Sutton, "Simulating Scenarios for Research on Culture & amp; Cognition Using a Commercial Role-play Game," in Proceedings of the Winter Simulation Conference, 2005., Orlando, FL. USA, 2005, pp. 1109–1117.

[44] M. Rastog, "PESTEL technique- A tool to identify external risks in construction project," vol. 3, p. 388, 2016.

[45] "An Introduction to the Business Model for Information Security," p. 27, 2009.

Appendix A: Interview Question and Answer

1. What are organizational/railways features as well as information, safety, and security requirements?

Interviewee 1

Interviewee 1 stated that operational systems are working together if one part of each system fail the operation will be stopped so that the railway systems are an integrated system. This system is Automatic train protection system, Computer-based interlocking, automatic train supervision system, SCADA, transmission system, telephone system, and Onboard signaling system. Regarding railways information security need, operation staffs (train masters, OCC staff and maintenance staffs) and support staffs (finance, HR and other departments staffs) need to be secured and need to have information security mind). And also he/she stated that there should be a system which detects an authorized system user (remote login).

Interviewee 2

Interviewee 2 explained that infrastructure should be protected from an external and internal threat. According to him/her the entire railway's system especially CBI, ATP, ATS, SCADA and all wayside equipment’s should be protected and safe (safety integrity level should be classified) because the systems are key features (the important part) of railways operation. Also, operation and supporting staffs should be protected and need to have a cybersecurity culture. The confidentiality, integrity of the systems and information should be confirmed always to ensure the safety of the train. Finally, he/ she stated that the organization should implement a tool that can detect different attack and threats.

Interviewee 3

Interviewee 3 stated that who access the system should be identified and authorization access type should be clear. He also mentions the communication between the operating control center and trainmaster (drivers) should be protected in addition to this all wayside equipment’s related to safety should be protected. All the systems, operation staffs, hardware also needs to protect.

Interviewee 4

Interviewee 4 stated that all operational process (documents) need to be secured. Need to identify who will have the privilege to access this document. In addition to this sensitive and important system need to be protected such as ATP, ATS, TCMS, CBI, SCADA, wayside equipment like responder, switch, signal lamp, and management information systems. It’s important to have a software which detects threat (attackers). Finally, he/ she suggest that all the railway's system should be reliable which means it should be followed fail-safe principle (guarantee the safety with the highest reliability in a critical situation when a fault occurs in the system).

Interviewee 5

Interviewee 5 explained that the very important system of railways operations is Automatic train control system, Computer-based interlocking (CBI), Onboard signaling system (ATP) and Wayside equipment that ensure safety and supervise train movement. Also, the SCADA system is very important to monitor power through the line. Regards information security requires the organization should have intruder, attacker (threat detection) mechanism to alert the IT staffs. The reliability of the systems is very important that means when the system fails always the output will be safe (for example when one part of CBI system fail the wayside equipment that is signal lamp should always indicate red light status).

Interviewee 6

Interviewee 6 explained that the main interesting part of the system is safety based rail systems are implemented in our country such as interlocking system. Concerning information security requirements authentication, Authorization, confidentiality, integrity and availability of the systems are required, reliability of the system is required and attack, threat discovery software’s are required. All railways system operation should be based on the failsafe principle (when the system fail always the output will be safe).

2. Does the corporation have any cybersecurity risk assessment framework, standards and guideline to conduct cybersecurity risk assessment? If yes describe them. What are the strength and gap of the framework? What are the challenges facing the corporation while using this framework and recommendation to improve the framework? What is the difficulty in the organization related to cybersecurity and recommendation to solve this problem?

Interviewee 1

Interviewee 1 stated that the corporation has a cybersecurity risk assessment framework in order to assess the corporation cybersecurity risks. This framework is prepared by temporary organizational cybersecurity risk assessment team (since January 2018 the corporation organized temporary information and cyber security team composed from Addis Ababa- Djibouti and Addis Ababa light rail transit IT, signaling and communication, safety and security department. This team is responsible for assessing organizational cybersecurity risks). The team adopted NIST SP 800-30 to assess the corporation cybersecurity.

According to interviewee 1 the challenge and the gap of the framework is generic (not explain step 1 and 4 of risk assessment steps in detail, it's not focused on railways industry (not context based), doesn't describe to what extent/covered risk assessment process conducted, doesn't describe which railways systems area should be assessed, doesn't describe the aim of this program. To improve the risk assessment process he/she recommend the standard should consider/fulfill all elements he/she described in the above.

