UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL
(UCI)

DEVELOPMENT OF A PROJECT MANAGEMENT METHODOLOGY FOR CYBER SECURITY ASSESSMENTS

Douglas Michael Oliver Westby

FINAL GRADUATION PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE
MASTER IN PROJECT MANAGEMENT (MPM) DEGREE

Belize City, Belize

June 2018

UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL
(UCI)

This Final Graduation Project was approved by the University as partial fulfillment of the requirements to opt for the Master in Project Management (MPM) Degree

Carlos Castro Torres
TUTOR

Jorge Enrique Trejos Gutierrez
REVIEWER No.1

Paula Jensy Villalta Olivares
REVIEWER No.2

Douglas Michael Oliver Westby
STUDENT

DEDICATION

This effort is dedicated to my daughter, Mikaela – keep on being smart, kind and brave; that is all you ever need to be.

And to my mother, Rose – if I had seen further, it was only because I stood on the shoulders of a giant. Rest in peace, and rise in glory.

ACKNOWLEDGEMENTS

Glory be to the Most High, through whom all things are possible; I am grateful for the gift of health and strength to see this project through.

To my family who are always there for me and who support me through thick and thin.

To my university and staff for providing the facility, good graces and opportunity to allow me continue my studies.

To my work colleagues and staff who supported and understood me.

To my friends who had to put up with my absence in their lives, especially the ones I had to say ‘no’ often to.

To the very few special persons who have been there for me unconditionally through this process and beyond – you know yourselves.

I am grateful for everything. Thank you.

INDEX OF CONTENT

DEDICATION ii

ACKNOWLEDGEMENTS iii

INDEX OF FIGURES vi

INDEX OF CHARTS vii

ABBREVIATIONS AND ACRONYMS viii

EXECUTIVE SUMMARY (ABSTRACT) ix

1. INTRODUCTION 1

1.1 Background 1

1.2 Statement of Problem 2

1.3 Purpose 3

1.4 General Objective 4

1.5 Specific Objectives 5

2. THEORETICAL FRAMEWORK 6

2.1 Organizational/Enterprise Framework 6

2.2 Project Management Concepts 8

2.3 Project Management Methodologies 24

2.4 Creating a Project Management Methodology 26

2.5 Cyber Security Concepts 27

3. METHODOLOGICAL FRAMEWORK 32

3.1 Information Sources 32

3.3 Tools and Techniques 36

3.4 Assumptions and Constraints 37

3.5 Deliverables 39

4. RESULTS 40

4.1 Research and Survey 40

4.2 Proposed Assessment Methodology 42

4.3 Implementation of Proposed Assessment Methodology 46

5. CONCLUSION 47

6. RECOMMENDATIONS 49

BIBLIOGRAPHY 52

APPENDICES .... *I*

Appendix 1: Final Graduation Project – Project Charter I

Appendix 2: Final Graduation Project – Work Breakdown Structure IV

Appendix 3: Final Graduation Project – Schedule VIII

Appendix 4: Proof of Philological Corrections X

Appendix 5: Credentials of Linguist XI

Appendix 6: Cyber Security Survey Report XIII

Appendix 7: Proposed Cyber Security Assessment Methodology XXIV

Appendix 8: Implementation of Cyber Security Assessment of NEMC CXLV

INDEX OF FIGURES

Figure 1 Organizational structure of a typical business. 7
Figure 2 Project Management Life Cycle of a single stage project.......................... 9

INDEX OF CHARTS

Chart 1 Overview of the Project Integration Management Knowledge Area (Project Management Institute, 2013).. 12
Chart 2 Overview of the Project Scope Management Knowledge Area (Project Management Institute, 2013).. 13
Chart 3 Overview of the Project Time Management Knowledge Area (Project Management Institute, 2013).. 14
Chart 4 Overview of the Project Cost Management Knowledge Area (Project Management Institute, 2013).. 16
Chart 5 Overview of the Project Quality Management Knowledge Area (Project Management Institute, 2013).. 18
Chart 6 Overview of Project Human Resource Management Knowledge Area (Project Management Institute, 2013). 19
Chart 7 Overview of the Project Communications Management Knowledge Area (Project Management Institute, 2013). 20
Chart 8 Overview of the Project Risk Management Knowledge Area (Project Management Institute, 2013).. 21
Chart 9 Overview of the Project Procurement Management Knowledge Area (Project Management Institute, 2013). 22
Chart 10 Overview of the Project Stakeholder Management Knowledge Area (Project Management Institute, 2013). 23
Chart 11 Primary and Secondary Sources of information related to the objectives of the project. 33
Chart 12 Research Methods applied to the objectives of the project. 35
Chart 13 Tools and Techniques applied to the objectives of the project. 37
Chart 14 Assumptions and Constraints applied to the objectives of the project.... 38
Chart 15 Objectives and corresponding Deliverables of the project..................... 39

ABBREVIATIONS AND ACRONYMS

CPM	Critical Path Method
CS	Cyber Security
CSA	Cyber Security Assessment
CSF	Cyber Security Framework
ETSI	European Telecommunications Standards Institute
ICT	Information and Communications Technology
ISF	Information Security Forum
ISMS	Information Security Management System
ISO	International Standards Organization
IT	Information Technology
MoH	Ministry of Health
NEMC	National Engineering & Maintenance Center
NIST	National Institute of Standards and Technology
PERT	Program Evaluation and Review Technique
PM	Project Management
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
UK	United Kingdom
WBS	Work Breakdown Structure

EXECUTIVE SUMMARY (ABSTRACT)

After computers and communication networks became more affordable and came into mainstream usage, a plethora of technologies have been subsequently developed. Along with these technologies came new ways of communicating and sharing information and new ways of doing business. Today, the rapid evolution of information and communications technology has influence society both positively and negatively, from personal life at home, to business and government as well as international organizations with global scopes.

The development of new information and communications technologies comes with inherent security issues that have been exploited over time by actors with malicious intent, resulting in loss of revenues, delays, downtime and even harm and loss of human lives. As these technologies continue to develop at a rapid rate and as they become more integrated into society and businesses and critical government infrastructure and major utilities become increasingly integrated, these types of threats will increase and potential risks and losses will invariably increase as well.

Governments and interested parties have been hard-pressed into keeping up-to-date with strategies to counteract risks related to information and communications security and associated threats. Unfortunately, the Caribbean and Latin American region are a step behind compared to other regions in the world.

In the near future, it is expected that major focus will be placed on information and communications security in Belize and the wider Caribbean and Latin America region. In order to do this, one of the first practical steps is to conduct assessments of organizations to see where they stand in terms of cyber security readiness.

The general objective of this work is to develop a project management methodology for cyber security assessments based on existing information and communications technology infrastructure in order to assess the cyber security needs for organizations of various sizes. The specific objectives are: to assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments; to propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes; to develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments; and to create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.

The analytical methodology is primarily used in carrying out this work. Additional information is gathered by researching current documentation, by observing the current state of affairs and by interviewing and surveying key stakeholders in the industry. Current project management methodologies and cyber security standards, frameworks and related documentation are studied.

Based on information gathered by research, survey and interviews, a project management based methodology for cyber security assessment was proposed and designed. The proposed methodology incorporated a full complement of tools, techniques and templates and was structured and formulated to be used as an implementation guide.

The proposed methodology was successfully implemented at the National Engineering & Maintenance Center, Ministry of Health and the assessment process and results were used to refine various aspects of the proposed methodology further.

The general conclusion was that all objectives where met for this work. However, it is possible to further develop and refine the proposed methodology in future studies and implementations.

1. INTRODUCTION

1.1 Background

Since the dawn of the first commercially available computers in the 1950’s, information technology has evolved at a very fast rate and has become a ubiquitous part of almost every aspect of human existence.

An incremental step was taken with the advent of the Internet in the 1980’s along with the affordability of desktop computers that made it possible to create a true World Wide Web. The ensuing ability to share information in almost real time has allowed humanity to make advances in all aspect of civilization at an astonishing rate as communications and information technology became more and more accessible to almost everyone at all levels of society.

Computers, the software that runs on them, and the networks that connect them together are constantly communicating, from tiny handheld devices to vastly complex supercomputers used to perform very complex tasks. The complexities of these interconnections have been increasing at a staggering rate and the layers of technology and protocols that make them work have become more and more sophisticated.

Security breaches and the creation and proliferation of malware have also existed since the beginning of the modern communications and information technology revolution and the issue of securing information and related resources has become more and more challenging. The terms ‘hacker’, ‘computer viruses’ and ‘antivirus’ have become common, everyday words.

As society becomes more and more dependent on technology, the dangers from loss of information as well as downtime of critical services, and the possibility of the commission of criminal and terrorist acts are becoming more and more real.

Belize and the broader Latin America and the Caribbean region have advanced along with the more industrialized countries when it comes to the implementation of information and communications technology solutions, albeit in a delayed fashion. On a very similar note, it has not been until recently that the problem of cyber security is beginning to be addressed at the national and regional levels with the participation of stakeholders from both the public and the private sectors.

Presently, the mechanism and governance structures in most Caribbean countries are not available to readily respond to cyber-threats and the extent of the damage being done is difficult to determined accurately since most private enterprises are not obligated to report cyber-crime to the authorities and most prefer to not to do so.

1.2 Statement of Problem

Many organizations and businesses exist entirely because of information and communications technology and most others at least partially depend on information and communications as a service. At the same time, many of these organizations and businesses are understaffed or lack the technical knowhow and human resources to deal with cyber-threats when they occur.

Due to the lack of centralized mechanisms and governance structure in the country, it is difficult to get cyber security assistance and based on the negative repercussions of being a victim of cyber-crime, most organizations and businesses try as much as possible to keep these problems quiet when they do occur.

As organizations and businesses become more and more dependent on information and communications technologies, and as critical government infrastructure such as banking systems and major utilities become increasingly integrated with information and communications technology, cyber-threats will increase and potential risks and losses will also increase.

Having an integrated cyber security response and taking preventative measures is and will be vital for the survival of most organizations and businesses. Sensitization, information sharing and education at both the user level and the technical and administrative levels will be essential in providing effective approach.

In order to implement an adequate response and to establish an acceptable stance, it is necessary to implement changes to the organization in terms of their cyber security readiness. The first and most logical step is by means of an assessment of the current state of readiness of the organization.

The processes related to the cyber security assessment can best be implemented by means of a project management approach.

1.3 Purpose

The approach to bolster an organization's cyber security stance must be methodical and in line with current trends and technologies. It must be detailed and should take a systems approach, address all levels and aspects of the organization and should be intimately tied to the nature of the organization and the environment in which it exists. The attitudes of the people that use the related information and communications technology services as well as the social and economic environment and other geographical and regional factors must also be taken into consideration. Future growth and trends in technology must be a factor in securing information resources and having the right cyber security stance.

It is necessary as a first step to assess the cyber security needs of the organizations and businesses in question in order to make the changes necessary to harden their cyber security stance. This assessment can be carried out internally or externally as a project, more or less independent of the day-to-day operations of the organization or business in question. These assessments need to be tied to current national and regional cyber security guidelines and frameworks and the methodology used to carry out the assessments must be designed to be adoptable to most scenarios and cover all major aspects of cyber security.

The purpose of this study is to look at current trends in technology in order to come up with the necessary components, techniques, tools and implementation plans that will then form the basis of a proposed project management methodology for cyber security assessments.

A cyber security assessment designed and implemented using a project management approach is ideal for the following reasons:

1. Cyber security assessments are essentially risk assessments, and existing project management knowledge and approaches are well suited to deal with risk assessment and management.

2. Due to the lack of internal expertise when it comes to cyber security, most organizations will seek to obtain external expertise; this implies that short-term projects with hired expertise would be ideally suited to resolve these types of issues.

3. Cyber security assessments are short term with clearly defined objectives; this makes it ideally suited to apply a project management approach.

4. In using project management approach, resources will be managed more efficiently and interruption to business-as-usual will be minimal.

1.4 General Objective

The main objective of this work is to develop a project management methodology for cyber security assessments based on existing information and communications technology infrastructure in order to assess the cyber security needs for organizations of various sizes.

1.5 Specific Objectives

The specific objectives of this project are:

1. To assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.

2. To propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.

3. To develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.

4. To create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.

2. THEORETICAL FRAMEWORK

2.1 Organizational/Enterprise Framework

The actions necessary to achieve the objectives of this project may be performed over a very large geographical area and in various environments and different economic and cultural backgrounds. The target organizations will invariably have different purposes, structure and goals.

The organizations in question would also be of different sizes and would have unique qualities and challenges. The needs of these organizations are also expected to change over time.

As a part of implementing an assessment, it would be necessary to study and understand the environment and nature of each target organization.

2.1.1 Company/Enterprise Background

Most organizations that this work applies to are medium to large enterprises with varying levels of complexity, purposes and backgrounds. Those that produce communications and information technology as a product or service are of special interest. However, almost all organizations use information and communications technology in some form.

Even if information and communications technology products and services are not the focus of an organization, the larger and more complex it is, the higher the likeliness that it will be heavily dependent on information and communications technology. In some cases, even very small businesses are completely dependent on information and communications technology in order to function.

2.1.2 Mission and Vision

Since this work covers a broad range of organizations, the missions and visions would vary. It is important to note that the individual missions and visions of each organization will influence their requirements as it relates to their individual cyber security needs. This will in turn influence how each assessment will be planned and executed. For this reason, the proposed methodology would need to be sufficiently flexible in order to be applicable to as many scenarios as possible.

2.1.3 Organizational Structure

A depiction of a typical organization structure for a typical medium sized business is show in Figure 1. This is the most prevalent organizational structure. It normally consists of a board of directors, a chief executive officer or executive director, followed by managers and supervisors by function or division, and then the workers. The size and complexity of the structure would depend on the nature of the organization.

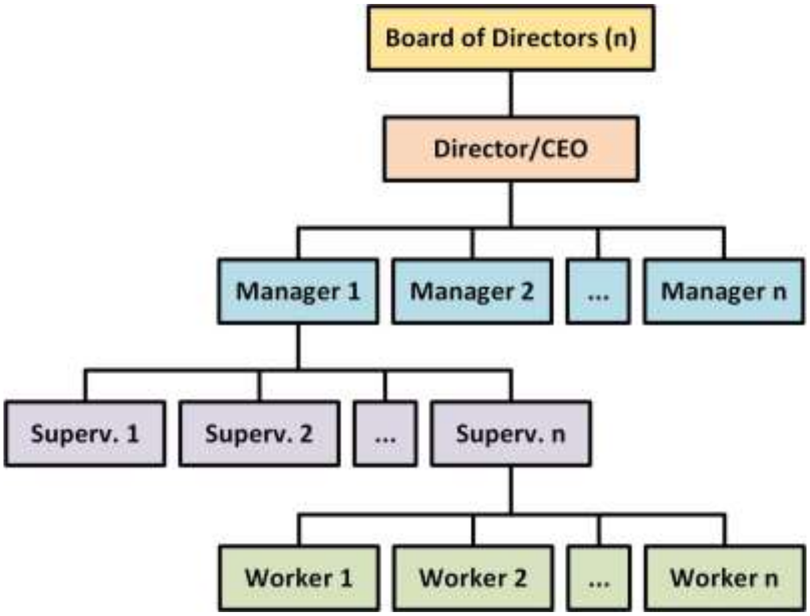


Figure 1 Organizational structure of a typical business.

2.1.4 Products Offered

Since this work covers a broad range of companies, the products and services offered by these organizations would vary. Most of the organizations that will benefit from the assessment methodology are essentially those that rely strongly on Information and Communications Technology (ICT) infrastructure in order to carry out their functions; these include organizations that have a lot of sensitive or private information as well as those that offer information and communications technology as a product or service. However, most organizations rely on some form or the other on information or communications technologies and therefore most of them stand to benefit.

2.2 Project Management Concepts

2.2.1 Project

A project is defined as “a temporary endeavor undertaken to create a unique product, service or result” (Project Management Institute, 2013).

A project is by definition temporary in the sense that it has a finite duration or timeline; this timeline will be consistent with the achievement of its scope which is all its defined goals and objectives. It is unique in the sense that it distinguishable from any other project or process.

A project has a cost associated with it, is shaped by the strategic goals of an organization or entity and is design to solve a problem or improve a system.

2.2.2 Project Management

Project Management is “the application of knowledge, skills, tools and techniques to project activities to meet the project requirements” (Project Management Institute, 2013). In other words, it is the discipline of initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and objectives within a specific period.

Apart from time and scope, a project is constrained by cost. This means that money and resources must be efficiently managed in order to successfully manage a project. Time, cost and scope are the main constraints however; there are many other factors that are critical to project success.

In practice, the management of projects is so diverse and critical that contemporary methodologies require experience, training and the development of distinct technical skills and management strategies.

2.2.3 Project Life Cycle

The project life cycle is defined as a "series of phases that a project passes through from its initiation to its closure" (Project Management Institute, 2013). The project life cycle provides a framework to manage any type of project and is used to guide the project from start to completion.

Figure 2 shows a graphical depiction of the phases and how they are interrelated in a simple single-phase project.

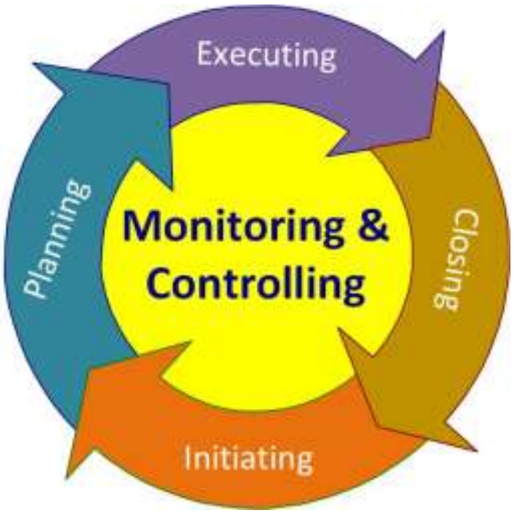


Figure 2 Project Management Life Cycle of a single stage project.

2.2.4 Project Management Process Groups

Project management processes are grouped together to form process groups. In essence, process groups are all the processes that form a phase in the project management life cycle and are related to each other. Each process group is outlined in the following subsections.

2.2.4.1 The Initiating Process Group

The Initiating Process Group is the first stage or group of processes. It helps to set the vision of what is to be accomplished. This is where the initial scope of the project is defined, the project is formally authorized by the sponsor and the stakeholders are identified. This process group is performed so that projects that are sanctioned and approved by a sponsoring entity are aligned with the strategic objectives of the organization.

2.2.4.2 The Planning Process Group

The Planning Process Group is where the roadmap or path to success is established. Important details such as milestones, cost, schedule and scope are laid out. Furthermore, a baseline is created in order to track progress.

2.2.4.3 The Executing Process Group

The Executing Process Group is where most of the budget will be spent and most of the deliverables will be produced. In essence, the project team carries out the tasks necessary to produce the objectives of the project with the guidance of the project manager who also controls resources and many other aspects of the project.

2.2.4.4 The Monitoring and Controlling Process Group

The Monitor and Controlling Process Group occur across all other process groups and therefore do not necessarily fit in sequentially into one part of the project life cycle. These are essentially processes that are required to keep track of, review and regulate the performance of the project. This group is also used to identify where changes or corrections need to be made to keep the project on track and to initiate the corresponding changes.

2.2.4.5 The Closing Process Group

The Closing Process Group is where the project is formally closed and acceptance and sign-off is obtained from the customer. In this process group, the remainder of all project deliverables are handed over and the final version of records are archived, lessons learnt are analyzed, final payments are made and contracts are closed. The project team and other resources are also released in this phase.

2.2.5 Project Management Knowledge Areas

A knowledge area represents “a complete set of concepts, terms, and activities that make up a professional field, project management field, or area of specialization” (Project Management Institute, 2013).

There are forty-seven processes that have been identified and grouped in Project Management Knowledge Areas. These knowledge areas are: Project Integration Management, Project Scope Management, Project Time Management, Project Cost Management, Project Quality Management, Project Human Resources Management, Project Communications Management, Project Risk Management, Project Procurement Management and Project Stakeholder Management.

Each of the ten knowledge areas contains the processes that are carried out in order to achieve effective project management although not all are necessary for every project.

2.2.5.1 Project Integration Management

Project Integration Management is comprised of “the processes and activities needed to identify, define, combine, unify, and coordinate the various processes and project management activities within the Project Management Process Groups” (Project Management Institute, 2013). An overview of Project Integration Management is shown in Chart 1.

Chart 1 Overview of the Project Integration Management Knowledge Area *(Project Management Institute, 2013)*.

Project Integration Management Overview		
4.1 Develop Project Charter	**4.2 Development Project management Plan**	**4.3 Direct and Manage Project Work**
.1 Inputs .1 Project statement of work .2 Business care .3 Agreements .4 Enterprise environmental factors .5 Organizational process assets .2 Tools & Techniques .1 Expert judgment .2 Facilitation techniques .3 Outputs .1 Project charter	.1 Inputs .1 Project charter .2 Output from other processes .3 Enterprise environmental factors .4 Organizational project assets .2 Tools & Techniques .1 Expert judgment .2 Facilitation techniques .3 Outputs .1 Project management plan	.1 Inputs .1 Project management plan .2 Approved change request .3 Enterprise environmental factors .4 Organizational process assets .2 Tool & Techniques .1 Expert judgment .2 Project management information system .3 Meetings .3 Outputs .1 Deliverables .2 Work performance data .3 Change requests .4 Project management plan updates .5 Project documents updates
4.4 Monitor and Control Project Work	**4.5 Perform Integrated Change Control**	**4.6 Close Project or Phase**
1. Inputs .1 Project management plan .2 Schedule forecasts .3 Cost forecasts .4 Validated changes .5 Work performance information .6 Enterprise environmental factors .7 Organizational process assets 2. Tools & Techniques .1 Expert judgment .2 Analytical techniques .3 Project management information system .4 Meetings 3. Outputs .1 Change Requests .2 Work performance report .3 Project management plan updates .4 Project document updates	1. Inputs .1 Project management plan .2 Work performance report .3 Change requests .4 Enterprise environmental factors .5 Organizational process assets 2. Tools & Techniques .1 Expert judgment .2 Meetings .3 Change control tools 3. Outputs .1 Approved change requests .2 Change log .3 Project management plan updates .4 Project document updates	1. Inputs .1 Project management plan .2 Accepted deliverables .3 Organizational project assets 2. Tools & Techniques .1 Expert judgment .2 Analytical techniques .3 Meetings 3. Outputs .1 Final product, service, or result transition .2 Organizational process assets updates

2.2.5.2 Project Scope Management

Project Scope Management is comprised of “the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully" (Project Management Institute, 2013). An overview of Project Scope Management is shown in Chart 2.

Chart 2 Overview of the Project Scope Management Knowledge Area *(Project Management Institute, 2013)*.

Project Scope Management Overview		
5.1 Plan Scope Management	**5.2 Collect Requirements**	**5.3 Define Scope**
1. Inputs 1. Project management plan 2. Project charter 3. Enterprise environmental factors 4. Organizational process assets 2. Tools & Techniques 1. Expert judgment 2. Meetings 3. Outputs 1. Scope management plan 2. Requirements management plan	1. Inputs 1. Score management plan 2. Requirements management plan 3. Stakeholder management plan 4. Project charter 5. Stakeholder register 2. Tools & Techniques 1. Interviews 2. Focus groups 3. Facilitated workshops 4. Group creativity techniques 5. Group decision-making techniques 6. Questionnaires and surveys 7. Observations 8. Prototypes 9. Benchmarking 10. Context diagrams 11. Document analysis 3. Outputs 1. Requirements documentation 2. Requirements traceability matrix	1. Inputs .1 Scope management plan .2 Project charter .3 Requirements documentation .4 Organizational process assets .2 Tools & Technician .1 Expert judgment .2 Product analysis .3 Alternatives generation .4 Facilitated workshops .3 Outputs .1 Project scope statement .2 Project documents updates
5.4 Create WBS	**5.5 Validate Scope**	**5.6 Scope Control**
.1 Inputs .1 Scope management plan .2 Project scope statement .3 Requirements documentation .4 Enterprise environmental factors .5 Organizational process assets .2 Tools & Techniques .1 Decomposition .2 Expert judgment .3 Outputs .1 Scope baseline .2 Project documents updates	.1 Inputs .1 Project management plan .2 Requirements documentation .3 Requirements traceability matrix .4 Verified deliverables .5 Work performance data .2 Tools & Techniques .1 Inspection .2 Group decision-making techniques .3 Outputs .1 Accepted deliverables .2 Change requests .3 Work performance information .4 Project documents updates	1. Inputs 1. Project management plan 2. Requirements documentation 3. Requirements traceability matrix 4. Work performance data 5. Organizational process assets 2. tools & Techniques 1. Variance analysis 3. Outputs 1. Work performance information 2. Change requests 3. Project management plan updates 4. Project documents updates 5. Organizational process assets updates

2.2.5.3 Project Time Management

Project Time Management is comprised of “the processes required to manage the timely completion of the project” (Project Management Institute, 2013). An overview of Project Time Management is shown in Chart 3.

Chart 3 Overview of the Project Time Management Knowledge Area *(Project Management Institute, 2013)*.

Project Time Management Overview			
6.1 Plan Schedule Management	**6.2 Define Activities**	**6.3 Sequence Activities**	**6.4 Estimate Activity Resource**
.1 Inputs .1 Project management plan .2 Project Charter .3 Enterprise environmental factors .4 Organizational process assets .2 Tools & Techniques .1 Expert Judgment .2 Analytical techniques .3 Meetings .3 Outputs .1 Schedule management plan	.1 Inputs .1 Schedule management .2 Scope baseline .3 Enterprise environmental factors .4 Organizational process assets .2 Tools & Techniques .1 Decomposition .2 Rolling wave planning .3 Expert Judgment .3 Outputs .1 Activity list .2 Activity .3 Attributes .4 Milestone list	.1 Inputs .1 Schedule management plan .2 Activity list .3 Activity attributes .4 Milestone list .5 Project Scope Statement .6 Enterprise environmental factors .7 Organizational process assets .2 Tools & Techniques .1 Precedence diagramming method (PDM) .2 Dependency determination .3 Leads and logs .3 Outputs .1 Project schedule network diagrams .2 Project documents updates	.1 Inputs .1 Schedule management plan .2 Activity list .3 Activity attributes .4 Resource calendar .5 Risk register .6 Activity cost estimates .7 Enterprise environmental factors .8 Organizational process assets .2 Tools & Techniques .1 Expert judgment .2 Alternative analysis .3 Published estimated data .4 Bottom-up estimating .5 Project management software .3 Outputs .1 Activity resource requirements .2 Resource breakdown structure .3 Project documents updates

6.5 Estimate Activity Durations	**6.6 Developing Schedule**	**6.7 Control schedule**	
.1 Inputs .1 Schedule management plan .2 Activity list .3 Activity attributes .4 Activity resource requirements .5 Resource calendars .6 Project scope statement .7 Risk register .8 Resource breakdown structure .9 Enterprise environmental factors .10 Organizational process assets .2 Tools & Techniques .1 Expert Judgment .2 Analogous estimating .3 Parametric estimating .4 Three-point estimating .5 Group decision-making techniques .6 Reserve analysis .3 Outputs .1 Activity duration estimates .2 Project documents updates	.1 Inputs .1 Schedule management plan .2 Activity list .3 Activity attributes .4 Project schedule network diagrams .5 Activity resource requirement .6 Resource calendars .7 Activity duration estimates .8 Project scope statement .9 Risk register .10 Project staff assignments .11 Resource breakdown structure .12 Enterprise environmental factors .13 Organizational process assets .2 Tools & Techniques .1 Schedule network analysis .2 Critical path method .3 Critical chain method .4 Resource optimization techniques .5 Modeling techniques .6 Leads and lags .7 Schedule compression .8 Scheduling tool .3 Outputs .1 Schedule baseline .2 Project schedule .3 Schedule data .4 Project calendars .5 Project management plan updates .6 Project document updates	.1 Inputs .1 Project management plan .2 Project schedule .3 Work performance data .4 Project calendars .5 Schedule data .6 Organizational process assets .2 Tools & Techniques .1 Performance review .2 Project management software .3 Resource optimization techniques .4 Modeling techniques .5 Leads and lags .6 Schedule compression .7 Scheduling tool .3 Outputs .1 Work performance information .2 Schedule forecasts .3 Change requests .4 Project management plan updates .5 Project document updates .6 Organizational process assets updates	

2.2.5.4 Project Cost Management

Project Cost Management is comprised of “the processes involved in planning, estimating, budgeting, financing, funding, managing, and controlling costs so that the project can be completed within the approved budget” (Project Management Institute, 2013). An overview of Project Cost Management is shown in Chart 4.

Chart 4 Overview of the Project Cost Management Knowledge Area *(Project Management Institute, 2013)*.

Project Cost Management Overview		
7.1 Plan Cost Management	**7.2 Estimate Costs**	**7.3 Determine Budget**
.1 Inputs .1 Project management plan .2 Project charter .3 Enterprise environmental factors .4 Organizational process assets .2 Tools & Techniques .1 Expert judgment .2 Analytical techniques .3 Meetings .3 Outputs .1 Cost management plan	.1 Inputs .1 Cost management plan .2 Human resource .3 management plan .4 Scope baseline .5 Project Schedule .6 Risk register .7 Enterprise environmental factors .8 Organizational process assets .2 Tools & Techniques .1 Expert judgment .2 Analogous estimating .3 Parametric estimating .4 Bottom-up estimating .5 Three-point estimating .6 Reserve analysis .7 Cost of quality .8 Project management software .9 Vendor bid analysis .10 Group decision-making techniques .3 Outputs .1 Activity cost estimate .2 Basis of estimates .3 Project documents updates	.1 Inputs .1 Cost management plan .2 Scope baseline .3 Activity cost estimates .4 Basis of estimates .5 Project schedule .6 Resource calendars .7 Risk register .8 Agreements .9 Organizational process assets .2 Tools & Techniques .1 Cost aggregation .2 Reserve analysis .3 Expert judgment .4 Historical relationships .5 Funding limit reconciliaion .3 Outputs .1 Cost baseline .2 Project funding requirements .3 Project documents updates

7.4 Control Costs		
.1 Inputs .1 Project management plan .2 Project funding requirements .3 Work performance data .4 Organizational process assets .2 Tools &Techniques .1 Earned value management .2 Forecasting .3 To-complete performance index (TCPI) .4 Performance reviews .5 Project management software .6 Reserve analysis .3 Outputs .1 Work performance information .2 Cost forecasts .3 Change requests .4 Project management plan updates .5 Project documents updates .6 Organizational process assets updates		

2.2.5.5 Project Quality Management

Project Quality Management is comprised of “the processes and activities of the performing organization that determine quality policies, objectives, and responsibilities so that the project will satisfy the needs for which it was undertaken” (Project Management Institute, 2013). An overview of Project Quality Management is shown in Chart 5.

Chart 5 Overview of the Project Quality Management Knowledge Area *(Project Management Institute, 2013)*.

Project Quality Management Overview		
8.1 Plan Quality Management	**8.2 Perform Quality Assurance**	**8.3 Control Quality**
.1 Inputs .1 Project management plan .2 Stakeholder register .3 Risk register .4 Requirements documentation .5 Enterprise environmental factors .6 Organizational process assets .2 Tools & Techniques .1 Cost-benefit analysis .2 Cost of quality .3 Seven basic quality tools .4 Benchmarking .5 Design of experiments .6 Statistical sampling .7 Additional quality planning tools .8 Meetings .3 Outputs .1 Quality management plan .2 Process improvement plan .3 Quality metrics .4 Quality checklists .5 Projects documents updates	.1 Inputs .1 Quality management plan .2 Process improvement plan .3 Quality metrics .4 Quality control .5 measurements .6 Project documents .2 Tools & Techniques .1 Quality management and control tools .2 Quality audits .3 Process analysis .3 Outputs .1 Change requests .2 Project management plan updates .3 Project documents .4 updates .5 Organizational process assets updates	.1 Inputs .1 Project management plan .2 Quality metrics .3 Quality checklists .4 Work performance data .5 Approved change requests .6 Deliverables .7 Project documents .8 Organizational process assets .2 Tools & Techniques .1 Seven basic quality tools .2 Statistical sampling .3 Inspection .4 Approved change request overview .3 Outputs .1 Quality control measurements .2 Validated changes .3 Verified deliverables .4 Work performance information .5 Change requests .6 Project management plan updates .7 Project document updates .8 Organizational process assets updates

2.2.5.6 Project Human Resource Management

Project Human Resource Management is comprised of “the processes that organize, manage, and lead the project team” (Project Management Institute, 2013). An overview of Project Human Resource Management is shown in Chart 6.

Chart 6 Overview of Project Human Resource Management Knowledge Area *(Project Management Institute, 2013)*.

Project Human Resource Management Overview		
9.1 Plan Human Resource Management	**9.2 Acquire Project Team**	**9.3 Develop Project Team**
.1 Inputs .1 Project management plan .2 Activity resource requirements .3 Enterprise environmental factors .4 Organizational process assets .2 Tools & Techniques .1 Organization charts and position description .2 Networking .3 Organizational theory .4 Expert judgment .5 Meetings .3 Outputs .1 Human resource management plan	.1 Inputs .1 Human resource management plan .2 Enterprise environmental factors .3 Organizational process assets .2 Tools & Techniques .1 Pre-assignment .2 Negotiation .3 Acquisition .4 Virtual teams .5 Multi-criteria decision analysis .3 Outputs .1 Project staff assignments .2 Resource calendars .3 Project management plan updates	.1 Inputs .1 Human resource management plan .2 Project staff assignments .3 Resource calendars .2 Tools & Techniques .1 Interpersonal skills .2 Training .3 Team-building activities .4 Ground rules .5 Co-location .6 Recognition and rewards .7 Personal assessment tools .3 Outputs .1 Team performance assessment tools .2 Enterprise environmental factors updates
9.4 Manage Project Team		
.1 Inputs .1 Human resource management plan .2 Project staff assignments .3 Team performance assessments .4 Issue log .5 Work performance reports .6 Organizational process assets .2 Tools & Techniques .1 Observation and conversation .2 Project performance appraisals .3 Conflict management .4 Interpersonal skills .3 Outputs .1 Change requests .2 Project management plan updates .3 Project document updates .4 Enterprise environmental factors updates Organizational process assets updates		

2.2.5.7 Project Communications Management

Project Communications Management is comprised of “the processes that are required to ensure timely and appropriate planning, collection, creation, distribution, storage, retrieval, management, control, monitoring, and the ultimate disposition of project information” (Project Management Institute, 2013). An overview of Project Communications Management is shown in Chart 7.

Chart 7 Overview of the Project Communications Management Knowledge Area *(Project Management Institute, 2013)*.

Project Communications Management Overview		
1.01 Plan Communications Management	**10.2 Manage Communications**	**10.3 Control Communications**
.1 Inputs .1 Project management plan .2 Stakeholder register .3 Enterprise environmental factors .4 Organizational process assets .2 Tools & Techniques .1 Communication requirements analysis .2 Communication technology .3 Communication models .4 Communication methods .5 Meetings .3 Outputs .1 Communications management plan .2 Project documents updates	.1 Inputs 1. Communications management plan 2. Work performance reports 3. Enterprise environmental factors 4. Organizational process assets .2 Tools & Techniques 1. Communication technology 2. Communication models 3. Communication methods 4. Communications management systems 5. Performance reporting .3 Outputs 1. Project communications 2. Project management plan updates 3. Project documents updates 4. Organizational process assets updates	.1 Inputs .1 Project management plan .2 Project communications .3 Issue log .4 Work performance data .5 Organizational process assets .2 Tools & Techniques .1 Information management systems .2 Expert management .3 Meetings .3 Outputs .1 Work performance information .2 Change requests .3 Project management plan updates .4 Project documents updates .5 Organizational process assets updates

2.2.5.8 Project Risk Management

Project Risk Management is comprised of “the processes of conducting risk management planning, identification, analysis, response planning, and controlling risk on a project” (Project Management Institute, 2013). An overview of Project Risk Management is shown in Chart 8.

Chart 8 Overview of the Project Risk Management Knowledge Area *(Project Management Institute, 2013)*.

Project Risk Management Overview		
11.1 Plan Risk Management	**11.2 Identity Risks**	**11.3 Perform Qualitative Risk Analysis**
.1 Inputs .1 Project management plan .2 Project charter .3 Stakeholder register .4 Enterprise environmental factors .5 Organizational process assets .2 Tools & Techniques .1 Analytical techniques .2 Expert judgment .3 Meetings .3 Outputs .1 Risk management plan	.1 Inputs .1 Risk management plan .2 Cost management plan .3 Schedule management plan .4 Quality management plan .5 Human resource management plan .6 Scope baseline .7 Activity cost estimates .8 Activity duration estimates .9 Stakeholder register .10 Project documents .11 Procurement documents .12 Enterprise environmental factors .13 Organizational process assets .2 Tools & Techniques .1 Documentation reviews .2 Information gathering techniques .3 Checklist analysis .4 Assumptions analysis .5 Diagramming techniques .6 SWOT analysis .7 Expert judgment .3 Outputs .1 Risk register	.1 Inputs .1 Risk management plan .2 Scope baseline .3 Risk register .4 Enterprise environmental factors .5 Organizational process assets .2 Tools & Techniques .1 Risk probability and impact assessment .2 Probability and impact matrix .3 Risk data quality assessment .4 Risk categorization .5 Risk urgency assessment .6 Expert judgment .3 Outputs .1 Project documents updates

11.4 Perform Quantitative Risk Analysis	11.5 Plan Risk Responses	11.6 Control Risks
.1 Inputs .1 Risk management plan .2 Cost management plan .3 Schedule management plan .4 Risk register .5 Enterprise environmental factors .6 Organizational process assets .2 Tools & Techniques .1 Data gathering and representation techniques .2 Quantitative risk analysis and modeling techniques .3 Expert judgment .3 Outputs .1 Project documents updates	.1 Inputs .1 Risk management plan .2 Risk register .2 Tools & Techniques .1 Strategies for negative risks or threats .2 Strategies for positive risks or opportunities .3 Contingent response strategies .4 Expert judgment .3 Outputs .1 Project management plan updates .2 Project documents updates	.1 Inputs .1 Project management plan .2 Risk register .3 Work performance data .4 Work performance reports .2 Tools & Techniques .1 Risk reassessment .2 Risk audits .3 Variance and trend analysis .4 Technical performance measurement .5 Reserve analysis .6 Meetings .3 Outputs .1 Work performance information .2 Change requests .3 Project management plan updates .4 Project documents updates .5 Organizational process assets updates

2.2.5.9 Project Procurement Management

Project Procurement Management is comprised of "the processes necessary to purchase or acquire products, services, or results needed from outside the project team" (Project Management Institute, 2013). An overview of Project Procurement Management is shown in Chart 9.

Chart 9 Overview of the Project Procurement Management Knowledge Area *(Project Management Institute, 2013)*.

Project Procurement Management Overview		
12.1 Plan Procurement Management	**12.2 Conduct Procurements**	**12.3 Control Procurements**
.1 Inputs .1 Project management plan .2 Requirements documentation .3 Risk register .4 Activity resource requirements .5 Project schedule .6 Activity cost estimates .7 Stakeholder register .8 Enterprise environmental factors .9 Organizational process assets .2 Tools & Techniques .1 Make-or-buy analysis .2 Expert judgment .3 Market research .4 Meetings	.1 Inputs .1 Procurement management plan .2 Procurement documents .3 Source selection criteria .4 Seller proposals .5 Project documents .6 Make-or-buy decisions .7 Procurement statement of work .8 Organizational process assets .2 Tools & Techniques .1 Bidder conference .2 Proposal evaluation techniques .3 Independent estimates .4 Expert judgment .5 Advertising	.1 Inputs .1 Project management plan .2 Procurement documents .3 Agreements .4 Approved change requests .5 Work performance reports .6 Work performance data .2 Tools & Techniques .1 Contract change control systems .2 Procurement performance reviews .3 Inspections and audits .4 Performance reporting .5 Payment systems .6 Claims administration .7 Records management systems .8 Outputs

.3 Outputs .1 Procurement management plan .2 Procurement statement of work .3 Procurement documents .4 Source selection criteria .5 Make-or-buy decisions .6 Change requests .7 Project documents updates	.6 Analytical techniques .7 procurement negotiations .3 Outputs .1 Selected sellers .2 Agreements .3 Resource calendars .4 Change requests .5 Project management plan updates .6 Project documents updates	.9 Work performance information .10 Change requests .11 Project management plan updates .12 Project documents updates .13 Organizational process assets updates
12.4 Close Procurements		
.1 Inputs 1. Project management plan 2. Procurement documents 3. Tools & Techniques 4. Procurement audits 5. Procurement negotiations 6. Records management system .2 Outputs 1. Close procurements 2. Organizational process assets updates		

2.2.5.10 Project Stakeholder Management

Project Stakeholder Management is comprised of "the processes required to identify all people or organizations impacted by the project, analyzing stakeholder expectations and impact on the project, and developing appropriate management strategies for effectively engaging stakeholders in project decisions and execution" (Project Management Institute, 2013). An overview of Project Stakeholder Management is outlined in Chart 10.

Chart 10 Overview of the Project Stakeholder Management Knowledge Area *(Project Management Institute, 2013)*.

Project Stakeholder Management Overview		
13.1 Identify Stakeholders	**13.2 Plan Stakeholder Management**	**13.3 Manage Stakeholder Engagement**
.1 Inputs .1 Project charter .2 Procurement documents .3 Enterprise environmental factors .4 Organizational process assets .2 Tools & Techniques .1 Stakeholder analysis .2 Expert judgment .3 Meetings .3 Outputs .1 Stakeholder register	.1 Inputs .1 Project management plan .2 Stakeholder register .3 Enterprise environmental factors .4 Organizational process assets .2 Tools & Techniques .1 Expert judgment .2 Meetings .3 Analytical techniques .3 Outputs .1 Stakeholder management plan .2 Project documents updates	.1 Inputs .1 Stakeholder management plan .2 Communications management plan .3 Change log .4 Organizational process assets .2 Tools & Techniques .1 Communication methods .2 Interpersonal skills .3 Management skills .3 Outputs .1 Issue log .2 Change requests .3 Project management plan updates

		.4 Project documents updates .5 Organizational process assets updates
13.4 Control Stakeholder Engagement		
.1 Inputs .1 Project management plan .2 Issue log .3 Work performance data .4 Project documents .2 Tools & Techniques .1 Information management systems .2 Expert judgment .3 Meetings .3 Outputs .1 Work performance information .2 Change requests .3 Project management plan updates .4 Project documents updates .5 Organizational process assets updates		

2.3 Project Management Methodologies

There are various project management methodologies in existence, each with various levels of completeness and designed for various environments and project types.

The most well-known and perhaps the most complete methodology is that offered by the Project Management Institute (PMI) and documented in various documents, the main reference document being *A Guide to the Project Management Book of Knowledge (PMBOK® Guide)*. The following are examples of other well-known project management methodologies:

- Agile – in this method, projects are broken down into short delivery cycles or milestones. This method is best suited for projects that need to be flexible and fast. It is focused on continuous development of a product or service (Alexander, 2018).
- Traditional Project Management – in this method, the project manager simply assess the various tasks for the project, and then provides a process to oversee and monitor the completion of the project. This method is based

on experience and predictability (Mrsic, Traditonal Project Management, 2017).

- Waterfall – in this method, each task depends on a previous one, and everything needs to be accomplished in sequence. Put simply, it is a sequential project management process that is normally geared towards software development. (Powell-Morse, 2016).
- Adaptive – in the adaptive method, the scope varies a lot, but not necessarily with time and cost. This method is best suited for business processes (Mrsic, Adaptive Project Management, 2017).
- Critical Path – this method is a systematic process that works well for projects in which tasks are dependent on one another. It is essentially a sequence of stages where the least time necessary to complete a task is determined (Ray, 2018).
- PERT – this method is often used in conjunction with the Critical Path Method (CPM). It stands for Program Evaluation and Review Technique and is well suited for developmental processes and manufacturing. It is a graphical tool to schedule, organize and coordinate tasks (Icasas, 2014).
- Critical Chain – This method builds on PERT and the Critical Path Method, except that it is oriented towards cost savings and benefits by reducing project time and making the schedule of the project more reliable (Mrsic, Critical Chain Project Management, 2017).
- Scrum – this is a methodology that is similar to the Agile Method, the project is divided into sprints or sessions and is facilitated by a Scrum Master rather than a project manager (Littlefield, 2016).
- Six Sigma – this is a methodology that data-driven and is focused in improving business processes and increase profits, primarily in a manufacturing environment (Graves, 2012).

2.4 Creating a Project Management Methodology

A project management methodology is a standardized, repeatable and documented collection of processes, tools, techniques and templates for managing projects. It is the main guiding resource that is used to deliver the project to completion.

It must also reflect the sizes and complexity of the projects that uses it and ideally be based on best practices that have already been found to be effective. It should also be flexible and scalable enough to be able to use on all related projects.

It is possible, and at times necessary, to implement or create a project management methodology in order to satisfy the requirements of an organization or to manage a specific subset of projects.

The following subsections gives additional insights on the process involved in the creation of a project management methodology.

2.4.1 Project Management Methodology Creative Process

In order to formulate a project management methodology, the processes involved are briefly outlined as follows:

- Maturity Assessment – study of the current state of the art and the maturity of the organization or organizations for which the methodology is being create.
- Development – the process of putting together the methodology along with the associated tools, techniques and templates and other related documentation.
- Implementation – the practical application of the methodology on real projects in order to test its effectiveness and then its proliferation to end users.

- Post-Implementation – continued implementation of the methodology, and adjusting and improving it based on feedback and experience obtained.

2.4.2 Existing Versus Customized Project Management Methodologies

In most cases, it may be possible to use existing, well-established methodology that best matches the environment and the type of projects that are being implemented. However, in some cases, it may be determined that it is more suitable to create a customized or tailored methodology based on current best practices and requirements.

There are benefits to developing or tailoring a methodology as opposed to using one that already exists. The main advantage is that it would be more efficient and better suited for a particular subset of projects or situations and is more readily accepted by users if it is written for them and in a way that they understand. However, one of the disadvantages of this approach is that it takes a lot of time and resources to develop.

2.5 Cyber Security Concepts

2.5.1 Information and Communications Technology

Information and communications technology is the infrastructure and components necessary to enable modern computing and communication. The term is generally accepted to mean all devices, network components, applications and systems that combine to allow people, devices and organizations to interact.

Information and communications technology encompasses but is not limited to the Internet and its components as well as mobile and cellular networks. It also includes older technologies such as landlines telephones, and radio and television broadcasts as well as navigation and other similar communications systems.