Concerning organizational difficulty he/she mentioned the organization top management not concerned about cybersecurity issue because of this, the organization doesn't have cybersecurity policy& strategy. Besides the organization doesn't have an annual plan and budget for cybersecurity program and department responsible for cybersecurity issue. To solve this problem he/she recommend the organization should fulfill/consider all elements he/she described in the above.

Interviewee 2

Interviewee 2 stated that the corporation used NIST SP 800-30 guideline to conduct a cybersecurity risk assessment.

As stated by interviewee 2 the challenge and the gap of the framework is generic, difficult to understand, difficult to use, not railways context-based, doesn't describe to what extent/covered risk assessment process conducted, doesn't describe which railways systems area should be assessed, doesn't describe for how long risk assessment result will be used and doesn't describe the objective of risk assessment. According to interviewee 2 in order to improve the risk assessment process, he/she recommend the standard should consider/fulfill all elements he/she described in the above.

Regarding organizational difficulty, he/she mentioned the organization doesn't have cybersecurity policy & strategy. In addition, the organization doesn't have a department responsible for a cybersecurity issue and cybersecurity risk assessment unit. To solve this problem he/she recommend the organization should fulfill/consider all elements he/she described in the above.

Interviewee 3

Interviewee 3 stated that the corporation used NIST SP 800-30 guideline to conduct a cybersecurity risk assessment.

As stated by interviewee 3 the challenge and the gap of the framework are difficult to understand & use, doesn't describe for how long risk assessment result will be used, not railways context, doesn't describe to what extent/covered risk assessment process conducted. To improve the risk assessment process he/she recommend the standard should consider/fulfill all elements he/she described in the above.

About organizational difficulty, he/she mentioned the organization doesn't have a cybersecurity policy, strategy, annual plan, and budget, the responsible person for the cyber security issue and cyber security department.

Interviewee 4

Interviewee 4 stated that the corporation used NIST SP 800-30 guideline to conduct a cybersecurity risk assessment. Even if he knows the type of standard that the corporation used he doesn't have knowledge about this standard and he couldn't identify the gap, challenge. The researcher identified interviewee 4 does not participate in the temporary cybersecurity team.

But according to interviewee 4 the main organization difficulties with respect to cybersecurity issues, the organization top management attentiveness is very low and the organization doesn't have cybersecurity department on the structure.

Interviewee 5

Interviewee 5 stated that the corporation used NIST SP 800-30 guideline to conduct a cybersecurity risk assessment.

As stated by interviewee 5 the challenge and the gap of the framework is not specific to railways, doesn't describe for how long risk assessment result will be used, generic (not explain step 1 and 4 of risk assessment steps in detail, it's not focused on railways industry (not context based), difficult to understand and follow the steps doesn't describe to what extent/covered risk assessment process conducted, doesn't describe which railways systems area should be assessed, doesn't describe the aim of this program. To improve the risk assessment process he/she recommend the standard should consider/fulfill all elements he/she described in the above.

About organizational difficulty he/she mentioned the organization doesn't have a cybersecurity policy, strategy, responsible person for cybersecurity issue, permanent risk assessment unit and cyber security department.

Interviewee 6

Interviewee 6 stated that the corporation used NIST SP 800-30 guideline to conduct a cybersecurity risk assessment.

As stated by interviewee 6 the challenge and the gap of the framework is generic, difficult to understand, and use, not railways context-based, doesn't describe to what extent/covered risk assessment process conducted, doesn't describe maintain the risk step in detail, doesn't describe for how long risk assessment result will be used and doesn't describe the objective of risk assessment. According to interviewee 2 in order to improve the risk assessment process, he/she recommend the standard should consider/fulfill all elements he/she described in the above.

Concerning organizational difficulty, he/she mentioned the organization doesn’t have a cybersecurity policy, strategy, annual plan, and budget. In addition, the organization doesn’t have a department responsible for a cybersecurity issue and cybersecurity risk assessment unit. To solve this problem he/she recommend the organization should fulfill/consider all elements he/she described in the above.

3. Does the corporation have any cybersecurity risk assessment framework, standards and guideline to conduct cybersecurity risk assessment? If yes, to what extent the framework is suitable for Ethiopia Railways?

Except for one person all five interviewees replied the same answer for this question because they have been working in the organizational temporary risk assessment unit

Interviewee 1, 2, 3, 4, 5

All the interviewees stated that they adopt the following parameters from international standards and using it. It helps them a lot, they described in the following ways.