Information and Communications Technology is often used synonymously with information technology (IT). However, it more adequately used to represent a broader, more comprehensive list of all components related to the computer and digital technologies.

Information and communications technology is more than just electronic components and devices and networks; it also encompasses the application of and rational use of these technologies. As it keeps on developing and evolving, the more useful and pervasive it will become and it is in this dependency that cyber security will become an increasingly important issue.

2.5.2 Cyber Security

Cyber security (also called computer security or information technology security) is the protection of information and communications systems from the theft and damage to hardware, software or information, as well as from the disruption and misdirection of the services they provide.

More specifically, cyber security is the body of technologies, practices and processes designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

2.5.3 Cyber Security Trends in the Region

When combined, Latin America and the Caribbean have the fastest growing Internet usage in the world. This rise in usage corresponds to an increase in cyber security incidents and threats in the region over the past few years.

The general observation in the Caribbean is that mechanisms for dealing with cyber-crime are not widely in place at the organizational level and not well developed at the national level. Many countries lack a coherent strategy to manage the issues related to cyber security. At the same time, there appear to be a gradual awareness of the threat posed by cybercrime by various governments, and this signals a readiness of the development of improved cyber security infrastructure in the region (Organization of American States, 2014).

2.5.4 Common Cyber Security Frameworks

Cyber security frameworks, standards, norms or guidelines are collections of documents, procedures, tools, and techniques that attempt to protect the cyber environment of a user or an organization. This environment includes the users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. The principal objective of these frameworks is to reduce cyber security related risks, including prevention or mitigation of cyber-attacks.

Most of the mainstream frameworks, standards, norms and guidelines are comprehensive with published materials consisting of policies, security concepts, security safeguards, risk management approaches, best practices and other technologies.

The following subsections outline some of the more well-known frameworks available.

2.5.4.1 ISF Standard of Good Practice for Information Security

The Information Security Forum (ISF) is an independent, not-for-profit organization dedicated to investigating, clarifying and resolving key issues in information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its members

The ISF delivers a range of contents, activities, and tools. One of its primary products is the *Standard of Good Practice for Information Security.* This standard is a business-focused, practical and comprehensive guide for identifying and managing information security risks in organizations (Information Security Forum, 2008).

2.5.4.2 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) is a measurement standards laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

One of the publications of NIST is the *Framework for Improving Critical Infrastructure Cybersecurity*, also known as the *NIST Cybersecurity Framework (NIST CSF)* which provides a policy framework of computer security guidance for how private and public sector organizations can assess and improve their ability to identify, prevent, detect, respond and recover from cyber-attacks (National Institute of Standards and Technology, 2018).

The framework is designed with the intention that individual businesses and other organizations can easily implement it in order to assess the business risks they face related to cyber security.

2.5.4.3 UK Government Cyber Essentials

The *United Kingdom (UK) Government's Cyber Essentials* is a government-backed, industry-supported scheme to help organizations protect themselves against common cyber-attacks. It has been developed by government and industry to fulfill two functions: it provides a clear statement of the basic controls all organizations should implement to mitigate the risk from common internet based threats and it offers a mechanism for organizations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions (UK Government, 2018).

2.5.4.4 ISO 27000 Family of Standards

The *ISO 27000 Family of Standards* is a series of standards developed by the International Standards Organization (ISO). These standards describe management systems used to manage information security risks and controls within an organization. Bringing information security deliberately under overt management control is a central principle throughout the standards.

The ISO 27001 Standard is one of the more well-known standards of the ISO 27000 family. It is a specification for an Information Security Management System (ISMS). Organizations that meet the standard may be certified compliant by an independent and accredited certification body on successful completion of a formal compliance audit (International Standards Organization, 2018).

Another well-known standard in the family is the *ISO 27002 Standard*. It provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (Isect Ltd., 2018).

2.5.4.5 ETSI Standards for Cyber Security

The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization in the telecommunications industry in Europe. It produces globally applicable standards for information and communications technologies.

Rather than offering a unifying framework, ETSI offers a series of fully developed standards to match different use cases and specific needs such as information sharing and computer forensics (European Telecommunications Standards Institute, 2008).

3. METHODOLOGICAL FRAMEWORK

3.1 Information Sources

An information source is a person, thing or place from which information comes, arises, or is obtained. Information sources can be divided into separate distinct categories, such as primary, secondary and so on. They are also classified as physical (print, analog) versus online (electronic, digital) as well as textual versus audio-visual. A final classification would be books versus journal, magazine or articles and so forth.

The recentness of the information source is important, i.e. how recent the information has been published. Other aspects to take into consideration is the type of information and how easily it can be obtained.

3.1.1 Primary Sources

The *Yale University Library Research Guides* defines a primary source of information as “original materials on which other research is based” (Yale University Library Research Guides, 2017).

Primary sources of information should be from around the time period involved and have not been altered or filtered through interpretation or evaluation. They are usually the first formal appearance of results in physical, print or electronic format and present original thinking, or they report a discovery or share new information.

3.1.2 Secondary Sources

The *Yale University Library Research Guide* defines secondary sources of information as “interpretations and evaluations of primary sources”; it goes on to say that secondary sources are “not evidence, but rather commentary on and discussion of evidence” (Yale University Library Research Guides, 2017)

In general, secondary sources of information are accounts written after-the-fact with the benefit of hindsight and are frequently interpretations and evaluations of primary sources.

For this work, Chart 11 shows a listing of primary and secondary sources.

Chart 11 Primary and Secondary Sources of information related to the objectives of the project.

Objectives	**Information Sources**	
	Primary	**Secondary**
To assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.	Regional assessments and report Existing project management documentation Existing frameworks and guidelines	Interviews with various stakeholders Existing news articles and other journalistic sources Local government authorities Experts in the field
To propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.	Regional assessments and report Existing project management documentation Existing frameworks and guidelines	Interviews with various stakeholders Local government authorities Experts in the field
To develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.	Regional assessments and report Existing project management documentation Existing frameworks and guidelines	Interviews with various stakeholders Experts in the field
To create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.	Regional assessments and report Existing project management documentation Existing frameworks and guidelines	Interviews with various stakeholders Experts in the field

3.2 Research Methods

The *Merriam-Webster Dictionary* defines research as “investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws” (Merriam-Webster, 2018).

There are different forms of research as well as different research methods. The research method is the process that is taken to produce the knowledge or understanding of a topic being investigated. There are no distinct boundaries between research methods and there are various processes that can be used to gather information on the same topic. Due to the investigative nature of this project, the four main methods used are outlined in the following subsections.

3.2.1 Analytical Method

The analytical method consists of the evaluation of facts and existing information in order to analyze and identify problems and potential solutions. This is the main method that is used during the course of this project.

3.2.2 Observation

The observation method is a systematic data collection approach where researchers use all of their senses to examine ongoing behavior in naturally occurring settings.

In this project, the observation method will be use to examine system users as they interact with information and communications technology in the context of behaviors relevant to cyber security.

3.2.3 Interviews

An interview refers to a one-on-one conversation with one person acting in the role of the interviewer, asking the questions; the other person is the interviewee who is the source of information relevant to the research topic. As a research method, interviews are used to gather information and insights that are not often apparent using other methods such as observation and experimentation.

There are various kinds of interviews; this project will depend mainly on unstructured interviews in order to gather information and insights on the current state of information and communications security. The interviews will be conducted primarily with industry professionals and system users.

3.2.4 Surveys

Surveys are instruments that are used to gather data from individuals from a certain population. This is done over a certain sample size of the number of individuals of the population being studied. Typically, an established questionnaire with a pre-established set of questions is used for all individuals of the population.

For this project, a survey will be done to complement the information gathered from the interview in order to add structure to the information being gathered.

Chart 12 Research Methods applied to the objectives of the project.

Objectives	Research Methods		
	Analytical Method	Observation	Interviews/Surveys
To assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.	To allow for analysis of existing and information obtained in order to assess and select appropriate framework and guidelines and to determine main components.	Use to gather information to supplement main information sources and support decision-making.	Use to gather information to supplement main information sources and support decision-making.
To propose and develop a project	To allow for analysis of existing and information	Use to gather information to	Use to gather information to

Objectives	Research Methods		
	Analytical Method	Observation	Interviews/Surveys
management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.	obtained in order to propose the project management methodology.	supplement main information sources and support decision-making.	supplement main information sources and support decision-making.
To develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.	To allow for analysis of existing and information obtained in order to develop the necessary project management templates, tools and techniques.	Not applicable.	Not applicable.
To create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.	To allow for analysis of existing and information obtained in order to formulate implementation plan.	Not applicable.	Not applicable.

3.3 Tools and Techniques

A tool is defined as “something tangible, such as a template or software program, used in performing an activity to produce a product or result” (Project Management Institute, 2013). A technique is the particular method that is used to carry out an activity or procedure.

Chart 13 lists the various tools and techniques that are used in executing this project.

Chart 13 Tools and Techniques applied to the objectives of the project.

Objectives	Tools and Techniques
To assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.	Information gathering techniques Analytical technique Expert judgment Meetings Interviews Document analysis
To propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.	Information gathering techniques Analytical technique Expert judgment Document analysis
To develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.	Information gathering techniques Analytical technique Risk probability and impact assessment Risk categorization Risk urgency assessment Risk audit Risk reassessment
To create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.	Information gathering techniques Analytical technique Risk probability and impact assessment Risk categorization Risk urgency assessment Risk audit Risk reassessment

3.4 Assumptions and Constraints

An assumption is defined as a “factor in the planning process that is considered to be true, real, or certain, without proof or demonstration” (Project Management Institute, 2013). A constraint is defined as a “limiting factor that affects the execution of a project, program, portfolio, or process.” (Project Management Institute, 2013).

Chart 14 lists the various assumptions that have been made and constraints that have been identified for this project.

Chart 14 Assumptions and Constraints applied to the objectives of the project.

Objectives	Assumptions	Constraints
To assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.	Organizations and individuals will be will willing to participate in surveys, interview and other forms of information gathering. Documentation will be readily available to carry out research. Cyber security standard and norms will be cost effective.	Scope, or how in-depth research can go, is limited by time. Information quality from organizations with poorly developed infrastructure and policy will be poor and may not be useful.
To propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.	There will be no issues in using or merging existing frameworks. It will be possible to create a methodology that will be applicable to various organization sizes. There will be no significant cost associated with the creation of the methodology	Scope, or how detailed the methodology will be, is limited by time.
To develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.	It will be possible to create tools, templates and techniques that are sufficiently generalized to function with the methodology is various scenarios. It will be possible to create tools, templates and techniques that are serve to complement the proposed methodology.	Scope, or how much and how detailed the templates, tools and techniques will be, is limited by time.
To create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.	Sufficient information will be available through various information sources in order to carry out this objective. Key staff members will be available to offer information about the implementation.	Scope, or how effectively the implementation is carried out, and how detailed the assessment will be, is limited by time. Available tools and software will be sufficient to carry out assessment.

3.5 Deliverables

A deliverable is defined as “any unique and verifiable product, result, or capability to perform a service that is required to be produced to complete a process, phase, or project” (Project Management Institute, 2013). The main deliverable of this project is a proposed project management methodology for cyber security assessments.

Chart 15 lists the various components or deliverables of the overall methodology in more detail.

Chart 15 Objectives and corresponding Deliverables of the project.

Objectives	Deliverables
To assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.	An assessment of the current state of information and communications technology infrastructure in the country and region. A survey report gives guidance in the design of proposed project management methodology for cyber security assessments.
To propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.	A project management methodology for cyber security assessments based on current cyber security guidelines and frameworks.
To develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.	Templates, tools and techniques necessary to be utilized in future projects related to the proposed project management methodology.
To create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.	An implementation plan guide for the propose project management methodology.

4. RESULTS

The results of this project is divided into three parts: the gathering of information and research on the current state of the art of both cyber security and project management, the formulation of the proposed assessment methodology (which doubles as an implementation guide), and the subsequent implementation of the methodology in a real-life scenario.

4.1 Research and Survey

It was necessary to research on the state of the art of cyber security and project management in order to determine what was the best way forward in putting the assessment methodology together. Apart from studying key literature on the topic, informal interviews were done with key actors in the IT industry in Belize.

The information gathered about project management methodologies and cyber security standards and the subsequent selection of these was complemented by a survey that was done at various organizations in-country. The purpose of the survey was essentially to determine the knowledge, attitudes and practices of organizations in the country of Belize in terms of cyber security. A detailed report of the survey entitled *Cyber Security Survey Report* has been produced (see Appendix 6, pp. XIII).

Of the 20 organizations that were polled, 15 responded while 5 organizations did not respond for various reasons. Some of the most notable results from the survey are outlined as follows:

In terms of security profile of the organizations surveyed:

1. Most were relatively large, about 60% of them had 200 employees or more.
2. Most of them identified themselves as financial institutions or as ‘other’ base on the options available.

3. Over 60% have suffered some form of cyber security attack or breach over the last 12 months.
4. A majority (60%) have an IT department of 5 people or less.

In terms of information security maturity of the organizations surveyed:

1. A majority (60%) thought they were at least sufficiently secure.
2. Over half (50%) had a business continuity plan as a policy.
3. Only about a quarter (25%) have a department dedicate to information security.
4. Most found out about information security attacks from either their clients or from publications.

In terms of information security measures taken the organizations surveyed:

1. Most attempts at breaching security appear to be email viruses or malware.
2. The most popular information security measures appear to be the implementation of antivirus and firewalls.
3. The most used cyber security solutions were commercial products.

In terms of information security awareness of the organizations surveyed:

1. Most (60%) felt that security awareness should be base on job role and function.
2. Most thought it was either somewhat difficult or very difficult to convince management to invest in security spending.

In terms of third party control by the organizations surveyed:

1. About a third (30%) either helped identified risks related to third parties as part of their function or addressed information security issues in contracts.

2. Most organizations do not share information on information security attacks with third parties.

The survey demonstrated that there are various levels of preparedness in the country when it came to cyber security and that there is no unified or common approach to address this issue and in some cases, implementation of security measures are lacking or nonexistent. Furthermore, it appears that there are limited resources available to implement the necessary measures that are required to acquire a reasonably good response.

4.2 Proposed Assessment Methodology

The proposed assessment methodology itself was based in merging of two well-recognized reference standards, one in project management and the other in cyber security. The selection of these references was based the research and the survey done and on cost and ease of implementation. The following two subsections gives the rationale behind the selection of both the reference project management methodology and the cyber security standard used.

4.2.1 Rationale for the Selection of Reference Project Management Methodology

There are various types and variations of project management methodologies presently in existence, each with various levels of completeness and designed for various environments and purposes.

The reference project management methodology that was selected to be used as the basis for the design of the project management methodology for cyber security assessment is *The Standard for Project Management of a Project* that is included in and is further developed in *A Guide to the Project Management Book of Knowledge* (Project Management Institute, 2013).

The rational for the use of this methodology is as follows:

1. The author is most familiar with this methodology. Furthermore, various parts of the methodology have been applied by the author to some degree or the other in Ministry of Health projects over the past few years.

2. Due to the completeness of the methodology, the knowledgebase of the Project Management Institute and the broad variety of available documents and references, it can easily be adapted to almost any project management scenario or need. For example, the ten knowledge areas can be used as needed for any kind of project – the project manager or designer can choose to remove or add processes and techniques as required.

4.2.2 Rationale for the Selection of Reference Cyber Security Standard

Based on information gathered from the survey, interviews with various technical experts and with individuals involved in the field of information and communications technology in the country of Belize as well as the author’s knowledge, it was determined that the most adequate cyber security standard to use is the *Framework for Improving Critical Infrastructure Cybersecurity* from NIST; it is notable this is a compendium of standards and not a single standard by itself. The rationale for the selection of this framework as a reference for the creation of a cyber security assessment methodology is as follows:

1. It is easy to implement and can be adopted to fit the requirements of organizations of various sizes and types.

2. It references other well-know standards that are presently being used and is a living document as it is widely used and frequently updated.

3. It easily available and free of cost to use.

4. Its principal objective is to reduce cyber security risk, including prevention or mitigation of cyber-attacks using a complete approach at all levels of the organization.

4.2.3 Breakdown of Proposed Assessment Methodology

The proposed methodology was written in a step-by-step format. Essentially, it was written in such a way that can be also used as an implementation plan guide covering two of the specific objectives of this work in one document. The document is called the *Proposed Cyber Security Assessment Methodology* (see Appendix 7, pp. XXIV) and is divided in to the following sections:

1. The *Introduction* contains background information about the methodology as well as the justification and the intended audience (see Appendix 7, pp. XXXII-XXXIII).

2. The *Description of the Methodology* contains information about how the methodology is formulated, its various components, how to use it, and where to get additional information to supplement its usage (see Appendix 7, pp. XXXIII-XXXIX).

3. The *Initiating Phase* defines what steps need to be taken to develop the project idea in order to get initial support (see Appendix 7, pp. XXXIX-XL).

4. The *Planning Phase* develops the assessment plan in detail in order to ensure that the assessment is carried out successfully (see Appendix 7, pp. XL-XLVI).

5. The *Executing and Controlling Phase* describes how the assessment plan will be put into action and the necessary steps to ensure that it is successfully completed (see Appendix 7, pp. XLVI-L).

6. The *Closing Phase* describes the actions and processes necessary to complete the project (see Appendix 7, pp. L-LIII).

A notable point is that the *Cyber Security Assessment Methodology* is modeled from the standard project management life cycle; this provides for a methodical way or a step-by-step guide to carry out cyber security assessments. It is also sufficiently generalized so that it can be used under various scenarios and environments.

4.2.4 Templates, Tools and Techniques

The proposed *Cyber Security Assessment Methodology* also includes various templates, tools and techniques that serve to complement it and provide more insight and information on its usage; these are referenced and are included in the appendices of the methodology itself and are listed as follows in the order:

- *Assessment Charter Template* (see Appendix 7, pp. LIII-LV)
- *Business Case Template* (see Appendix 7, pp. LVI-LVIII)
- *Basic Cyber Security Survey* (see Appendix 7, pp. LIX-LXVI)
- *Initial Cyber Security Assessment Report Template* (see Appendix 7, pp. LXVII-LXXIII)
- *Statement of Work Template* (see Appendix 7, pp. LXXIV-LXXXI)
- *Assessment Management Plan Template* (see Appendix 7, pp. LXXXII-XC)
- *Information and Communications Technology Inventory Control Template* (See Appendix 7, pp. XCI-XCVII)
- *Cyber Security Risk Analysis Template* (see Appendix 7, pp. XCVIII-CX)
- *Cyber Security Master Profile* (see Appendix 7, pp. CXI-CVVIV)
- *Final Assessment Report Template* (see Appendix 7, pp. CXXV-CXXX)
- *Assessment Closure Document Template* (see Appendix 7, pp. CXXXI-CXXXVII)
- *Archive Listing Document Template* (see Appendix 7, pp. CXXXVII-CXLIV)

Apart from the templates, tools and techniques provided, the proposed methodology does not go much into detail except for risk analysis, which is the basis of cyber security. This is because the *Framework for Improving Critical Infrastructure Cybersecurity* from NIST and *A Guide to the Project Management Book of Knowledge* from the PMI are defined as main reference documents and should be referred to as needed. Furthermore, it is expected that the project team and the project manager (or lead assessor) are knowledgeable about both project management and cyber security and are able to adopt and implement various other templates, tools and technique on a case-by-case basis in order to successfully initiate, plan, execute and control, and close an assessment.

4.3 Implementation of Proposed Assessment Methodology

The final part this work was the implementation of the proposed *Cyber Security Assessment Methodology* in a real project scenario primarily to determine if it is practical as well to determine its functionality and potential flaws that could then be studied to improve it.

The proposed methodology was applied to an assessment carried out at the National Engineering and Maintenance Center of the Ministry of Health, Belize. The full result of the assessment entitled *Cyber Security Assessment of NEMC* is included (see Appendix 8, pp. CXLV).

The assessment was carried out successfully within the required timeframe. It had a minimal cost since it was done in-house. In terms of scope, the assessment primarily covered the National Engineering and Maintenance Center of the Ministry of Health.

The two main deliverables of the assessment are listed as follows:

- The *Initial Cyber Security Assessment Report* (see Appendix 8, pp. CLXVIII-CLXXVI)

- The *Final Assessment Report* (see Appendix 8, pp. CXLVI-CLII) that included the *Information and Communications Technology Inventory Control* (see Appendix 8, pp. CCI-CCVII), the *Cyber Security Profile* (see Appendix 8, pp. CCVIII-CCXVII) and the *Cyber Security Risk Analysis* (see Appendix 8, pp. CCVIII-CCXXXI)

Other documents that were a part of the assessment are listed as follows:

- *Assessment Charter* (see Appendix 8, pp. CLIII-CLVI)
- *Business Case* (see Appendix 8, pp. CLVII-CLVIII)
- *Basic Cyber Security Survey* (see Appendix 8, pp. CLX-CLXVII)
- *Statement of Work* (see Appendix 8, pp. CLXXVII-CLXXXV)
- *Assessment Management Plan* (see Appendix 8, pp. CLXXXVI-CC)
- *Assessment Closure Document* (see Appendix 8, pp. CCXXXI-CCXXXVIII)
- *Archive Listing Document* (see Appendix 8, pp. CCXXXIX-CCXLIV)

The results of the assessment demonstrated that the National Engineering and Maintenance Center has a very poor stance with regards to cyber security in all five functional areas of the *NIST Cybersecurity Framework*: these are the Identify, Protect, Detect, Respond and Recover functions. The assessment also proposed a new security profile for the unit and then gave suggestions and advice on how to fill these security gaps through the risk analysis that was done. Getting these results helped to demonstrate that the proposed methodology was effective and useful in carrying out the assessment.

5. CONCLUSION

The general objective of this Final Graduation Project was to develop a project management methodology for cyber security assessments based on existing information and communications technology infrastructure in order to assess the cyber security needs for organizations of various sizes. In order to achieve the general objective, various specific objectives were formulated:

1. As put forth by the first specific objective, it was necessary to assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.

   This first objective was achieve by means of gathering data using various research methods, including a cyber security survey, interviews, as well as the author's knowledge of project management and information technology.

2. The second specific objective was to propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.

   Bases on the information gathered by achieving the first specific objective, this was achieved by proposing and developing a tailored cyber security assessment methodology base on the *Project Management Body of Knowledge* and the *Cybersecurity Framework* offered by PMI and NIST, respectively.

3. The third specific objective was to develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.

   This objective was achieved by creating and incorporating templates, tools and techniques into the proposed methodology in order to create a more complete final product that was consistent with present practices in project management and in line the cyber security framework chosen as the reference standard.

4. The fourth specific objective was to create an implementation guide for the use of the proposed project management methodology in order to effectively implement the methodology along with the various associated templates, tools and techniques.

   This objective was achieved by formulating the proposed methodology (the second specific objective) in accordance with the Project Management Life Cycle and by incorporating a flowchart and the necessary tools to carry out the assessment for most cases. By designing the methodology in an instructive, sequential manner, and providing sufficient templates, tools and techniques, it became redundant to create a separate guide for implementation.

The *Cyber Security Assessment Methodology* was implemented in a practical application and was overall successful. However due to time constraints, it was difficult to perform the assessment with a very high level of detail. Furthermore, the dynamics of performing an assessment internally is different than having it done by an external service provider. Nonetheless, the information that was obtained from the assessment was useful and the assessment helped to shed light on the proposed methodology and the underlying technical references. During the assessment, some adjustments and improvements were made to the methodology's documentation based on practical lessons learnt.

The final product, which is the methodology and accompanying supporting documents, complied with all the objectives set forth at the beginning of the project. It is expected that the methodology will be further developed and implemented in the country of Belize in the future.

6. RECOMMENDATIONS

The following are a listing of perceived limitations of this project and some key recommendations:

1. One of the main limitations of this work is the restricted time that was available to develop and implement the methodology; because of this, some of the reports and elements of the project may appear to lack in-depth information, especially in the implementation of the assessment.
2. One of the key limitations of this work is that it was not widely tested in order to verify the effectiveness of the methodology that was developed. It is recommended that the methodology along with the supporting documents be implemented in various scenarios in order to determine how well it works and to continue to make adjustments as necessary.
3. Due to the fact that the methodology was designed to generally meet the needs of organizations of different types, sizes and functions, some areas were intentionally left without in-depth analysis and development; this is to allow for more flexible implementation. The main disadvantage of this is that it may not be very useful to implementers who are not very knowledgeable about cyber security or project management.
4. When carrying out the interviews and surveys, it was noted that many people were unaware of cyber-threats and how it affected them, or provided conflicting information. This was both at the level of the individual in their private lives as well as at the organizational level. More can be done to order to increase awareness and promote cyber security.
5. As the methodology document matures, it may be necessary to add to the available templates, tools and techniques or to upgrade them as needed. In some cases, it may be necessary to use other templates, tools and techniques. It is up the implementer to decide what to use.
6. In terms of the survey that was carried out, a bigger and better distributed sampling size could have been obtained to gather more accurate results, however given the time and resources required, it was not practical to do so.

7. As technology evolves, it is important that the methodology that was developed be updated to reflect these changes. The main document and related documents must be updated regularly in order to remain relevant.
8. It is important to note that the merging of a completely different project management methodology with a different cyber security norm, standard or framework is possible and can achieve similar results; there is by no means a singular way to approach the problem.
9. Cyber security assessments are only the first step in developing and implementing a complete cyber security strategy; this work does not represent a complete approach or solution to all the problems of cyber security in any given organization.

BIBLIOGRAPHY

Alexander, M. (2018, March 1). *Agile project management: A comprehensive guide*. Retrieved from CIO.com - Tech News, Analysis, Blogs, Videos: https://www.cio.com/article/3156998/agile-development/agile-project-management-a-beginners-guide.html

European Telecommunications Standards Institute. (2008, May 12). *ETSI*. Retrieved from Cyber security: http://www.etsi.org/technologies-clusters/technologies/cyber-security

Graves, A. (2012, October 19). *What is Six Sigma?* Retrieved from Six Sigma Daily: http://www.sixsigmadaily.com/what-is-six-sigma/

Icasas, P. (2014, March 25). *Project Management 101: What is PERT?* Retrieved from Easy Projects: https://explore.easyprojects.net/blog/project-management-101-pert

Information Security Forum. (2008, May 12). *The ISF Standard of Good Practice for Information Security*. Retrieved from Information Security Forum: https://www.securityforum.org/tool/the-isf-standardrmation-security/

International Standards Organization. (2018, May 12). *ISO/IEC 27001 Information security management*. Retrieved from ISO - International Organization for Standardization: https://www.iso.org/isoiec-27001-information-security.html

Isect Ltd. (2018, May 12). *ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls (second edition)*. Retrieved from ISO/IEC 27002 code of practice: http://www.iso27001security.com/html/27002.html

Littlefield, A. (2016, September 2). *The Beginner's Guide To Scrum And Agile Project Management*. Retrieved from Trello: https://blog.trello.com/beginners-guide-scrum-and-agile-project-management

Merriam-Webster. (2018, May 12). *Research* | *Definition of Research by Merriam-Webster*. Retrieved from Dictionary by Merriam-Webster: https://www.merriam-webster.com/dictionary/research

Mrsic, M. (2017, July 5). *Adaptive Project Management*. Retrieved from ActiveCollab: https://activecollab.com/blog/project-management/adaptive-project-management

Mrsic, M. (2017, June 28). *Critical Chain Project Management*. Retrieved from Active Collab: https://activecollab.com/blog/project-management/critical-chain-project-management-ccpm

Mrsic, M. (2017, May 17). *Traditonal Project Management*. Retrieved from ActiveCollab: https://activecollab.com/blog/project-management/traditional-project-management

National Institute of Standards and Technology. (2018, May 12). *Framework for Improving Critical Cybersecurity Infrastructure Version 1.1*. Retrieved from Cybersecurity Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Organization of American States. (2014, June 14). Latin American+Caribbean Cyber Security Trends. Washington, District of Columbia, Unites States of America.

Powell-Morse, A. (2016, December 8). *Airbrake*. Retrieved from Waterfall Model: What It Is and When Should You Use It?: https://airbrake.io/blog/sdlc/waterfall-model

Project Management Institute. (2013). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) Fifth Edition.* Pennsylvania: Project Management Institute, Inc.

Ray, S. (2018, January 3). *Understanding Critical Path in Project Management*. Retrieved from Project Manager: https://www.projectmanager.com/blog/understanding-critical-path-project-management

UK Government. (2018, January 16). *Cyber Essentials Scheme: overview* . Retrieved from GOV.UK: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Yale University Library Research Guides. (2017, December 20). *Primary, secondary & tertiary sources - Comparative Literature - Yale University Library Guides at Yale Univeristy*. Retrieved from Yale University Library: https://guides.library.yale.edu/c.php?g=295913&p=1975839

APPENDICES

Appendix 1: Final Graduation Project – Project Charter

PROJECT CHARTER **Formalizes the project start and confers the project manager with the authority to assign company resources to the project activities. Benefits: it provides a clear start and well-defined project boundaries.**	
Date	**Project Name**
November 13, 2017	Development of a Project Management Methodology for Cyber Security Assessments of Information and Communications Technology Infrastructure
Knowledge Areas / Processes	**Application Area (Sector / Activity)**
Knowledge areas: Project Integration Management, Project Scope Management, Project Time Management, Project Cost Management, Project Quality Management, Project Human Resource Management, Project Communications Management, Project Risk Management, Project Procurement Management and Project Stakeholders Management. **Process groups:** Initiating, Planning, Executing, Monitoring & Controlling, Closing	Project Management Information and Communications Technology Cyber Security
Start Date	**Finish Date**
20th of August, 2018	26th November, 2018

Project Objectives (General and Specific)

General Objective:

To develop a project management methodology for cyber security assessments based on existing information and communications technology infrastructure in order to assess the cyber security needs for organizations of various sizes.

Specific Objectives:

1. To assess the current state of information and communications technology infrastructure and services as well as current cyber security guidelines and frameworks in order to determine the main components for the project management methodology for cyber security assessments.
2. To propose and develop a project management methodology for cyber security assessments based on current cyber security guidelines and frameworks in order to carry out assessments to organization of various sizes.
3. To develop project management templates, tools and techniques to be utilized in future projects related to the proposed project management methodology in order to easily implement assessments.
4. To create an implementation guide for the use of the proposed project management methodology in order to

effectively implement the methodology along with the various associated templates, tools and techniques.

Project Purpose or Justification (Merit and Expected Results)

In the recent years, the importance of cyber security has become more and more apparent. Governments in various countries have invested large amounts of resources in order to keep up with cyber-threats and to protect critical national infrastructure. In the private sector, the same has happened as organizations have had to quickly embrace new technologies that are not designed with security in mind. Unfortunately, Belize and the broader Caribbean have been slow in keeping up, and even though steps are being taken in the right direction, there is much more that can be done to promote and implement better cyber security measures.

In a similar manner, project management has increased in importance over the years and has become an integral part of most organizations. Corrective actions and improvements to existing business processes and infrastructure are normally handled as projects as organizations have come to understand and accept the benefits of using the project management approach to solve some of the bigger problems and tasks that they have, or to improve their business processes.

This project attempts to address the issue of the lack of proper cyber security measures in organizations of various types and sizes by providing a generalized methodology to carry out cyber security assessments based on current project management practices. It is designed to be applicable in the context of the local and near-future information and communications technology infrastructure in Belize but can be applicable in the broader Caribbean as well.

Description of Product or Service to be generated by the Project – Project Final Deliverables

1. Documentation of current guidelines for cyber security.
2. A proposal for project management methodology developed to fit current cyber security guidelines.
3. Templates, tools and techniques to support developed project management methodology.
4. Documentation guidelines for implementation of the propose project management methodology.

Assumptions

The primary assumption is that organizations will be willing to share information related to their present and past cyber security postures, real and perceived cyber-threats and incidents as well as information about their information and communications technology infrastructure.

Since this is a new endeavor, the estimated time of completion is difficult to determine with a high degree of accuracy and therefore it may be possible that the deliverables may be delayed, incomplete or may not be thoroughly tested.

Constraints

Cost: there may hidden costs, such as the purchase of documentation related to standards.
Human Resources: There will be only one person working on the project.
Time: The project should be completed in four work months, taking into consideration holidays and other obligations.
Quality: The project should a high level of quality to be used as a reference or practical guide in the future.
Confidentiality: Most of the on-the-ground information gathered may have to be confidential in nature; some organizations may be unwilling to reveal certain information.

Preliminary Risks

If the author of the project cannot complete the work required, the project will fail.

If supervision and guidance is not readily available and timely, it may cause delays in the project.

If the information related with quality required is not obtained, it may lower the quality of the project or cause it to be delayed.

Budget

The costs of this project will be the purchase of documentation related to standards, norms, guidelines and frameworks as well as software that are needed to complete the objectives. These costs cannot be determined at the moment until after preliminary research is done.

Since it is a project management methodology is being developed and not a project, costs are not expected to be influential.

Milestones and Dates

Milestones	Start Date	End Date
Submission of Project Charter, Initial Chapters of FGP & Schedule	20th of August, 2018	20th of August, 2018
Submission of Completed Methodology	10th of September, 2018	10th of September, 2018
Submission of Case Study applying Methodology	1st October, 2018	1st October, 2018
Submission of FGP for Approval by Tutor	21st October, 2018	21st October, 2018
Review of FGP	23rd October, 2018	6th November, 2018
Adjustments to FGP	5th November, 2018	9th November, 2018
Presentation to the Board of Examiners	11th November, 2018	16th November, 2018

Relevant Historical Information

The main objective of this project is the formulation of a project management methodology that is applicable to various use cases. To the best of knowledge of the author, there are no similar efforts being carried out at the moment in Belize.

There have been various cyber-attacks that have been documented on local media. There have also been various other incidents that were not reported officially. As these issues become more and more relevant, there will be an urgent need to address them quickly and efficiently, hence the need to lay the groundwork to be able to assess and address potential cyber-threats.

Recently, the first national cyber security symposium took place and had the participation from various stakeholders from both the public and private sectors (more information can be found at https://cybersecurity.nigf.bz/).

Stakeholders

Direct Stakeholders: Final Graduation Project Tutor**,** Final Graduation Project Author. **Indirect Stakeholders:** Potential users of the methodology (all organizations or business, in both the public and private sector).

Project Manager: Douglas Michael Oliver Westby	**Signature:**
Authorized by:	**Signature:**

Appendix 2: Final Graduation Project – Work Breakdown Structure

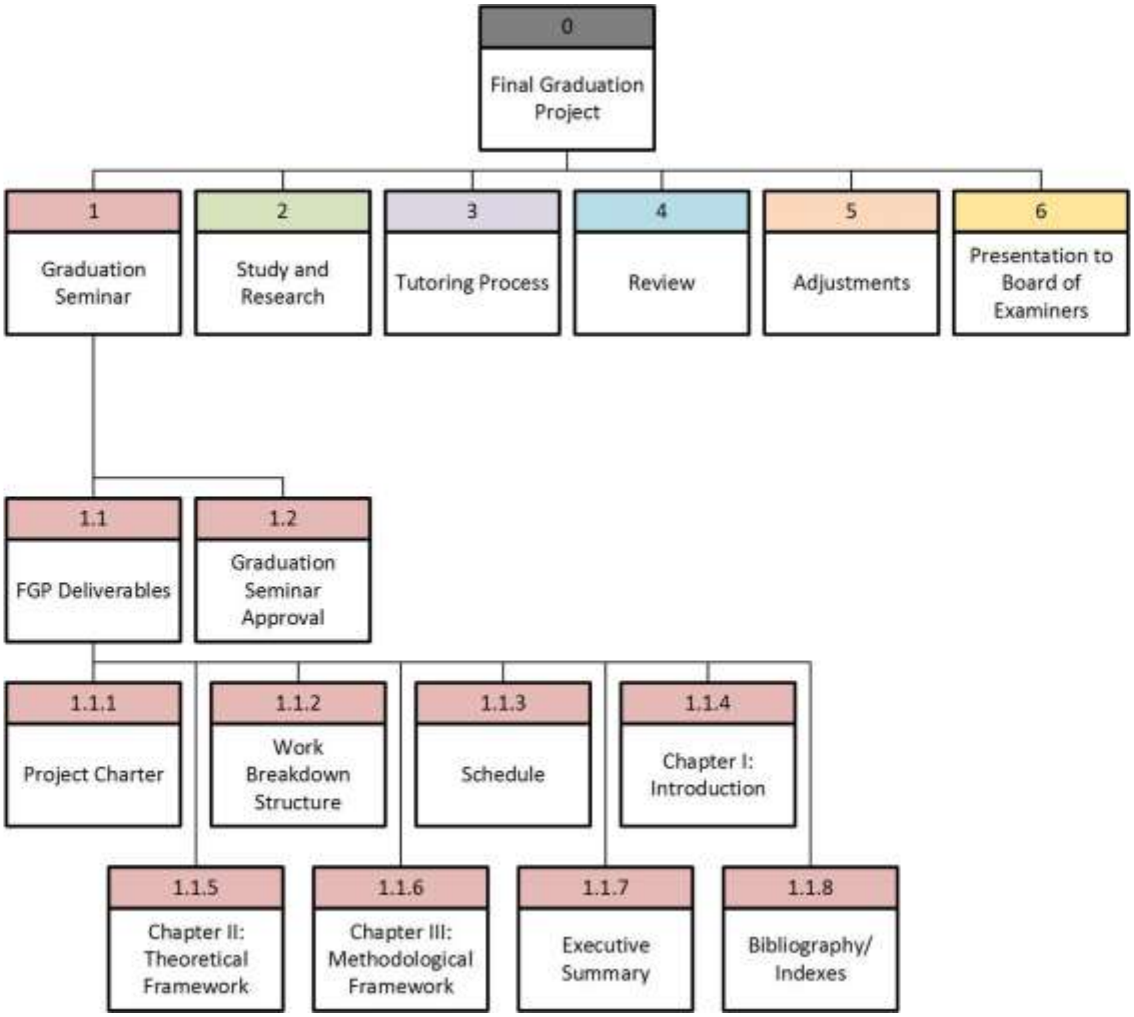


Figure 1 First level of WBS and complete breakdown of Package 1: Graduation Seminar.

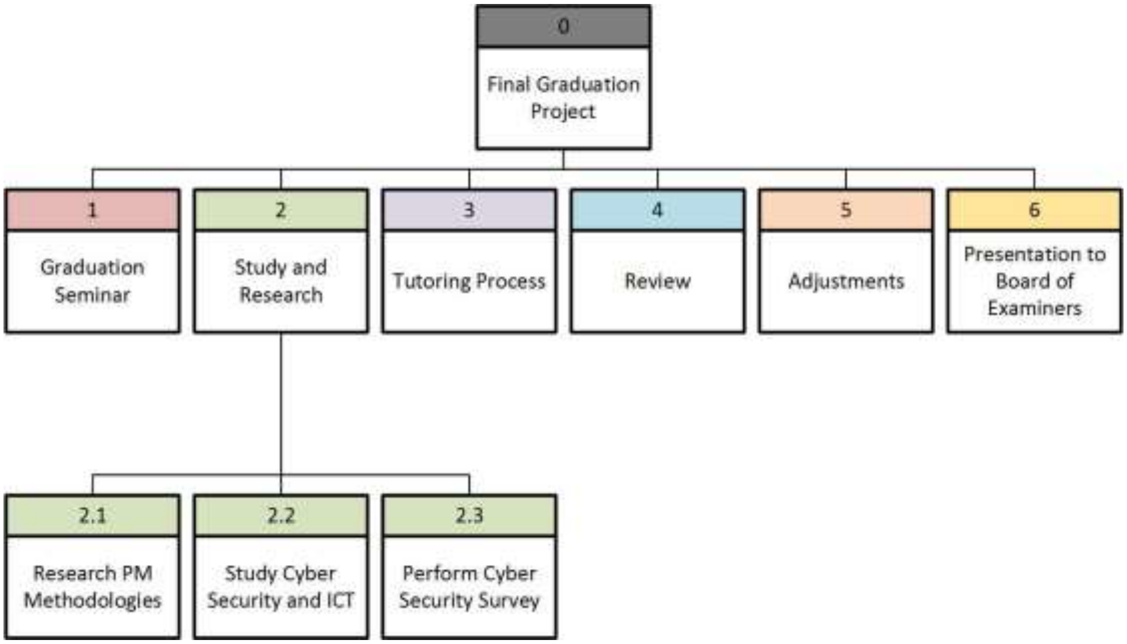

0
Final Graduation Project
1
Graduation Seminar
2
Study and Research
3
Tutoring Process
4
Review
5
Adjustments
6
Presentation to Board of Examiners
2.1
Research PM Methodologies
2.2
Study Cyber Security and ICT
2.3
Perform Cyber Security Survey

Figure 2 First level of WBS and complete breakdown of Package 2: Study and Research.

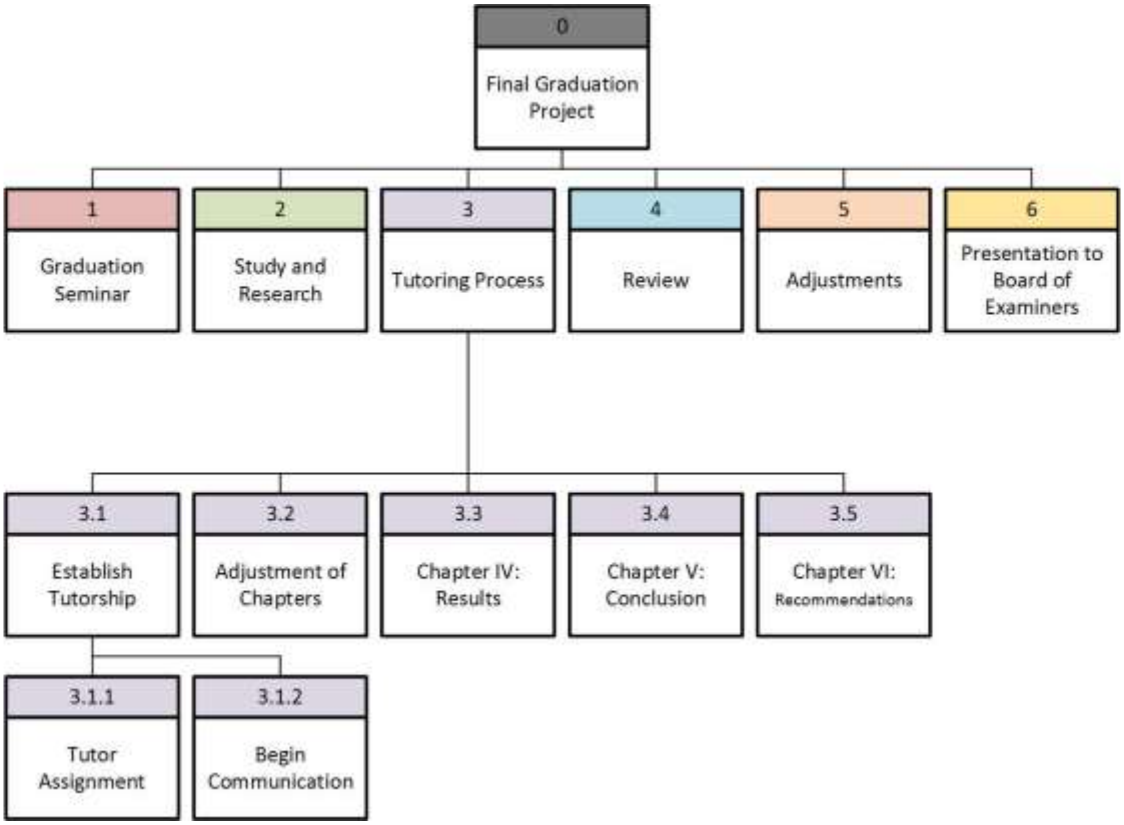


Figure 3 First level of WBS and complete breakdown of Package 3: Tutoring Process.

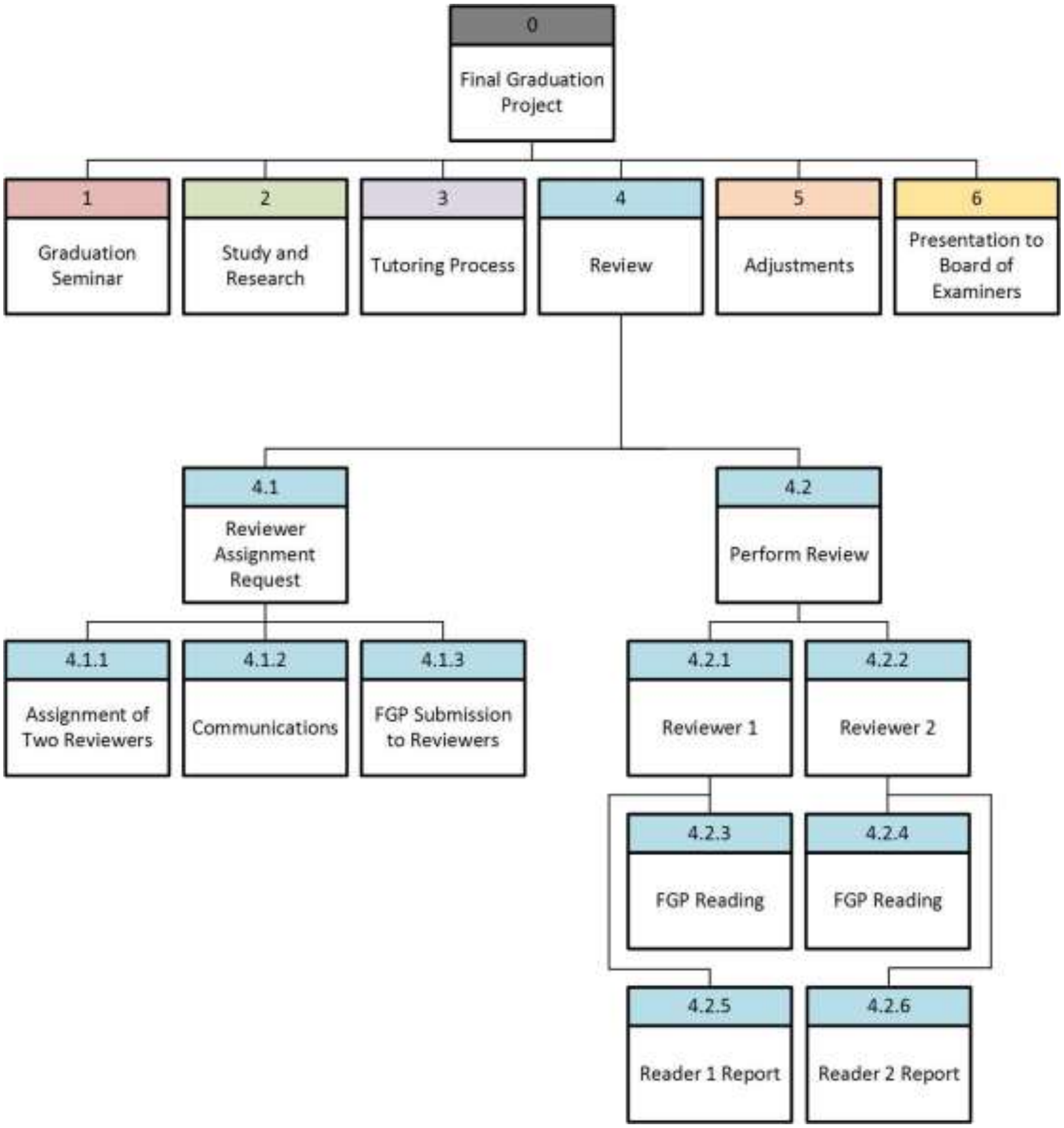


Figure 4 First level of WBS and complete breakdown of 4: Review.