- ➢ The standard guide us to categorize, find out, classify interlocking system, automatic train supervision system, automatic train control system, supervisory control and data acquisition system, financial information, employee information, design documents, trainmasters operation daily record, operation control center records, maintenance records and service level agreement document with contractor, workflows and procedure manuals, internetworking and communication devices, wayside signaling and commination equipment’s, train, optical fiber cables, e operation maintenance client software, e sight ICT unified network management system, operation staffs, users and support staffs, hackers, intruders, attackers, fire, flood, earthquake, system weakness, physical weakness, Document weakness, Process weakness and Awareness weakness.
- ➢ The standard guide us to define the chance that the threat event happen is Very low, Very high, High, Low and 0-100 scale.
- ➢ The standard guide us to define the consequence of possible attack such as injury, death, disruption of railways operation, economic lose and helps us to assign value based on the comparison which is Low or non-existing and High or critical.
- ➢ The standard guide us to estimate the risk. Also, it guide us on how to make the decision about future based on the understanding of the risk obtained by risk analysis (determine impact vs likelihood).
- ➢ The standard guide us on how to report the risk assessment result and element of results.

Besides the above benefits, the standard identified the last step of risk assessment that maintains risk assessment. But as stated by all the interviewees they can't identify the detail process of how to maintain the risk assessment. Then they aligned these step with ERC hazard identification & risk evaluation and control procedure. The procedure helps them:

- To know organizational risk identification, evaluation, and update opportunity
- To identify how many times a risk assessment process should be updated.

Appendix B: - Interview Questions

1. Does our country have sectorial (transportation sector) and national cybersecurity risk assessment methodology?

2. Does our country have cyber security standard?

Appendix C: Strategic and Tactical Risk Assessment

1. Strategic Risk Assessment

The strategic risk assessment of the organization should focus on organizational strategic risk. The risk assessment is based on the national strategic risk assessment profile and sectoral strategic risk assessment profile. This risk assessment can be analyzed using SGOC (strength, gap, opportunity, and challenge) with PESTEL (political, economic, social, technological, legal and environmental) in it.

I. SGOC (Strength, Gap, Opportunity and Challenge)

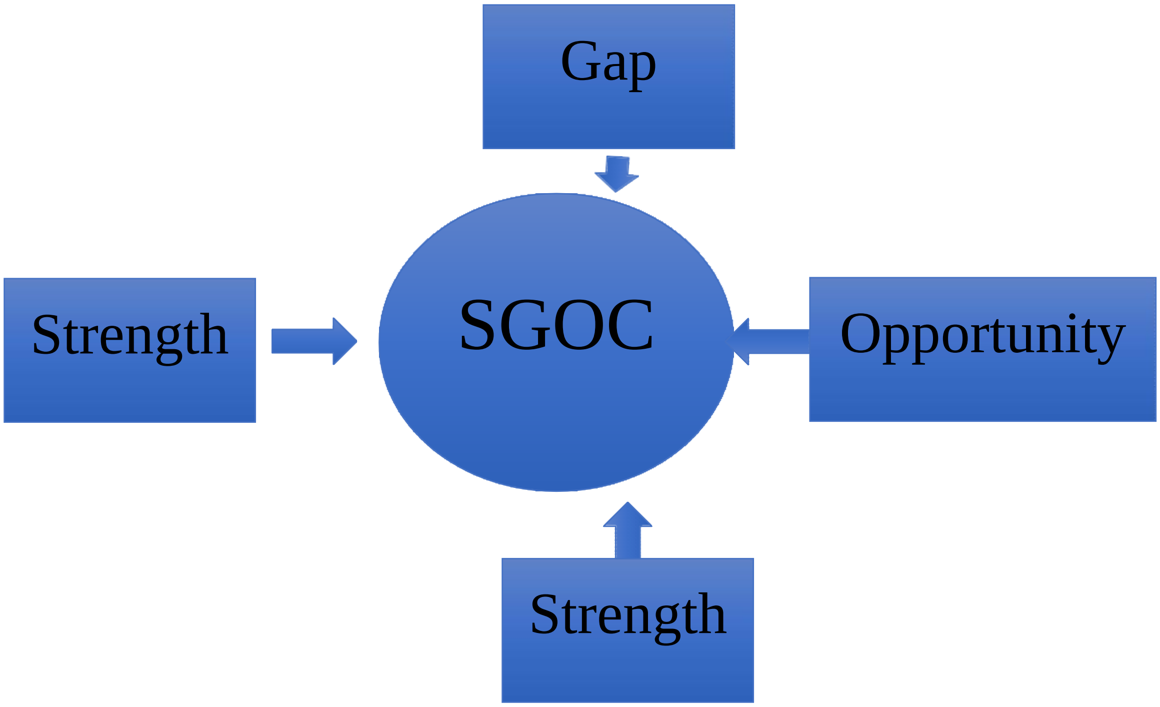


Fig C.1 SGOC

- ➢ What is the strength of railways organization while securing cyberspace?