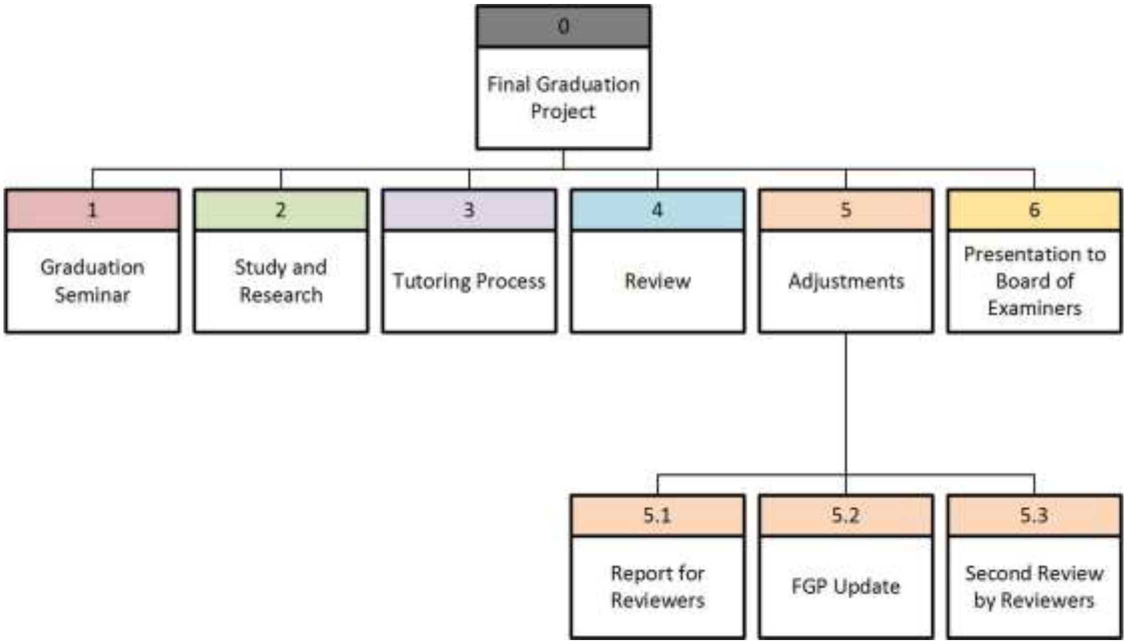


Figure 5 First level of WBS and complete breakdown of Package 5: Adjustments.

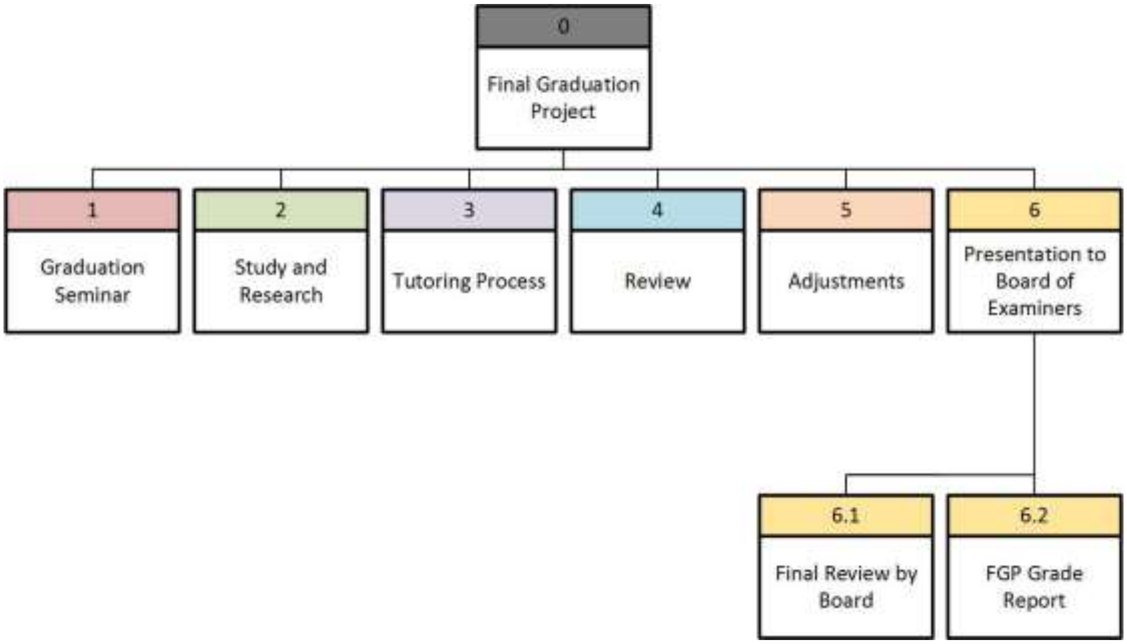


Figure 6 First level of WBS and complete breakdown of Package 6: Presentation to Board of Examiners.

Appendix 3: Final Graduation Project – Schedule

Chart 1 Schedule of Graduation Seminar (WBS Package 1).

WBS	Task Name	Duration	Start	Finish	13. 11	20. 11	27. 11	04. 12	11. 12
1	Graduation Seminar	25 days	11/13/17	12/17/17					
1.1	FGP Deliverables	25 days	11/13/17	12/17/17					
1.1.1	Project Charter	6 days	11/13/17	11/19/17	🟦				
1.1.2	Work Breakdown Structure	6 days	11/13/17	11/19/17	🟦				
1.1.3	Schedule	6 days	11/20/17	11/26/17		🟦			
1.1.4	Chapter I: Introduction	6 days	11/20/17	11/26/17		🟦			
1.1.5	Chapter II: Theo. Framework	6 days	11/27/17	12/3/17			🟦		
1.1.6	Chapter III: Meth. Framework	6 days	12/4/17	12/10/17				🟦	
1.1.7	Executive Summary	6 days	12/11/17	12/17/17					🟦
1.1.8	Bibliography/Indexes	6 days	12/11/17	12/17/17					🟦
1.2	Graduation Seminar Approval	6 days	12/11/17	12/17/17					🟦
1.3	Complete Graduation Seminar	0 days	12/17/17	12/17/17					🟩

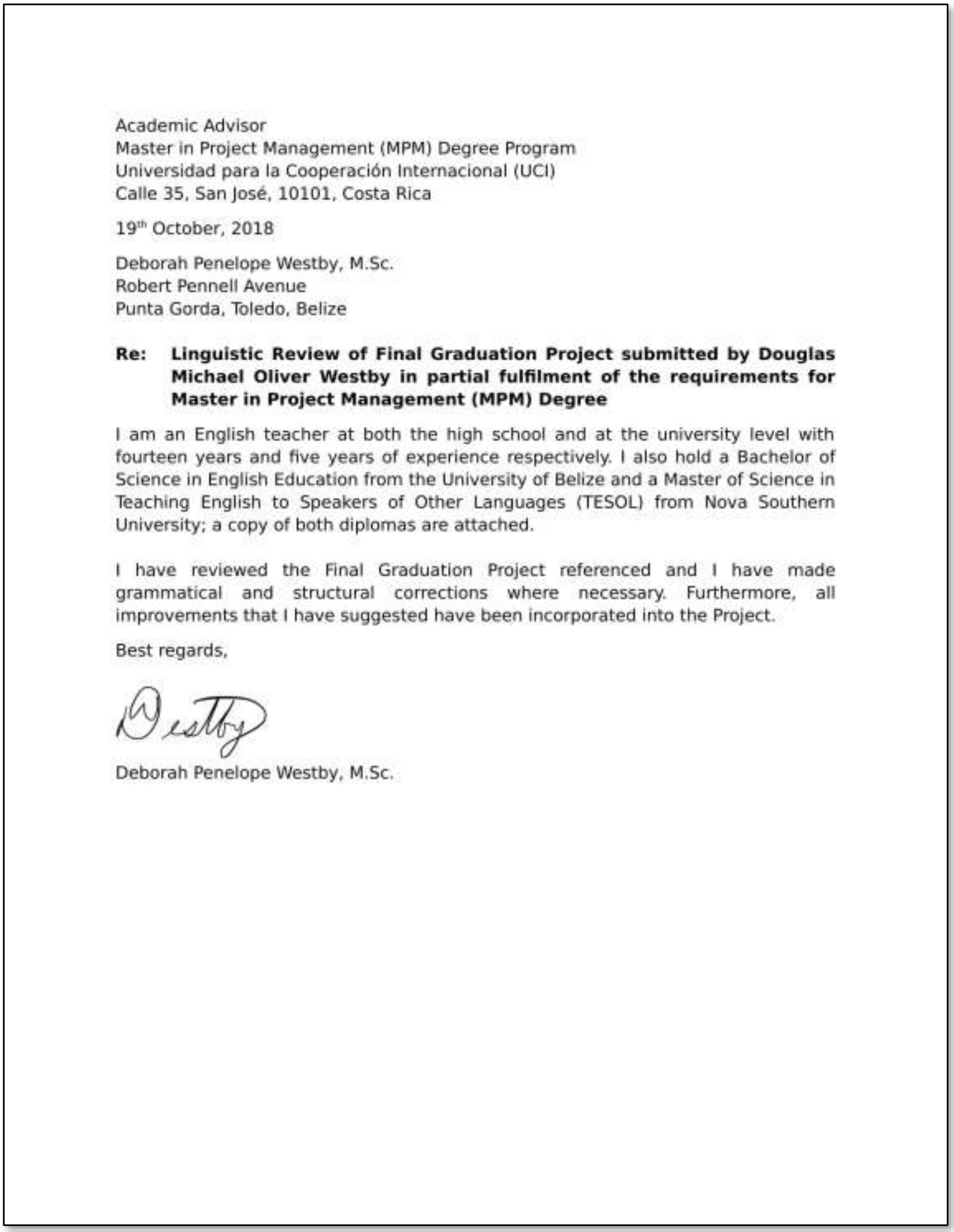
Chart 2 Schedule of Study and Research (WBS Package 2).

WBS	Task Name	Duration	Start	Finish	28. 05	04. 06	11. 06	11. 06	25. 06	02. 07	09. 07	16. 07	23. 07
2	Study and Research	133 days	1/24/18	7/27/18									
2.1	Research: PM Methodologies	45 days	1/24/18	3/27/18	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
2.2	Study Cyber Security and ICT	45 days	3/27/18	5/28/18	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
2.3	Perform Cyber Security Survey	45 days	5/28/18	7/27/18	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
2.4	Complete Study and Research	0 days	7/27/18	7/27/18									🟩

Chart 3 Schedule of Final Graduation Project (WBS Packages 3 to 6).

WBS	Task Name	Duration	Start	Finish	30. 07	06. 08	13. 08	20. 08	27. 08	03. 09	10. 09	17. 09	24. 09	01. 10	08. 10	15. 10	22. 10	29. 10	05. 11	12. 11
3	Tutoring Process	61 days	7/30/18	10/22/18																
3.1	Establish Tutorship	60 days	7/30/18	10/19/18	🟦															
3.2	Adjustments of Chapters	2 days	8/3/18	8/6/18		🟦														
3.3	Chapter IV: Results	45 days	8/9/18	10/10/18		🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦					
3.4	Chapter V: Conclusion	4 days	10/11/18	10/16/18												🟦				
3.5	Chapter VI: Recommendations	4 days	10/17/18	10/22/18													🟦			
3.6	Final Submission of FGP	0 days	10/22/18	10/22/18													🟩			
4	Review	11 days	10/23/18	11/6/18																
4.1	Review Assignment Request	3 days	10/23/18	10/25/18													🟦			
4.1.1	Assignment of Two Reviewers	1 day	10/23/18	10/23/18													🟦			
4.1.2	Communications	1 day	10/24/18	10/24/18													🟦			
4.1.3	FGP Submission to Reviewers	1 day	10/25/18	10/25/18													🟦			
4.2	Perform Review	8 days	10/26/18	11/6/18													🟦			
4.2.1	Reviewer 1	8 days	10/26/18	11/6/18													🟦			
4.2.1.1	FGP Reading	8 days	10/26/18	11/6/18													🟦			
4.2.1.2	Reader 1 Report	1 day	11/2/18	11/2/18														🟦		
4.2.2	Reviewer 2	8 days	10/26/18	11/6/18													🟦			
4.2.2.1	FGP Reading	8 days	10/26/18	11/6/18													🟦			
4.2.2.2	Reader 2 Report	1 day	11/2/18	11/2/18														🟦		
5	Adjustments	5 days	11/5/18	11/9/18																
5.1	Report for Reviewers	1 day	11/5/18	11/5/18															🟦	
5.2	FGP Update	4 days	11/6/18	11/9/18															🟦	
5.3	Second Review by Reviewers	2 days	11/8/18	11/9/18																
6	Presentation to Board of Examiners	5 days	11/12/18	11/16/18																🟦
6.1	Final Review by Board	5 days	11/12/18	11/16/18																🟦
6.2	FGP Grade Report	2 days	11/15/18	11/16/18																🟦
6.3	FGP Completed	0 days	11/16/18	11/16/18																🟩

Appendix 4: Proof of Philological Corrections



Academic Advisor
Master in Project Management (MPM) Degree Program
Universidad para la Cooperación Internacional (UCI)
Calle 35, San José, 10101, Costa Rica

19th October, 2018

Deborah Penelope Westby, M.Sc.
Robert Pennell Avenue
Punta Gorda, Toledo, Belize

Re: Linguistic Review of Final Graduation Project submitted by Douglas Michael Oliver Westby in partial fulfilment of the requirements for Master in Project Management (MPM) Degree

I am an English teacher at both the high school and at the university level with fourteen years and five years of experience respectively. I also hold a Bachelor of Science in English Education from the University of Belize and a Master of Science in Teaching English to Speakers of Other Languages (TESOL) from Nova Southern University; a copy of both diplomas are attached.

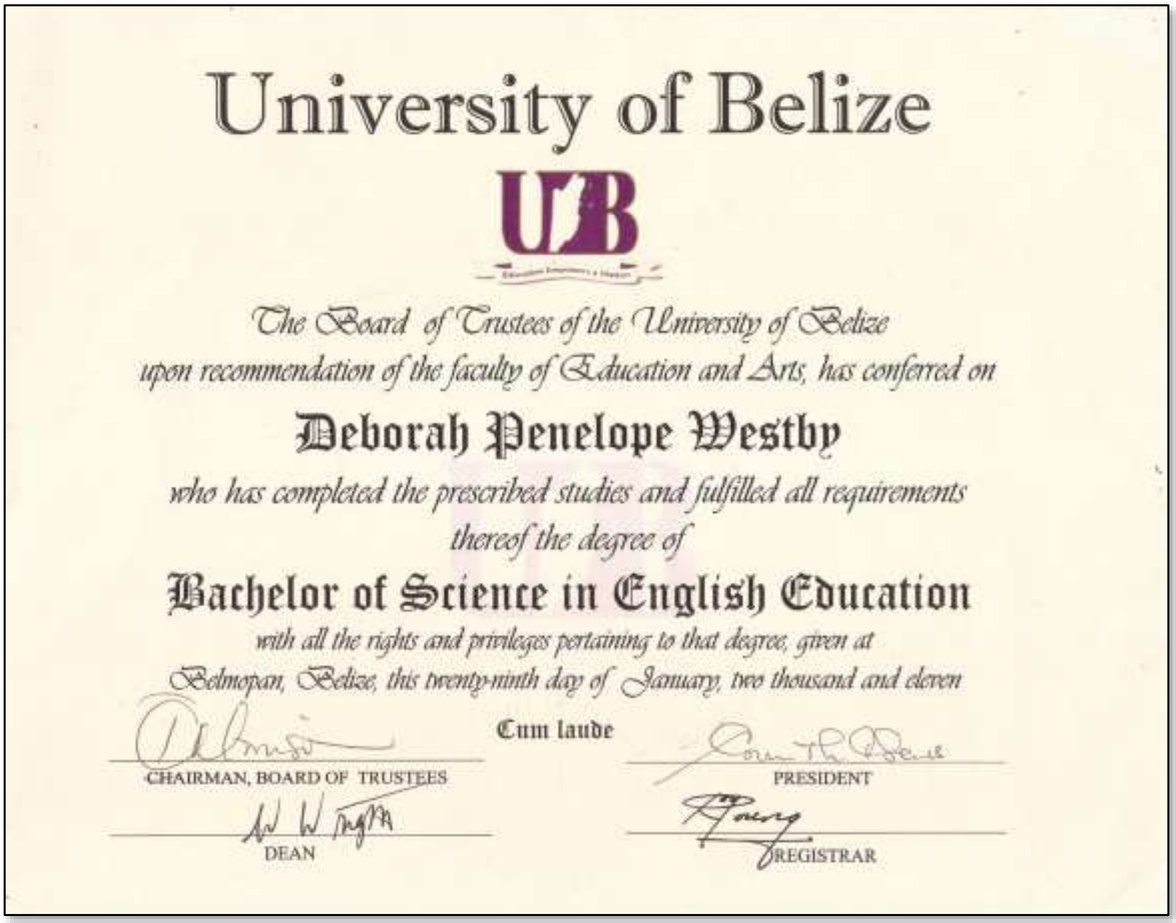
I have reviewed the Final Graduation Project referenced and I have made grammatical and structural corrections where necessary. Furthermore, all improvements that I have suggested have been incorporated into the Project.

Best regards,

Westby

Deborah Penelope Westby, M.Sc.

Appendix 5: Credentials of Linguist



University of Belize

UB

The Board of Trustees of the University of Belize
upon recommendation of the faculty of Education and Arts, has conferred on

Deborah Penelope Westby

who has completed the prescribed studies and fulfilled all requirements
thereof the degree of

Bachelor of Science in English Education

with all the rights and privileges pertaining to that degree, given at
Belmopan, Belize, this twenty-ninth day of January, two thousand and eleven

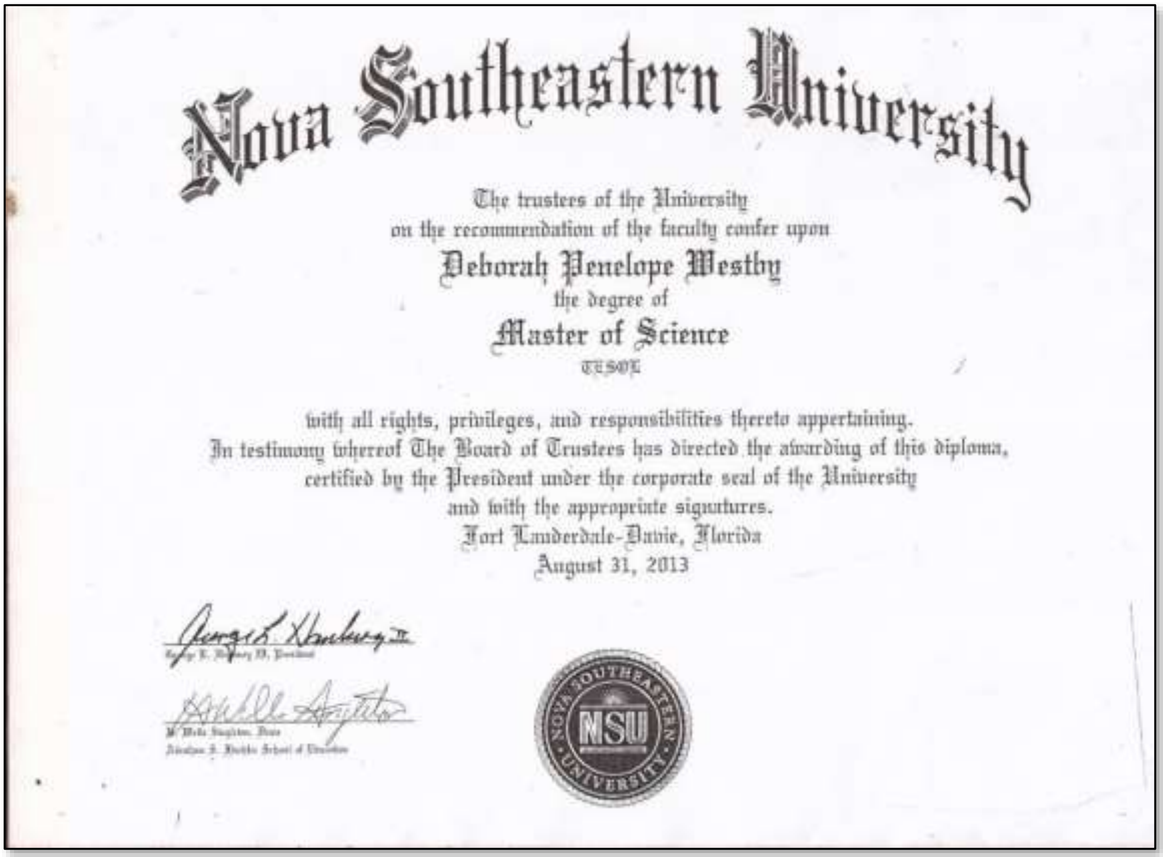
Cum laude

CHAIRMAN, BOARD OF TRUSTEES

PRESIDENT

DEAN

REGISTRAR



Nova Southeastern University

The trustees of the University
on the recommendation of the faculty confer upon
Deborah Penelope Westby
the degree of
Master of Science
TESOL

with all rights, privileges, and responsibilities thereto appertaining.
In testimony whereof The Board of Trustees has directed the awarding of this diploma,
certified by the President under the corporate seal of the University
and with the appropriate signatures.
Fort Lauderdale-Davie, Florida
August 31, 2013

George L. Hanbury II
George L. Hanbury II, President

H. Wells Singleton, Dean
Abraham S. Fischler School of Education

NOVA SOUTHEASTERN UNIVERSITY
NSU

APPENDIX 6: CYBER SECURITY SURVEY REPORT

Tabulated Results

Organizational Knowledge, Attitudes and Practices

Version 1.0 – 10/04/2018

Contact Information:
Douglas M. O. Westby, P. ENG.
Apt. No. 14. Ladyville Apartments
Ladyville, Belize District
Belize, Central America
Telephone: +501-610-6465
Email: douglas.westby@gmail.com

CONTENTS

ABOUT THIS REPORT .... *XV*
SECTION I: ORGANIZATIONAL INFORMATION SECURITY PROFILE .... *XVI*
SECTION II: INFORMATION SECURITY MATURITY .... *XVII*
SECTION III: INFORMATION SECURITY MEASURES .... *XX*
SECTION IV: INFORMATION SECURITY AWARENESS .... *XXI*
SECTION V: THIRD PARTY CONTROL .... *XXII*
SECTION VI: CONCLUSION .... *XXIII*

ABOUT THIS REPORT

This document contains the results of an *Information Security Survey* done in the month of April, 2018. This report is formatted in the same way the survey is laid out, and all the data gathered is presented in the same sections and in the same sequence.

The survey questions are based on already established cyber security surveys and lines of questioning, however it has been formatted and tailored to meet the perceived needs of on-the-ground organizations in Belize.

Representatives from twenty organizations were asked to participate. Results were recovered from fifteen organizations, five did not submit. The results are presented in the form of the tabulated data; zero percentages are not shown.

In general terms, the purpose of the survey was to gather information from people involved in information technology at various kinds and sizes of organizations in the country of Belize in order to determine the present level of knowledge, attitudes and practices towards information security at these organizations.

Specifically, the survey was comprised of a series of questions in six different subject areas related to information security and business functions. The questions were formulated to determine the size of the organization and its functions, the resources it has as it relate to information security, and the general attitude and overall posture of the organization in terms of information security.

The information will be used to assist in formulating a methodology to carry out information security assessments that are tailored to be cost effective and that can be implemented at organizations of various sizes, purposes and backgrounds.

SECTION I: ORGANIZATIONAL INFORMATION SECURITY PROFILE

1. What is the size of your organization?

Response	Tally
Less than 25 employees	2
25 to 50 employees	2
51 to 100 employees	1
101 to 200 employees	0
More than 200 employees	7

2. Your organization is primarily a part of which one of the following sectors or industry?

Response	Tally
Agriculture	0
Education	1
Energy	1
Finance	5
Government	2
Health	1
Imports/Exports	1
Manufacturing	0
Retail or Trade	0
Technology (including IT)	0
Telecommunications	1
Tourism and Hospitality	1
Transport and Logistics	2
Other	4

3. Have your organization suffered information security attacks or breaches in the last 12 months? (multiple answers possible)

Response	Tally
None	5
None, but weaknesses were highlighted during testing	3
Hacker attacks	1
Malware attacks	4
Loss of information/data assets	2
Loss of physical assets	0
Other	4

4. **How many people does your IT department employ?**

Response	Tally
1 to 2	6
3 to 5	3
6 to 10	0
11 to 15	0
More than 15	6

5. **Does your organization adhere to any information security frameworks and/or standards, and if so, which ones? (multiple answers possible)**

Response	Tally
Cyber Essentials (UK Government Standard)	0
ETSI TC CYBER	0
NIST Cybersecurity Framework	0
ISACA COBIT	1
ISF Standard of Good Practice for Information Security	0
ITIL (AXELOS/UK Government)	0
ISO/IEC 27000 family of standards	7
National or local regulatory standards	2
Parent organization or internal standards	6
We do not adhere to any standards	2
Other	1

SECTION II: INFORMATION SECURITY MATURITY

1. **How secure do you think your organization’s information technology network and resources are?**

Response	Tally
Highly secure	3
Sufficiently secure	6
Secure to a certain extent	5
Not Secure	0
Information not available	1

2. Which of the following policies or procedures has your organization documented and approved? (multiple answers possible)

Response	Tally
Information security governance structure	5
Business continuity plans	8
Information security roadmap	2
Cyber incident response plans	6
Information security strategy	6
Policies and procedures will be developed over the next 12 months	5
Nothing has been developed	2
Other	4

3. Does your organization have a dedicated department responsible for information security?

Response	Tally
Yes, we have a dedicated department/division	4
Yes, but it is a part of another department	3
No	8

4. To who do your organization's information security executives or personnel report?

Response	Tally
Board (Board of Directors)	3
Chief Executive Officer (CEO)	5
Chief Financial Officer (CFO)	0
Other	4

5. What has raised your awareness of information security attacks? (multiple answers possible)

Response	Tally
Clients of our organization were attacked	8
The infrastructure of our organization was under attack	3
Legal and/or regulatory requirements	4
Publications in magazines, on websites and mailing lists	8
Presentations and discussions at conferences	4
On the news or social media	6
Other	1

6. **How do you keep informed of new forms of information security attacks and threats? (multiple answers possible)**

Response	Tally
Mailing lists	6
Security conferences	6
News on websites and blogs from professional associations	11
Social networks	6
Service providers	5
Scientific publications	1
Consulting firms/external consulting	1
To date, there is no way our organization can trace cybercrime promptly	2
Other	1

7. **Which of the following maturity level is your organization currently at?**

Response	Tally
Level 1 - Basic: undocumented, dynamic change, ad hoc, uncontrolled and reactive, individual random responses	2
Level 2 - Repeatable: some processes are repeated, perhaps with reliable results, poor discipline process, agreed benchmarks	0
Level 3 - Fixed: a set of defined and documented standard processes, some degree of improvement over time	6
Level 4 - Managed: benchmarking process, effective management control, adaptation without losing quality	2
Level 5 - Optimized: focus is on continuous improvement and innovation	4
Information not available	0

8. **What do you think will help improve your organization's security levels? (multiple answers possible)**

Response	Tally
Senior management commitment	3
Larger budgets	8
Increased security department staff numbers	7
Better employee security awareness	8
Employee reward/disciplinary systems	4
IT steering committees	4
Advanced security technology	6
Other	0

SECTION III: INFORMATION SECURITY MEASURES

1. What do you consider to be your organization's greatest information security risk? (multiple answers possible)

Response	Tally
Insider attacks	4
Hacking attempts by hackers	4
E-mail viruses	11
Malware	5
Internet downloads	4
Incorrect configuration	0
Uncontrolled portable devices	5
Information not available	0
Other	0

2. What information security measures has your organization implemented? (multiple answers possible)

Response	Tally
Antivirus	13
Firewalls	10
Antispam/spyware/phishing solutions	8
IDS/IPS	5
Vulnerability Management	6
Data Loss Prevention/file encryption (memory)	4
Managing event logs (SIEM solutions)	4
Endpoint security management	6
Information not available	1
Other	0

3. **What measures do you usually take to mitigate network security attacks targeted at your organization's infrastructure/customers? (multiple answers possible)**

Response	Tally
ACL's/packet filters	10
Firewalls	11
IPS/IDS	4
Source-based remote-triggered black holes	0
Destination-based remote-triggered black holes	0
Information not available	2
Other	1

4. **What tools does your organization use to detect attacks? (multiple answers possible)**

Response	Tally
Commercial products	10
Open source software	5
Self-developed tools	2
Information not available	3

SECTION IV: INFORMATION SECURITY AWARENESS

1. **Does your organization provide employee training to raise information security awareness?**

Response	Tally
Yes, according to job role and function	9
Yes, through general training	4
Yes, but only where mandated by law/regulations	0
No	4
Other	2

2. **How difficult is it, in your opinion, to convince management to invest in security solutions?**

Response	Tally
Very difficult	3
Somewhat difficult	7
Easy	4
Very easy	0
Information not available	1

3. **What percentage of your IT budget has been spent on security in the last 12 months?**

Response	Tally
0-10%	5
11-30%	2
31-50%	2
More than 50%	0
Information not available	5

4. **Can you describe year-to-year spending in terms of your information security budget?**

Response	Tally
Budget increased	7
Budget has not changed	3
Budget was reduced	0
No information security budget was allocated	3
Information not available	2

SECTION V: THIRD PARTY CONTROL

1. **How does your organization ensure an adequate level of information security when interacting with third parties? (multiple answers possible)**

Response	Tally
Identifies risks related to third parties as part of information risk assessments	6
Addresses information security issues in a contract	5
Signs confidentiality and/or non-disclosure agreements	4
Imposes corporate security policy and controls on third parties	3
Where permitted, performs background verification checks on selected high-risk systems and behaviors	2
Controls third-party access to systems and data	4
Performs random spot checks of third-party sites	0
Requires independent attestation (e.g. ISAE3402, ISO27001:2005 certification)	0
Regularly monitor and review of third party services	3
Not applicable	1
Information not available	2
Other	1

2. How confident are you in the information security practices of third parties?

Response	Tally
Not confident	2
Confident to a certain extent	4
Confident	4
Very confident	0
Not applicable	4

3. Does your organization share information on information security attacks with third parties?

Response	Tally
Yes	3
No	6
Not applicable	5

SECTION VI: CONCLUSION

The data gathered in this is useful in determining the present state of cyber security awareness at various organizations in the country. However, there are some limitations that must be pointed out:

1. The sample size, in this case feedback from only 15 organizations, can be increased order to obtain exceedingly more accurate data.
2. The survey can be extended to the rest of Latin America and the Caribbean Region. This would allow for perspectives at a regional level.
3. There are indications of discrepancies present between responses given across different questions for each individual survey. This may indicate that the responses are not altogether accurate or that the survey takers are not altogether knowledgeable about what they are being asked.

APPENDIX 7: PROPOSED CYBER SECURITY ASSESSMENT METHODOLOGY

A Project Management Approach to Cyber Security Assessments

Based on PMI's PMBOK® 5th Edition and the NIST Cybersecurity Framework

Version 1.1 – 19/10/2018

Formulated by:

Douglas M. O. Westby, P. ENG.
Apt. No. 14. Ladyville Apartments
Ladyville, Belize District
Belize, Central America
Telephone: +501-610-6465
Email: douglas.westby@gmail.com

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas M. O. Westby, P. ENG.	First draft version of this document. No appendices. Submitted for review.	Douglas M. O. Westby, P. ENG.		02/09/18
1.1	Douglas M. O. Westby, P. ENG.	Final version of this document for submission. Appendices added. Grammatical and formatting corrections made.	Douglas M. O. Westby, P. ENG.		19/10/18

Contents

Table of Figures .... *XXIX*

Table of Appendices .... *XXX*

Executive Summary .... *XXXI*

Introduction .... *XXXII*

Background XXXII

Justification XXXII

Intended Audience XXXIII

Choice of Project Management Methodology XXXIII

Choice of Cyber Security Framework XXXIII

Description of the Methodology .... *XXXIII*

Assumptions XXXIV

Methodology Flowchart XXXIV

Phases XXXVII

Processes XXXVII

Sub-processes XXXVII

Conditions XXXVII

Major Inputs XXXVII

Major Outputs XXXVIII

Data XXXVIII

Templates XXXVIII

How to Use Templates XXXVIII

Supplementary Sources of Information XXXVIII

The Initiating Phase (PH.1) .... *XXXIX*

Create Assessment Charter (P.1) XXXIX

Perform Initial Cyber Security Assessment (P.2) XXXIX

Create Statement of Work (P.3) XL

The Planning Phase (PH.2) .... *XL*

Create Assessment Management Plan (P.4) XL

Complete Scope and Cost (P.4.1) XLI

Create Schedule (P.4.2) XLI

Plan Stakeholder Management (P.4.3) XLII

Stakeholder Analysis XLII

Stakeholder Management Plan XLIII

Plan Team Management (P.4.4) XLIII

Plan Communication Management (P.4.5) XLIII

Communication Interactions XLIV

Forms of Communication XLIV

Plan Risk Management (P.4.6) XLIV

Risk Analysis XLIV

Risk Management Plan XLV

Plan Quality Management (P.4.7) XLV

Plan Issue and Change Management (P.4.8) XLV

Issue Management Plan XLV

Change Management Plan XLVI

Conduct Kick-off Meeting (P.4.9) XLVI

The Executing and Controlling Phases (PH.3 and PH.4) XLVI

Execute Assessment (P.5) XLVI

Perform Cyber Security Audit (P.5.1) XLVII

Perform Cyber Security Risk Assessment (p.5.2) XLVII

Determine Required Cyber Security Stance (P.5.3) XLVII

Control Assessment (P.6) XLVIII

Monitor and Control Scope and Cost (P.6.1) XLVIII

Monitor and Control Schedule (P.6.2) XLIX

Manage Stakeholders (P.6.3) XLIX

Manage Team (P.6.4) XLIX

Manage Communications (P.6.5) XLIX

Manage Risks (P.6.6) XLIX

Manage Quality (P.6.7) XLIX

Manage Issues and Change (P.6.8) XLIX

Issue Management L

Change Management L

The Closing Phase (PH.5) .... *L*
Close Assessment (P.7) L
Prepare Final Report (P.7.1) L
Prepare Closure Document (P.7.2) LI
Conduct Assessment Closure Meeting (P.7.3) LI
Archive Documentation (P.7.4) LI

Table of Figures

Figure 3 Methodology Flowchart (part one of two). XXXV
Figure 4 Methodology Flowchart (part two of two). XXXVI
Figure 5 Sub-processes related to P.4 (Create Assessment Management Plan). XLI
Figure 6 First level of NIST Cybersecurity Framework process tree showing the five functions. XLII
Figure 7 Sub-processes related to P.6 (Control Assessment). XLVIII
Figure 8 Sub-processes related to P.7 (Close Assessment). L

Table of Appendices

Appendix A - Assessment Charter Template
Appendix B - Business Case Template
Appendix C - Basic Cyber Security Survey
Appendix D - Initial Cyber Security Assessment Report Template
Appendix E - Statement of Work Template
Appendix F - Assessment Management Plan Template
Appendix G - Information and Communications Technology Inventory Control Template
Appendix H - Cyber Security Risk Analysis Template
Appendix I - Cyber Security Master Profile
Appendix J - Final Assessment Report Template
Appendix K - Assessment Closure Document Template
Appendix L - Archive Listing Document Template

Executive Summary

In order to have an effective cyber security response tailored to its needs, the first thing an organization needs to do is to conduct a well-planned, complete cyber security assessment. The next step would be essentially to make the changes based on the results of the assessment. After the required changes, it would be necessary to maintain that security posture and repeat the assessment at regular intervals in order to improve and maintain an adequate response to constantly evolving cyber-threats.

In order to carry out a well-designed assessment covering all cyber security aspects of the organization, it is necessary to be well prepared and to approach the assessment in a methodical way. Assessments are short-term endeavors, and in most cases, especially in larger organization, it is necessary to manage these assessments using a project management approach to maximize resource usage, reduce time, and to guarantee complete, technically sound outputs.

This work attempts to formulate a methodology for cyber security assessments by applying the Project Management Institute's *Project Management Body of Knowledge* to the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*. Since it uses these two works as references, it does not go in depth as it assumes that the reader will also reference them when necessary. Instead, it forms the groundwork for assessments and contains sufficiently detailed templates that go more in-depth into the cyber security assessment process.

It is expected that this methodology will grow and more details and changes will be added as the matter of information and communications technology and cyber security becomes more prevalent in the region.

Introduction

Background

As society becomes more and more dependent on technology, the dangers from loss or intentional corruption of information as well as downtime of critical services and the possibility of the commission of criminal and terrorist acts using technology have become more and more possible.

Belize and the broader Caribbean has advanced at a very fast pace when it comes to the implementation of information and communications technology solution. However, it has not been until recently that the problem of cyber security is beginning to be addressed at the national and regional levels with the participation of stakeholders from both the public and the private sector.

In most Caribbean countries including Belize, mechanisms and governance structures are not readily available to respond to cyber-threats and the extent of how much damage is being done is difficult to determine accurately since most private enterprises are not obligated to report cyber-crime to the authorities, and most prefer not to do so.

Due to the lack of centralized mechanisms and governance structure in-country, it is difficult to get assistance when needed and most organizations and businesses try as much as possible to keep these problems quiet when they do occur due to the negative repercussions of being a victim of cyber-crime.

Justification

Most organizations are dependent on information and communication technologies and as critical government infrastructure such as banking systems and major utilities becomes increasingly integrated with information and communications technology, cyber-threats will increase and potential risks and losses will increase proportionally along with it.

Having an integrated cyber security response and taking preventative measures is and will be vital for the survival of most organizations.

In order to implement an adequate response and to establish an acceptable stance, it is necessary to implement changes to the organization in terms of their cyber security readiness. The first and most logical step is by means of an assessment of the current state of readiness of the organization.

This work outlines a project management approach to cyber security assessments based on existing information and communications technology infrastructure and the cyber security needs organizations of various sizes.

Intended Audience

This methodology is intended to be implemented at organizations of various sizes in country and in the region. It is designed to be adoptable and easy to implement.

Choice of Project Management Methodology

There are various project management methodologies in existence, each with various levels of completeness and designed for various environments and purposes.

The most well-known and perhaps the most complete methodology is that offered by the Project Management Institute® (PMI) and documented in various documents, the main being *The Standard for Project Management of a Project* that is further described in *A Guide to the Project Management Book of Knowledge (PMBOK® Guide).*

This methodology is based on the knowledgebase of the Project Management Institute® due to its completeness and because it is the most widely used.

Choice of Cyber Security Framework

Cyber security frameworks or standards are combinations of guidelines, techniques rules and best practices that attempt to protect the cyber environment of a user or an organization. This environment includes users themselves, networks, devices, software, processes, information in storage or transit, applications, services and systems that can be connected directly or indirectly to networks. The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks.

This methodology uses the *Framework for Improving Critical Infrastructure* of the National Institute of Standards and Technology (NIST) due to its availability, ease of implementation and its adoptability to organization of various sizes. It also references other well-known standards that are presently being used. It is also a living document that is frequently used and updated.

Description of the Methodology

This methodology is divided into two parts:

The first part, which is this document, describes the various phases, processes, documents and other components, sub-process and steps that are to be taken to carry out the cyber security assessment. For guidance, the following labeling is use throughout the document:

- ‘PH.X’ denotes a phase where ‘X’ is the unique number identifying the phase.
- ‘P.X’ denotes a process where ‘X’ is the unique number identifying the process. Sub-processes are listed in the ‘P.X.Y’ format.
- ‘D.X’ denotes a document, which is either a Major Output or Major Input of a process where ‘X’ is the unique number identifying the document.

The second part is a collection of templates, tools and techniques that complements and references this methodology. These are illustrative and instructional and are an important part of the methodology.

The rest of this section describes how to use this methodology and lists the various subcomponents and templates that come along with it.

Assumptions

The following are a list of assumptions that are to be considered when using this methodology:

1. The main references for project management framework and cyber security frameworks as outlined in this document are readily available and will be used as a reference when necessary to initiate, plan, execute and control and close cyber security assessments.
2. The users of this methodology are sufficiently versed in information technology and cyber security as well as project management in order to understand and implement this methodology.

Methodology Flowchart

The Methodology Flowchart gives a diagrammatic representation of the most important aspects of this methodology laid out as a series of major processes, inputs and outputs and other actions and complemented by main decision branches. It is divided into Phases, each with its Processes, Sub-processes, Conditions, Major Inputs and Major Outputs. The whole flowchart is show in Figure 1 and Figure 2.

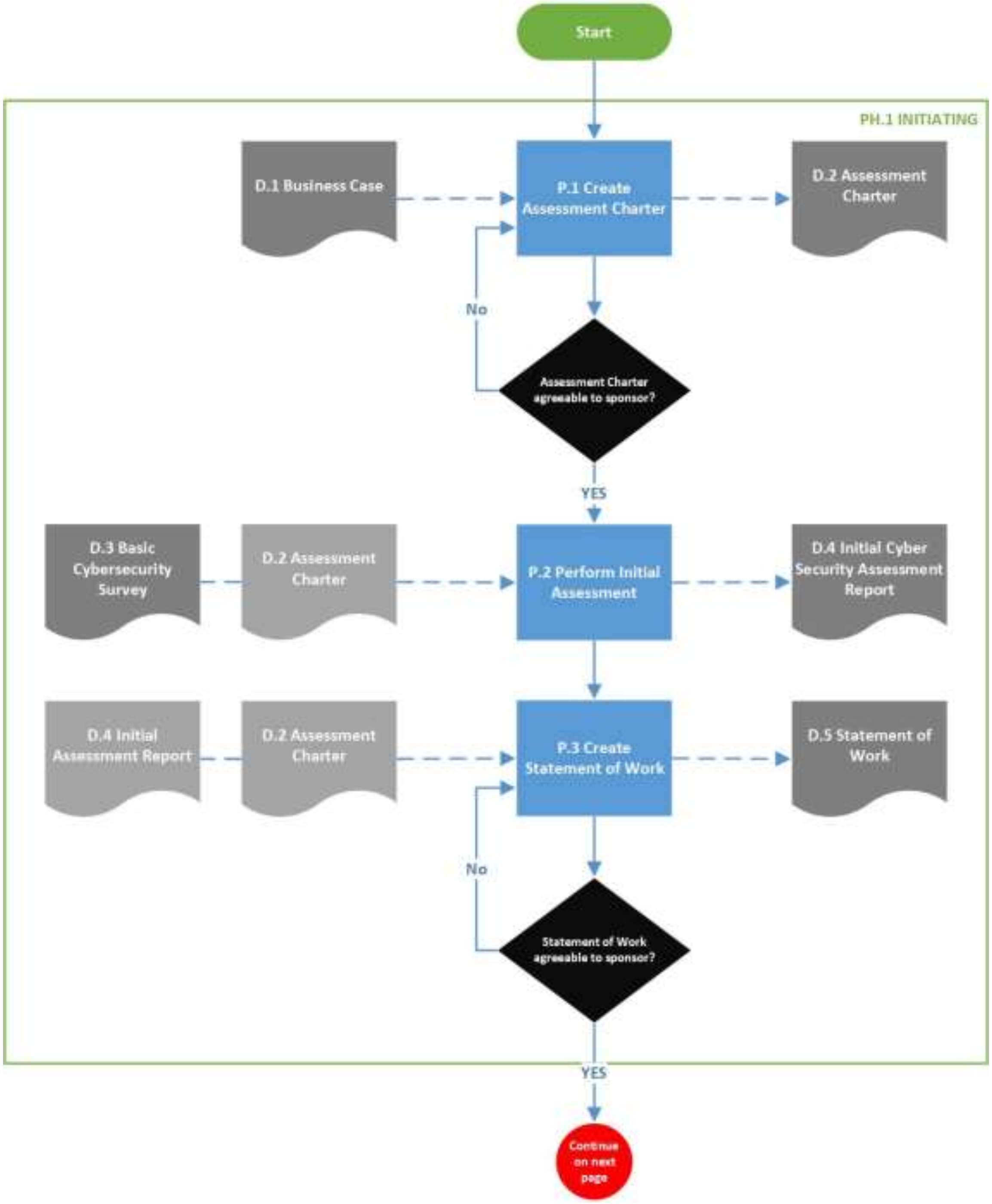

Start
PH.1 INITIATING
D.1 Business Case
P.1 Create Assessment Charter
D.2 Assessment Charter
No
Assessment Charter agreeable to sponsor?
YES
D.3 Basic Cybersecurity Survey
D.2 Assessment Charter
P.2 Perform Initial Assessment
D.4 Initial Cyber Security Assessment Report
D.4 Initial Assessment Report
D.2 Assessment Charter
P.3 Create Statement of Work
D.5 Statement of Work
No
Statement of Work agreeable to sponsor?
YES
Continue on next page

Figure 3 Methodology Flowchart (part one of two).