Strengths are internal to the organization. Strengths include any kinds of capabilities or resources that the organization (and potentially any partners involved, and any stakeholders who are active participants in a development effort) can bring to bear, in order to achieve the desired result.

- ➢ What is the gap of railways organization while securing cyberspace?

Gap are internal factors within the organization such as existing gaps in capabilities or resources in the implementing organization, relevant areas where a need for improvement has been identified and known vulnerability,

- What is the opportunity of railways organization while securing cyberspace?

Opportunities are external factors such as Events or trends that offer opportunities: Political (government policies, favorable changes in power/influence of relevant actors, political agendas), economic (rising prosperity, new economic opportunities or other favorable economic change), social (behavior patterns, demographic change), technological (innovations, changes in technology use), environmental (favorable climate/weather), legal (upcoming legislation or treaties/international agreements).

- What is the challenge of railways organization while securing cyberspace?

Challenge are internal or external factors such as risks that would be incurred by a given action under consideration (risk to the staff and partner, financial risk, political risk, cost) and events or trends that could threaten the railways organization or that put progress at risk, political, social, technological, environmental and legal.

II. PESTEL (Political, Economic, Social, Technological, Legal and Environmental)

PESTLE is a strategic planning tool used to evaluate the impact of political, economic, social, technological, environmental and legal factors might have on a project. It involves an organization considering the external environment before starting a project. It is agood way of ensuring one has captured all potential risks and issues [44].

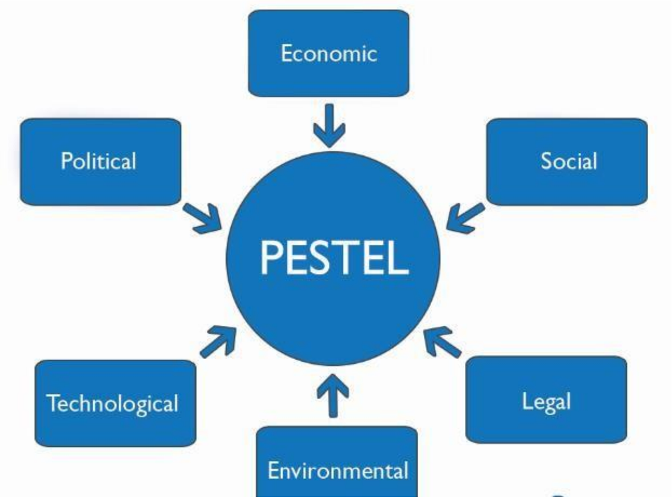


Fig C.2 PESTEL

➢ What is the political factor of railways organization?

□Government stability.

□ Regulation trends.

□ Tax policy, and trade controls.

□ War

□ Government policy

□ Elections

□ Terrorism

□ Likely changes to the political environment.

➢ What is the economic factor of railways organization?

□ Stage of the business cycle.

□ Current and projected economic growth

□ International trends

□ Job growth

□ Inflation and interest rates.

□ Unemployment and labor supply.

□ Levels of disposable income across the economy and income distribution.

□ Globalization.

□ Likely changes to the economic environment.

➢ What is the social factor of railways organization?

□Population growth and demographics.

□ Health, education and social mobility of the population

□ Consumer attitudes

□ Advertising and media

□ National and regional culture

□ Lifestyle choices and attitudes to these.

□ Levels of health and education

□ Major events

□ Socio-cultural changes.

➢ What is the technological factor of railways organization?

□ Impact of new technologies.

□ Inventions and innovations

□ The internet and how it affects working and business

□ Licensing and patents

□ Research funding and Development.

➢ What is the legal factor of railways organization?

□ Home legislation
□ International legislation
□ Employment law
□ New laws
□ Regulatory bodies
□ Environmental regulation
□ Industry-specific regulations
□ Consumer protection

➢ What is the environmental factor of railways organization?

□ Ecology
□ International environmental issues
□ National environmental issues
□ Local environmental issues
□ Environmental regulations
□ Organizational culture
□ Staff morale and attitudes

2. Tactical Risk Assessment

The tactical (managerial) risk assessment should focus on governance and managerial risks. This risk assessment should be based on the organizational strategic assessment and sectorial tactical risk assessment. This risk assessment is based on BMIS (governance, process, people, technology and the six dynamic interconnections that is governance, architecture, culture, emergence, enabling & support and human factor).

I. Business Model for Information Security (BMIS)

It defines the core concepts that will evolve into practical aids information security and business unit managers can use to align security program activities with organizational/ERC goals and priorities, effectively manage risk, and increase the value of information security program activities to the enterprise [45].