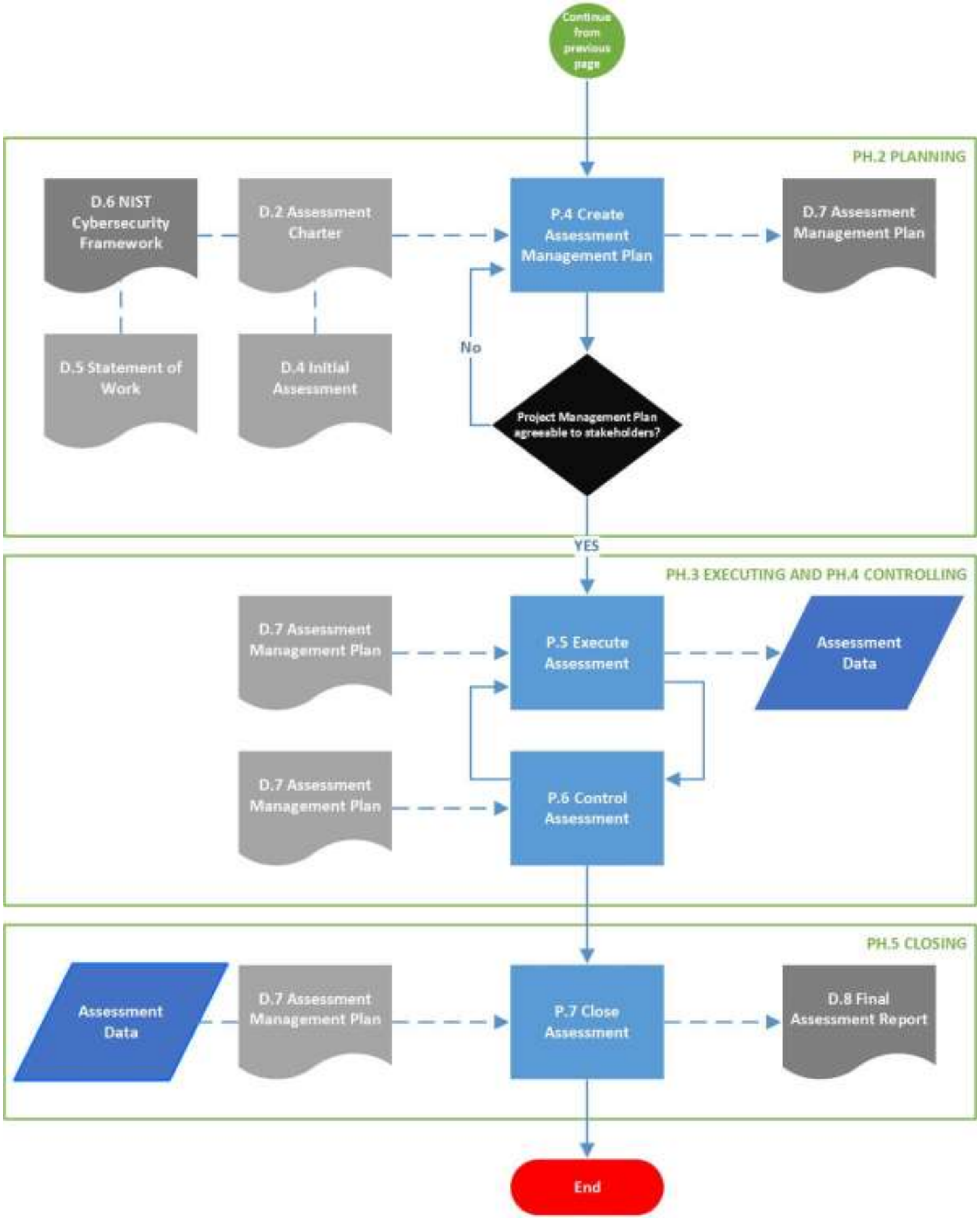

Continue from previous page
PH.2 PLANNING
D.6 NIST Cybersecurity Framework
D.2 Assessment Charter
P.4 Create Assessment Management Plan
D.7 Assessment Management Plan
D.5 Statement of Work
D.4 Initial Assessment
No
Project Management Plan agreeable to stakeholders?
YES
PH.3 EXECUTING AND PH.4 CONTROLLING
D.7 Assessment Management Plan
P.5 Execute Assessment
Assessment Data
D.7 Assessment Management Plan
P.6 Control Assessment
PH.5 CLOSING
Assessment Data
D.7 Assessment Management Plan
P.7 Close Assessment
D.8 Final Assessment Report
End

Figure 4 Methodology Flowchart (part two of two).

Phases

The complete methodology, as reflected in the Methodology Flowchart, is divide into five phases consistent with the traditional project management life cycle. These are Initiating, Planning, Executing and Controlling, and Closing; the next four main sections of this document lays out these phases in more detail.

In the Methodology Flowchart, phases are represented by a light green frames that are appropriately labeled.

Processes

Phases are further grouped into processes. Processes are a series of actions or steps taken to produce an output necessary in order to move the assessment forward.

In the Methodology Flowchart, processes are represented by light blue boxes.

Sub-processes

The Methodology Flowchart does not represent sub-processes such the various ones involved in the Create Assessment Management Plan or those involved in the Perform Assessment, Execute & Control Assessment Processes and the Close Assessment Process.

The reason why sub-processes are not show in the Methodology Flowchart is to maintain simplicity. However, sub-processes will be described and used throughout this document and where additional diagrams are used; they are represented by white boxes.

Conditions

Conditions or conditional statements are essentially points of agreements or consensus between the entity carrying out the assessment and client in order to move forward.

In the Methodology Flowchart, Conditions are represented by a black diamond, and the two possible output branches are either ‘yes’ or ‘no’.

Major Inputs

Major Inputs are main documents, instruments or data that is used by a process to produce an output. They are represented on the left side of the Methodology Flowchart as gray, rectangular, irregular shapes.

Inputs of one process can be outputs of other processes as can be seen on the Methodology Flowchart.

Major Outputs

Major Outputs are main documents, instruments or data that are a result of a process. They are represented on the right side of the Methodology Flowchart as gray, rectangular, irregular shapes.

Outputs of one process can be inputs of other processes as can be seen on the Methodology Flowchart.

Data

Data is represented in the Methodology Flowchart by a dark blue parallelogram; this is the information gathered from the cyber security analysis and is the precursor to the main delivery which is the Final Assessment Report.

Templates

Templates are guides that serve as a starting point to formulate a new document or form. Templates allows for an easy and uniform way to document and carry out the project from initiation to closure. They represent the main documentation that is to be produced in order to complete an assessment.

The templates available that complement this methodology can be found in the appendices of this document and are referenced throughout this work; however, note that what is provided is not definitive since requirements and needs may vary from project to project. The user of this methodology is not limited to or obligated to use the templates provided; other templates can be used or the ones available can be modified on a case-by-case basis.

How to Use Templates

In order to produce a document, copies of the templates can be edited. Each template is formulated in such a way that:

- Italicized statements enclose in square bracket ('[]') should be replaced with pertinent information.
- Italicized statements enclose in angle bracket ('<>') are instructional and should be removed.

As the case may be, templates can be edited more in detail, and sections can be added and removed; or they can be completely replaced by different templates of the user's choice.

Supplementary Sources of Information

There are two documents that are important reference sources; primarily because these are the documents from which this methodology is based on and contain additional details that can be used to assist in formulating and executing assessments:

- *A Guide to the Project Management Book of Knowledge (PMBOK® Guide)* from the *Project Management Institute® (PMI).* This book is commercially available in both digital and hard copy.
- The *Cybersecurity Framework* from the *National Institute of Standards and Technology (NIST).* A downloadable copy of this document and related resources are available at: https://www.nist.gov/cyberframework.

The Initiating Phase (PH.1)

The initiation phase marks the beginning of the project. In this phase, the idea for the project is explored and sufficiently elaborated on in order to get a high-level understanding of why it is needed and what it is about. The goal of this phase is to determine whether or not it makes sense to carry through the assessment. In addition, some initial information about the nature of the assessment and about the client's organization and environment is gathered during this phase.

Create Assessment Charter (P.1)

The very first step toward doing the cyber security assessment is to create an Assessment Charter. An assessment charter is a high-level, preliminary statement of scope, objectives and participants in the assessment. It provides a preliminary delineation of roles and responsibilities, outlines the assessment objectives, identifies the main stakeholders, and defines the authority of the assessment manager.

A template for a typical *Assessment Charter* is available in **Appendix A**.

The main input for the creation of the assessment charter is the Business Case. A business case captures the reason for initiating a project or task. The logic of the business case is that, whenever resources such as money or effort are consumed, they should be in support of a specific business need. This is important because cyber security assessments are a relatively new endeavor and come with an associated cost.

A template for a *Business Case* is available in **Appendix B**.

Perform Initial Cyber Security Assessment (P.2)

In order to actually carry out an in-depth assessment, it is necessary to have certain initial high-level information about the size of the organization, its resources as well as its attitude towards cyber security and how prepared the organization is to handle cyber-threats. In order to do so, an Initial Assessment should be carried out. This assessment will provide information that will allow for the creation of a better statement of work, as well as provide very valuable information that can be used in the planning stage of the assessment.

The main input for the Initial Cyber Security Assessment is the Assessment Charter and the Basic Cyber Security Survey. Information gathering can be carried out by interviewing key personnel who are knowledgeable about information technology and about how the organization works as well as using other methods. The following areas should be covered:

- Organizational Identification
- Business Scope
- Firewalls and Gateways
- Secure Configuration
- Access Control
- Malware Protection
- Patch Management
- Any other information that may be pertinent

An example of a *Basic Cyber Security Survey* can be found in **Appendix C**. The survey can be used in conjunction with interviews and other data-gathering techniques.

A template for the *Initial Cyber Security Assessment Report* can be found in **Appendix D**. This covers the information gathered from the initial assessment process.

Create Statement of Work (P.3)

If the assessment requires an additional level of a detail, or requires an agreement that is more detailed and legally binding, it may be necessary to create a Statement of Work. In cases where this is not necessary, this process can be omitted.

A template for a *Statement of Work* is available in **Appendix E**.

The Planning Phase (PH.2)

Create Assessment Management Plan (P.4)

In the Planning Phase, various plans are put together to ensure that scope, schedule, cost, quality, change, risk and other issues are managed properly. It also helps to manage staff and people. The overall objective of this phase is to ensure that the assessment team is sufficiently prepared to carry out the assessment and that key stakeholder are apprised of and are in agreement with these preparations.

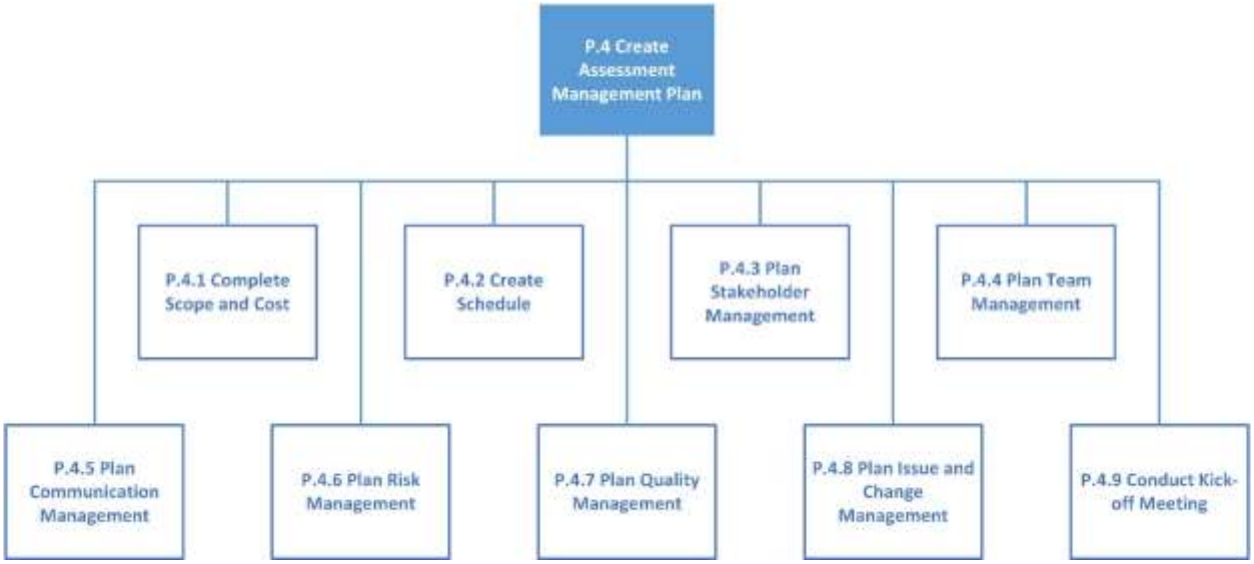

P.4 Create Assessment Management Plan
P.4.1 Complete Scope and Cost
P.4.2 Create Schedule
P.4.3 Plan Stakeholder Management
P.4.4 Plan Team Management
P.4.5 Plan Communication Management
P.4.6 Plan Risk Management
P.4.7 Plan Quality Management
P.4.8 Plan Issue and Change Management
P.4.9 Conduct Kick-off Meeting

Figure 5 Sub-processes related to P.4 (Create Assessment Management Plan).

Due to the nature of this assessment, some of the information that is normally gathered in the planning stage is already collected in the Initiating Stage.

The Assessment Management Plan incorporates all the processes that are described in this section and is the main output of this phase. A template for an *Assessment Management Plan* can be found in **Appendix F**.

Complete Scope and Cost (P.4.1)

At this point in the project, most of the scope and cost had already been created in the assessment charter and statement of work in the initiating phase. However, there may be finer details to add. This can be done as a standalone document or a part of the assessment management plan.

The *Scope and Cost* can be found in the *Assessment Management Plan Template* in **Appendix F**.

Create Schedule (P.4.2)

The assessment Schedule is completed in the planning stage along with scope and cost since all three are closely related. The schedule allows for the distribution of work and the usage of resources over time. One of the key issues with cyber security assessments is the access to organizational resources in order to gather information; this is an important part of the schedule as the assessment must be done with minimum interruption and the information being gathered is sensitive. Furthermore, many interactions and exchanges will occur in order to gather behavioral data from employees and this normally happens during working hours.

The schedule is dependent on the Work Breakdown Structure (WBS). The work breakdown structure subsequently is based on the hierarchical system of functions, categories and subcategories system as defined by the NIST Cybersecurity Framework. At the subcategories level, the work breakdown structure can be further divided in smaller packages if necessary.

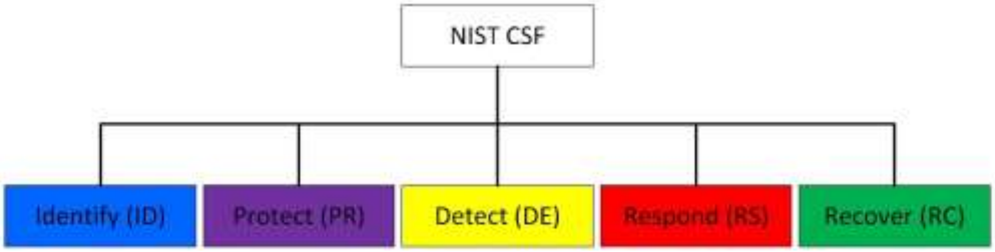


Figure 6 First level of NIST Cybersecurity Framework process tree showing the five functions.

The following are the five functions and corresponding categories that are to be assessed:

- Identify – Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.
- Protect – Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance and Protective Technology.
- Detect – Anomalies and Events, Security Continuous Monitoring and Detection Processes.
- Respond – Response Planning, Communications, Analysis, Mitigation and Improvements.
- Recover – Recovery Planning, Improvements and Communications.

This breakdown and process tree structure can aid in the creation of the WBS and the schedule.

The *Schedule* can found in the *Assessment Management Plan* template in **Appendix F**.

Plan Stakeholder Management (P.4.3)

A stakeholder can be defined as any individual or group that can affect, be affected by, or perceive themselves to be affected by a project or other endeavor. Stakeholder management creates positive relationships with stakeholders through the appropriate management of their expectations and agreed objectives. Because of this, the Stakeholder Management Plan is closely related to the Communications Management Plan.

Stakeholder Analysis

The first step in performing a Stakeholder Analysis is to identify stakeholders and determine their levels of interest and influence on the assessment. This process may have already started in the Initiating Phase; if that is the case, it is further developed in this process.

The *Stakeholder Analysis Plan* can be found in the *Assessment Management Plan template* in **Appendix F**.

Stakeholder Management Plan

A complement to stakeholder analysis is stakeholder management which is deciding what to do with each type or category of stakeholder and establishing actions that can be taken to ensure how and when they should be informed and interacted with.

The Stakeholder Management Plan is created as a result of the stakeholder analysis and should contain stakeholder-actions pairing for at least the more influential stakeholders associated with the assessment.

The *Stakeholder Management Plan* can be found in the *Assessment Management Plan* template in **Appendix F**.

Plan Team Management (P.4.4)

The assessment team is comprised of the people with the necessary expertise to carry out the assessment. This is done after the scope has been formulated; the rationale behind this is that the necessary technical expertise and the number of team members are determined by the scope of the project. Depending on the scope of the project, the following is a list of standards and guidelines the assessment should be familiar with as these are the main references:

- CCS CSC
- COBIT 5
- ISA 62443-2-1:2009
- ISA 62443-3-3:2013
- ISO/IEC 27001:2013
- NIST SP 800-53 Rev. 4
- ISO/IEC 27001:2013

The *Assessment Team Management Plan* can be found in the *Assessment Management Plan* template in **Appendix F**.

Plan Communication Management (P.4.5)

The Communication Plan is important in order to share information and to make it possible to target communication accurately. It gives a structure to determine who need to be reached, how often and how.

There are two important aspects of communications that must be considered; there are communications that is necessary to carry out the assessment, and the communications necessary to obtain critical information about cyber security.

Communication Interactions

There are various lines of interactions or communications that takes place and it is important to identify them in order to better communicate. These are outlined as follows:

- Communications between project or assessment manager and team members.
- Communications in between members of the assessment team.
- Communications between assessment team or project manager and contact persons, key stakeholders and sponsor for the client.
- Communications between assessment team and employees, agents or users of the information technology systems of the client. This form of communication is a part of planning the scope of the assessment and will not be discussed in this section.

Forms of Communication

There are various forms of communication that are customarily used in assessments. The main ones are outlined as follows:

- Face-to-face and online meetings
- Email communications
- Face-to-face interviews
- Questionnaires and surveys, online and in print
- Telephone conversations
- Group chat and messaging
- Verbal communications
- Written reports and correspondences

The *Communication Management Plan* can be found in the *Assessment Management Plan* template in **Appendix F**.

Plan Risk Management (P.4.6)

Risk is the potential to gain or lose something of value. It is essentially divided into two parts, risk analysis and risk management. It is important that risk management of the project is separate from the risk analysis of cyber security that will take place as part of the assessment.

Risk Analysis

Risk analysis can be defined as the identification, evaluation and measurement of the probability and impact of risk on the assessment itself. A risk analysis must be done as a part of the planning process. Preliminary risk analysis may have been done in Initiation Phase; it is further developed in order to develop the Risk Management Plan.

The *Risk Analysis* template can be found in the *Assessment Management Plan* template in **Appendix F**.

Risk Management Plan

A complement to risk analysis is risk management which is essentially deciding what to do about risks when they occur by establishing actions that can be taken to mitigate or eliminate them.

The Risk Management Plan is created as a result of the risk analysis and should include risk-response pairs for at least all risks that are severe and are likely to occur.

The *Risk Management Plan* can be found in the *Assessment Management Plan* template in **Appendix F**.

Plan Quality Management (P.4.7)

The Quality Management Plan defines the acceptable level of quality of the project and describes how the project will ensure this level of quality in its deliverables and processes. Quality management activities ensure that the assessment is carried out with the agreed-upon standards and requirements, work processes are performed efficiently as documented and nonconformance found are identified and appropriate corrective action is taken.

The Quality Management Plan applies to both the assessment deliverables and the assessment processes. It is important to note that the reference standard has their own quality standards, and this will largely define the quality standards of the assessment being carried out.

The Quality Management Plan should have two main objectives:

1. Ensure that the assessment is carried out as planned and with a high level of efficiency.
2. Ensure that the quality standards required by the reference standards are adhered to.

The *Quality Management Plan* can be found in the *Assessment Management Plan* template in **Appendix F**.

Plan Issue and Change Management (P.4.8)

Due to the relationship between issues and changes, the issue and change management plans have been grouped together.

Issue Management Plan

An issue is a major problem, opportunity, concern or situation that will impede the progress or successful completion of the project and requires immediate resolution. An issue management plan defines activities and business rules to manage and control issues that arise during the project.

The Issue Management Plan should be designed to bring visibility to issues and accountability for how issues are acted upon and helps to ensure issues are resolved effectively and in a timely manner. There should also be rules for prioritization and escalation of issues that ensures that the project's objectives are not adversely affected.

Change Management Plan

A Change Management Plan helps manage the change process, and ensures control in scope, schedule, cost and other processes and resources.

Elements of the change management plan should include a reporting and authorizing structure. Changes should be in line with the general objectives of the assessment and there should be a clear mechanism to update major project documents as well as detailed history of changes.

The *Issue and Change Management Plan* can be found in the *Assessment Management Plan* template in **Appendix F**.

Conduct Kick-off Meeting (P.4.9)

After assessment management plan is completed and all required documents have been created, it is necessary to schedule a kick-off meeting for the assessment. All team members and other key stakeholders should be a part of the meeting. Key processes such as the purpose of the assessment, the scope and extent should be discussed. Expectations with regards to all major aspects of the assessment should be managed and questions regarding the project should be addressed.

The Executing and Controlling Phases (PH.3 and PH.4)

Project execution is the phase in which the plan designed in the previous phase is put into action. The purpose of Executing Phase is to deliver the project expected results.

The Controlling Phase consists of monitoring the activities of the executing stage in order to identify problems and risks, and carry out mitigating actions in order to guide the process to completion.

Although the Executing and Controlling Phases are distinct, they are group into one since they are conducted simultaneously.

Execute Assessment (P.5)

The execution of the cyber security assessment is essentially carrying out the assessment plan primarily in terms of scope and schedule and cost. This is the main action to be carried out after the planning phase. There are typically three main processes that need to occur during the cyber security assessment as shown in Figure 5 and are normally defined during the planning phase.

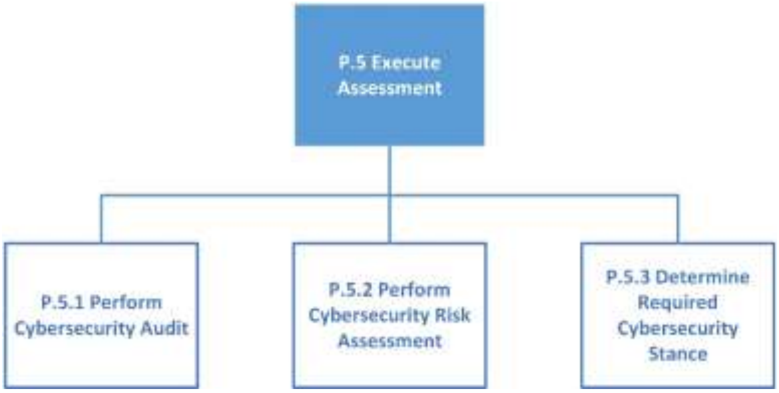

P.5 Execute Assessment
P.5.1 Perform Cybersecurity Audit
P.5.2 Perform Cybersecurity Risk Assessment
P.5.3 Determine Required Cybersecurity Stance

Figure 5 Sub-processes related to P.5 (Execute Assessment).

Perform Cyber Security Audit (P.5.1)

This process determines what is in place at that particular point in time to address matters of cyber security readiness. Information is gathered about the organization itself, the environment, the nature and business of the organization, etc. This information will then be used to create a Cyber Security Profile (see process P.5.3) of the organization.

Part of the assessment is the performance of inventory control the technology and equipment being used at the organization as this forms the basis of issues and risk related to cyber security. To do this, inventory control must be taken. A basic *Information and Communications Technology Inventory Control* template can be found in **Appendix G**. This can be used to document inventory information.