Structure of the Model

The model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections. All aspects of the model interact with each other [45].

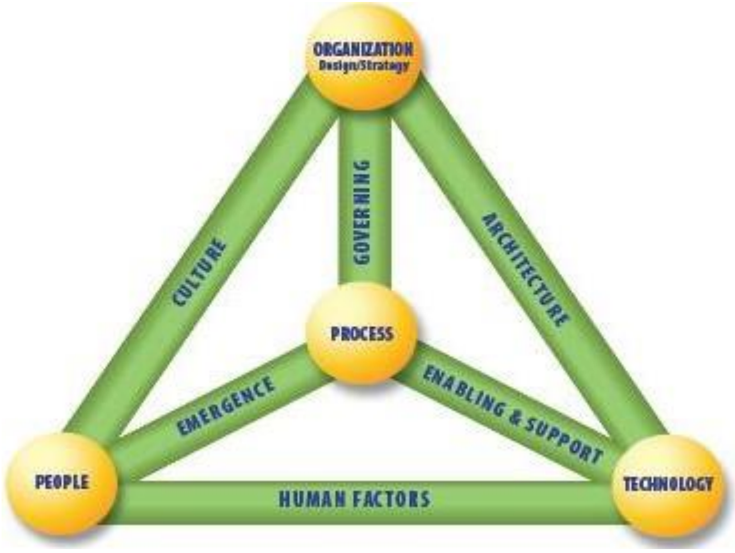


Fig C.3 Business Model for Information Security

The four elements of BMIS model are:

A. Organization Design and Strategy: An organization is a network of people, assets, and processes interacting with each other in defined roles and working toward a common goal. An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction.

Ethiopian Railways Corporation should assess people, asset and process interaction risk. The organization cybersecurity strategy should be assessed.

- What is the organizational cybersecurity strategy?
- What are organizational people, asset and process interaction?

B. People: The people element represents the human resources and the security issues that surround them. It defines who implement (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases.

Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:

- Recruitment strategies (access, background checks, interviews, roles, and responsibilities)
- Employment issues (location of the office, access to tools and data, training and awareness, movement within the enterprise)
- Termination (reasons for leaving, the timing of exit, roles and responsibilities, access to systems, access to other employees)

Externally, customers, suppliers, media, stakeholders, and others can have a strong influence on the railway's organization and need to be considered within the security posture.

Ethiopian Railways Corporation should assess the people internal and external elements risks.

- Identify peoples in the railway's organization who implement each part of the strategy?

C. Process: Process includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections. Processes identify, measure, manage and control risk, availability, integrity, and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

Ethiopian Railways Corporation should assess organizational all kind of process (formal and informal) risks.

- What are the formal railways organizational process?
- What are the informal railways organizational process?

D. Technology: The technology element is composed of all of the tools, applications, and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risks. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Ethiopian Railways Corporation should assess organizational technological risks.

- What are the tools, application, and infrastructure that makes the process more efficient?
- What are the tool and application to resolve security threats and risks?

Dynamic Interconnection

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium [45]. The six dynamic interconnections are:

A. Governing: Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions.

Ethiopian Railways Corporation should assess organizational governance risks.

- What are organizational cybersecurity policies, standards, frameworks?

B. Culture: Culture is a pattern of behaviors, beliefs, assumptions, attitudes, and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history.

Ethiopian Railways Corporation should assess organizational culture risks.

- What is the organization cybersecurity culture?

C. Enabling and Support: The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures are to make processes usable and easy. Policies, standards, and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Ethiopian Railways Corporation should assess organizational enabling and support risks, dynamic interconnection that connects the technology element to the process element.

- What is the organizational cybersecurity measure?
- What are the organizational cybersecurity policies?
- What is the organizational cybersecurity procedure?
- What is the organizational cyber security standard?
- What is the organizational cybersecurity guideline?

D. Emergence: Emergence—which means surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management [8].

Ethiopian Railways Corporation should assess organizational all kind of emergency risks.

- What are organizational emergent issues in cybersecurity?

E. Human Factor: The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection [6].

Ethiopian Railways Corporation should assess organizational human factor that is the interaction and gap between technology and people risks.

- What is the organizational cybersecurity knowledge gap?
- Which organizational employee experience level has cybersecurity knowledge gap?

F. Architecture: A security architecture is a comprehensive and formal encapsulation of the people, processes, policies, and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing security architecture.

Ethiopian Railways Corporation should assess organizational architectural risks.

- What are organizational cyber security controls are positioned?

How organizational information and cyber security controls relate to the overall IT architecture?