Perform Cyber Security Risk Assessment (p.5.2)

This risk analysis determines the possible cyber security threats that can affect the organization along with severity and probability of occurrence.

A typical *Cyber Security Risk Assessment* template for cyber security assessments base on the reference cyber security framework can be found in **Appendix H.** The template also serves as a checklist or a guidance document and is broken down into functions, categories and subcategories as defined by the reference framework.

Determine Required Cyber Security Stance (P.5.3)

This process determines what needs to be in place at some point in the future, or where the organization wants to be in terms of readiness. This can be presented as the Target Profile of organization – other words it is a representation of where the organization needs to be in terms of cyber security.

A *Cyber Security Master Profile* based on the NIST Cybersecurity Framework that can be used to create the Cyber Security Profile can be found in **Appendix I**. The listing contains all functions, categories and subcategories as defined by the framework and should be tailored to each assessment by removing elements that are not necessary.

Control Assessment (P.6)

As the assessment is being done, the control assessment phase ensures that the assessment goes as planned. This requires that various aspects and processes of the assessment are monitored and actions taken if they are not going as planned.

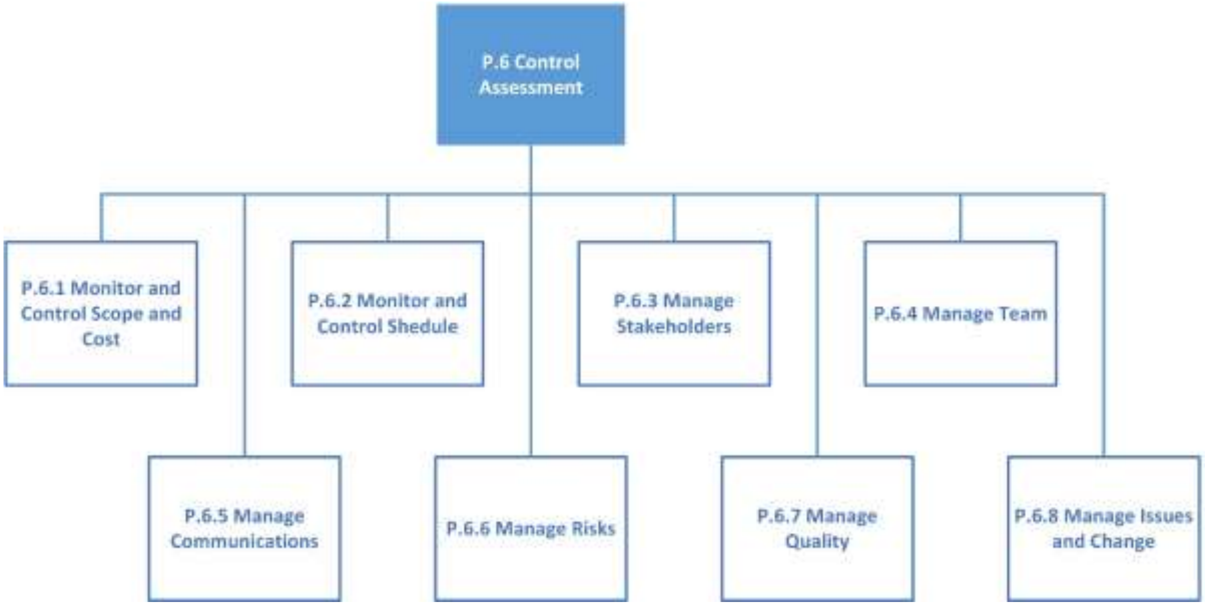

P.6 Control Assessment
P.6.1 Monitor and Control Scope and Cost
P.6.2 Monitor and Control Shedule
P.6.3 Manage Stakeholders
P.6.4 Manage Team
P.6.5 Manage Communications
P.6.6 Manage Risks
P.6.7 Manage Quality
P.6.8 Manage Issues and Change

Figure 7 Sub-processes related to P.6 (Control Assessment).

Monitor and Control Scope and Cost (P.6.1)

The purpose of implementing scope control is to identify and manage all elements of the project, especially those that may increase or decrease the project scope beyond the already defined objectives, goals and baselines of the project.

Scope changes will come from the perceived need for a change in a project deliverable that may also affect other aspects of the project such as cost and schedule. Because scope changes frequently require a change in resources and time, all scope change requests should be submitted in writing using the process defined in the Change Control Plan.

Cost is important as well, but due to the nature of the kind of work being carried out, cost does not vary greatly. Cost will vary with scope and schedule, therefore care must be taken and changes to cost or budget must be manage by means of the Cost Management Plan.

Monitor and Control Schedule (P.6.2)

It is important for the Project Team as well as the client and some stakeholders to be aware of where the project is in terms of schedule and completion. It becomes necessary for the project manager to request feedback from various members of the project team and from other stakeholders to determine the status of the project. The Communication Plan will define how these update are supposed to happen.

Manage Stakeholders (P.6.3)

Stakeholders are managed based on the information gathered from the stakeholder analysis process and the stakeholder management plan.

Manage Team (P.6.4)

The assessment team must be coordinated base on the schedule and scope of the assessment. During the assessment process is when it is most necessary to acquire feedback from the assessment team members.

Manage Communications (P.6.5)

The managing communications is an important factor in the executing and controlling phase. A large part of a project manager's responsibility during this stage of the project is keeping the stakeholders informed of project status. This is done according to the communications plan.

Manage Risks (P.6.6)

Based on probability of occurrence and severity, risks must be monitored and mitigated in order for the project to be successfully completed. Monitoring must occur frequently and the communication plan must be used where possible to keep stakeholder informed and to acquire risk related feedback.

Manage Quality (P.6.7)

In the case of a cyber security assessment, it is the responsibility of the Assessment Manager and assessment team as well as the client's technical team to ensure that quality is managed. The reason for this is that it is frequently the technical people who are aware of the quality requirements for the assessment. This is especially true if this is the first time the assessment is being done.

Manage Issues and Change (P.6.8)

Managing change is the carrying out by the Change Management Plan. This deals with how issues and change requests are identified, reported and acted upon.

Issue Management

The issue management process is dictated by the Issue Management Plan. It is the responsibility of the Assessment Manager to ensure that issues are documented and addressed.

Change Management

The change management process is dictated by the Change Management Plan. It is the responsibility of the Assessment Manager to ensure that changes are documented and project documents are updated.

The Closing Phase (PH.5)

The closing phase is composed of the actions taken to wind down the project. The actions taken typically involves handing over the deliverables to the customer, archiving and passing the documentation to the client organization, completing payments, releasing resources, and informing stakeholders of the closure of the project.

Close Assessment (P.7)

This phase essentially has one principal process that is further broken down into four sub-processes as show in Figure 6.

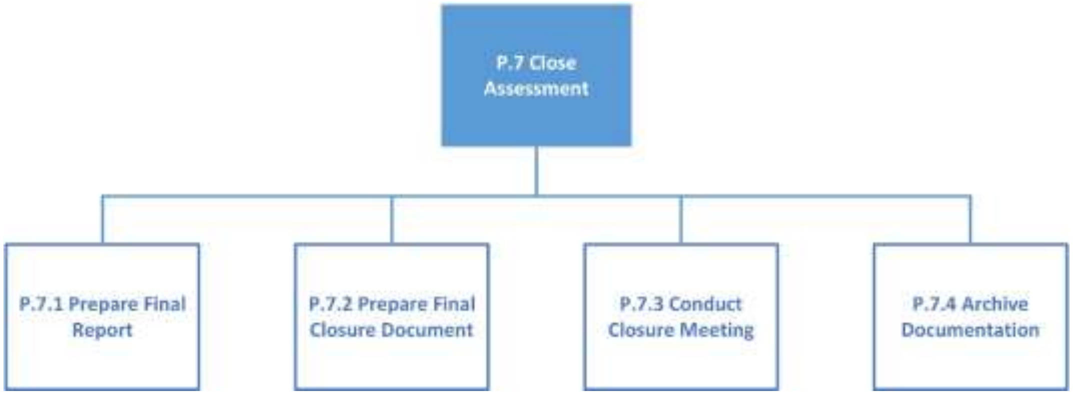

P.7 Close Assessment
P.7.1 Prepare Final Report
P.7.2 Prepare Final Closure Document
P.7.3 Conduct Closure Meeting
P.7.4 Archive Documentation

Figure 8 Sub-processes related to P.7 (Close Assessment).

Prepare Final Report (P.7.1)

The process of preparation of the Final Assessment Report is the most important function of the Closing Phase and of the whole project since this is the main deliverable.

A template for a typical *Final Assessment Report* template is available in **Appendix J**.

Prepare Closure Document (P.7.2)

The purpose of the Assessment Closure Document is to get verification and signoff from the client that the deliverables identified in the Scope are complete. This document is customized to the particular project to include pertinent deliverables, key features and important information about final product which is essentially the Final Assessment Report.

If there was a deviation from the normal course or the deliverables were not completed for any reason, this should be documented and the reasons why given.

A template for a typical *Assessment Closure Document* is available in **Appendix K**.

Conduct Assessment Closure Meeting (P.7.3)

The most important event in the closure of the project is the acceptance of the final products which are the results of the assessment. The best way to ensure this is to convene a final meeting with all the necessary stakeholders in order to avoid clearing up open issues on an individual basis and in order to have consensus.

During this time, the Final Assessment Report is presented along with all supporting documentation, and the trajectory of the project is discussed along with all the issues and modifications to the scope, schedule and cost that took place if any. Any pending work, open items or program level issues can be officially closed or reassigned to the client or support organization.

The final deliverable of this meeting should be the Assessment Closure Document created by the Project Manager describing the project's final deliverables in comparison with the authorized project baseline documents (or statement of work, if applicable). Approval is verified via the signature of Assessment Closure Document by the Stakeholders who signed off on the original project document.

Archive Documentation (P.7.4)

Archiving documentation is important for the executors of the assessment since it is an importation source of information that can improve future assessments.

The specific information being archived will vary, but typically they are all the documents produced and outlined in this methodology as well as notes, estimates, technical documents and any other information that may be useful.

It is advisable to submit all documents in a single file or archive with a cover document such as an *Archive Listing Document* that lists all the documents that is being handed over, this document should be received and signed off by authorized agent of the client. If information is available digitally, it can be properly organized and handed over in a portable media device and signed off on using the same *Archive Listing Document*.

The client may already have an archiving system so it is necessary to consult with them in order to deliver archives in a medium that is convenient.

For the assessment team or project management organization, it may be necessary and convenient to archive all document digitally as the number of projects grow.

A template for a typical *Archive Listing Document* is available in **Appendix L**.

Appendix A: Assessment Charter Template

Assessment Charter

Project Identification

Name	
Description	
Sponsor	
Start Date	
End Date	
Project Manager	

Background

Justification

Scope

Objectives

Key Deliverables

Name	Description

Milestones

Milestone	Dates

Success Criteria

Resources Required	
Human Resources	Other Resources

Budget

Assumptions

Constraints

Risks	
Description	Severity

Authorization			
Sponsor		Project Manager	
Signature		Signature	
Full Name		Full Name	
Title		Title	

Appendix B: Business Case Template

Business Case

Project Identification	
Name of Organization	
Author	
Sponsor	
Start Date	
End Date	
Project Manager	

Executive Summary

[Give a summary of key points of the business case including a brief overview of the current state of affairs and of the project or endeavor and key benefits.]

Justification

[Define the reasons for undertaking the project or endeavor, explains how the undertaking will enable the achievement of corporate strategies and objectives.]

Expected Outcomes

[Express the benefits that the project or endeavor will deliver in measureable terms. Define what problem will be solved. Express what the possible scenarios are if actions are not taken.]

Time, Cost and Scope

[Provides a summary of what the plan is expected to look like in terms of time, scope and cost. This section is optional, applicable only if the information is available.]

Major Risks

[Give a summary of possible major risks associated with the endeavor, what would be their impact, and how would they be mitigated or managed.]

Approvals

The following (signed) approvals are required for this document:

Name	Title	Signature	Date
[Name 1]	*[Title 1]*		
[Name 2]	*[Title 2]*		
[Name 3]	*[Title 3]*		
[…]	*[…]*		

Distribution

This document has been distributed to those listed below:

Name	Title	Signature	Date
[Name 1]	*[Title 1]*		
[Name 2]	*[Title 2]*		
[Name 3]	*[Title 3]*		
[…]	*[…]*		

Appendix C: Basic Cyber Security Survey

[Name of Project]

Basic Cyber Security Survey

A preliminary survey to determine initial requirements for cyber security assessment plan.

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Contents

Confidentiality Statement .... *LXIII*
Introduction .... *LXIII*
Instructions .... *LXIII*
Organization Identification .... *LXIV*
Scope .... *LXIV*
Firewall and Gateways .... *LXIV*
Secure Configuration .... *LXV*
Access Control .... *LXV*
Malware Protection .... *LXVI*
Patch Management .... *LXVI*
Other Information .... *LXVI*

Confidentiality Statement

All information gathered by this survey will be used for the sole purpose of designing an appropriate Project Management Plan and/or Statement of Work in order to carry out a full cyber security assessment at the business or organization in question and within the defined scope.

No personal, confidential, privileged or proprietary information will be released, disclosed, reproduced or otherwise used.

Introduction

This survey is comprised of a series of questions in six different subject areas related to business function and cyber security. It is designed to:

1. Determine the state of readiness of the business or organization, or its state of readiness in terms of cyber security.
2. The size of the business and organization and its resources.

This information will then be used to generate an Initial Assessment Report which will then be used to design an appropriate Statement of Work and Project Management Plan.

This most of the questions and subsections in this are based on or taken from the *Cyber Essentials Common Questionnaire V1.1.*

Instructions

1. This survey is designed to gather information from IT personnel who have knowledge of the information technology being used and the cyber security policies and practices of the organization.
2. It is important that answers are presented as accurately and as completely as possible.
3. Only answer questions that are applicable to the organization.

Organization Identification

Organization Name	
Parent Organization Name	
Brief Description	
Product or Services Offered	
No. of Employees	
Contact Person Name	
Contact Person Job Title	
Contact Person Email Address	
Contact Person Telephone Number	

Scope

Identify the scope of the systems or subsystems to be assessed under this survey, including locations, network boundaries, management and ownership. Where possible include IP addresses and/or ranges.

Firewall and Gateways

1. Have you installed firewalls or similar devices at the boundaries of the networks in the scope?

2. Have the default usernames/passwords on all boundary firewalls (or similar devices) been changed to a strong passwords?

3. Have all open ports and services on each firewall (or similar device) been subject to justification and approval by an appropriately qualified and authorized business representative and has this approval been properly documented?

4. Have all commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOS, tftp, RPC, rlogin, rsh, rexec) been disabled or blocked by default at the boundary firewalls?

5. Confirm that there is a corporate policy requiring all firewall rules that are no longer required to be removed or disabled in a timely manner and that this policy has been adhered to (meaning that there are currently no open ports or services that are not essential for the business).

6. Confirm that any remote administrative interfaces has been disabled on all firewall (or similar) devices.

7. Confirm that where there is no requirement for a system to have Internet access, a Default Deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the Internet.

Secure Configuration

1. Have all unnecessary or default user accounts been deleted or disabled?

2. Confirm that all accounts have passwords, and that any default passwords have been changed to strong passwords.

3. Has all unnecessary software, including OS utilities, services and applications, been removed or disabled?

4. Has the Autorun (or similar service) been disabled for all media types and network file shares?

5. Has a host based firewall been installed on all desktop PCs or laptops and is this configured to block unapproved connections by default?

6. Is a standard build image used to configure new workstations, does this image include the policies, controls and software required to protect the workstation, and is the image kept up-to-date with corporate policies?

7. Do you have a backup policy in place and are backups regularly taken to protect against threats such as ransomware?

8. Are security and event logs maintained on servers, workstations and laptops?

Access Control

1. Are user account requests subject to proper justification, provisioning and an approvals process and assigned to named individuals?

2. Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?

3. Are accounts removed or disabled when no longer required?

4. Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorized individuals?

5. Are special access privileges documented and reviewed regularly (e.g. quarterly)?

6. Are all administrative accounts only permitted to perform administrator activity with no Internet or external email permissions?

7. Does your password policy enforce changing administrator passwords at least every 60 days to a complex password?

Malware Protection

1. Please confirm that malware protection software has been installed on at least all computers with an ability to connect outside of the network(s) in the scope of this survey.

2. Does corporate policy require all malware protection software to have all engine updates applied, and is this applied rigorously?

3. Have all malware signature files been kept up to date (through automatic updates or through centrally managed deployment)?

4. Has malware been configured for on-access scanning and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning?

5. Has malware protection software been configured to run regular (at least daily) scans?

6. Are users prevented from running executable code or programs from any media to which they also have write access?

7. Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function?

Patch Management

1. Is all software installed on computers and network devices in the scope licensed and supported?

2. Are all operating system security patches applied within 14 days of release?

3. Are all application software security patches applied within 14 days of release?

4. Is all legacy or unsupported software isolated, disabled or removed from devices within the scope?

5. Is a mobile working policy in force that requires mobile devices (including BYOD) to be kept up to date with vendor updates and app patches?

Other Information

Include any other information that may be pertinent to this survey or that can assist with clarifying any matter related to the cyber security within the business.

Appendix D: Initial Cyber Security Assessment Report Template

[Name of Project]

Initial Cyber Security Assessment Report

A preliminary report to determine initial requirements for cyber security assessment plan.

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Contents

Confidentiality Statement .... *LXXI*
Introduction .... *LXXI*
Organization Identification .... *LXXII*
Scope .... *LXXII*
Firewalls and Gateways .... *LXXII*
Secure Configuration .... *LXXII*
Access Control .... *LXXII*
Malware Protection .... *LXXII*
Patch Management .... *LXXIII*
Other Information .... *LXXIII*

Confidentiality Statement

All information gathered by this survey will be used for the sole purpose of designing an appropriate Project Management Plan and/or Statement of Work in order to carry out a full cyber security assessment at the business or organization in question and within the defined scope.

No personal, confidential, privileged or proprietary information will be released, disclosed, reproduced or otherwise used.

Introduction

[Give a brief description of the purpose of this report and additional background information.]

This Initial Assessment Report is based on a survey that was comprised of a series of questions in six different subject areas related to business function and cyber security. It is designed to:

1. Determine the state of readiness of the business or organization or its state of readiness in terms of cyber security.
2. The size of the business and organization and its resources.

This information in this Initial Assessment Report will be used to design a Statement of Work and Assessment Management Plan.

[Add any other information relevant to this section.]

Organization Identification

Organization Name	
Parent Organization Name	
Brief Description	
Product or Service	
No. of Employees	
Contact Person Name	
Contact Person Job Title	
Contact Person Email Address	
Contact Person Telephone Number	

Scope

[Outline information about the scope of the organization relevant to the scope of the proposed assessment.]

Firewalls and Gateways

[Outlines information related to firewalls and gateways relevant to the scope of the proposed assessment.]

Secure Configuration

[Outline information related to secure configuration relevant to the scope of the proposed assessment.]

Access Control

[Outline information related to access control relevant to the scope of the proposed assessment.]

Malware Protection

[Outline information related to malware protection relevant to the scope of the proposed assessment.]

Patch Management

[Outline information related to patch management relevant to the scope of the proposed assessment.]

Other Information

[Include any other information that may be pertinent to this survey or that can assist with clarifying any matter related to the cyber security within the organization.]

Appendix E: Statement of Work Template

[Name of Project]

Statement of Work

Agreement # [N] to provide Cyber Security Assessment Services to [Organization].

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Contents

Introduction .... *LXXVIII*

Background Information .... *LXXVIII*

Current Environment LXXVIII

Goals and Objectives LXXVIII

Scope of Work .... *LXXVIII*

Deliverables LXXVIII

Milestones LXXIX

Period of Performance .... *LXXIX*

Place of Performance .... *LXXIX*

Applicable Standards .... *LXXIX*

Specific Requirements .... *LXXIX*

Resource Requirements .... *LXXIX*

Human Resources LXXIX

Other Resources LXXIX

Service Provider Responsibilities .... *LXXX*

Client Responsibilities .... *LXXX*

Risks .... *LXXX*

Assumptions .... *LXXX*

Completion Criteria .... *LXXX*

Change Control Procedure .... *LXXX*

Contracting and Payment Procedures .... *LXXX*

Other Information and Supporting Documents .... *LXXXI*

Points of Contact .... *LXXXI*

Acceptance .... *LXXXI*

Introduction

[Provide a short description of what is being sought without listing the specific assessment requirements and objectives.]

Background Information

[Provide context for the assessment. Offer high-level background information that describes why the product or service is needed. Describe how did the need arise and its relation to other assessments or activities. From a high level, describe what will be gained by implementing the assessment.]

Current Environment

[Describe the current state of affairs. Include mission and strategic objectives. Describe the current technology, constraints and stakeholders.]

Goals and Objectives

[List the goals and objectives. Include business and solution objectives, technical objectives, service objectives and security objectives.]

Scope of Work

[Describe the assessment work and what it entails. Describe what is included; also describe what is not included in the assessment. Explain what will be accomplished. Describe the size of the effort, special areas of interest and the methods of delivery.]

Deliverables

[List and briefly describe all assessment deliverables.]

Name	Description

Milestones

[List all major milestones and their estimated delivery dates.]

Milestone	Estimated Delivery Date

Period of Performance

[Describe the period of performance for the assessment - how long will the assessment last, on what date or event will it begin and on what date or event will it be completed.]

Place of Performance

[Describe where the assessment work be performed.]

Applicable Standards

[Describe any industry specific standards that should be adhered to.]

Specific Requirements

[List and describe the specific requirements for the assessment.]

Resource Requirements

[Outline the resources required to execute the assessment based on the requirements and available information.]

Human Resources

Name	Title	Knowledge/Skills

Other Resources

Resources

Service Provider Responsibilities

[List and describe the responsibilities of the implementers of the assessment.]

Client Responsibilities

[List and describe the responsibilities of the client.]

Risks

[From a high-level perspective, identify all risks associated with implementing the assessment and explain whether they are known or perceived. Also indicate impact and probability of occurrence.]

Risk	Severity

Assumptions

[List all assumptions made at this point.]

Completion Criteria

[Describe the requirements for the assessment to be considered complete.]

Change Control Procedure

[Describe how and what process will be followed in the event that there are any changes to the Statement of Work.]

Contracting and Payment Procedures

[Describe the contract type, breakdown of costs and payment schedule. Describe the invoice procedures, how often should invoices be remitted, to whom should invoices be remitted.]

Other Information and Supporting Documents

[List any other pertinent information and list and attach any supporting documentation.]

Points of Contact

[Outline contact information from contractor and other pertinent information related to communications.]

Name	Role	Contact information

Acceptance

By initialing each page and signing below, I ________________________________, in my capacity as _______________________________, of ____ agree to and accept the terms set forth in this Statement of Work.

____

Signature

____

Full Name

____

Date

____

Signature (witness)

____

Full Name

____

Date

Appendix F: Assessment Management Plan Template

[Name of Project]

Cyber Security Assessment Management Plan

[A brief statement describing the assessment being done.]

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Distribution History

[Provide information on the distribution of the various versions of the Project Management Plan.]

Version Number	[Stakeholder 1]	[Stakeholder 2]	[Stakeholder 3]	[Stakeholder 4]	[Stakeholder 5]	[Stakeholder 6]	[Stakeholder 7]	[Stakeholder 8]	[Stakeholder 9]	[Stakeholder 10]	[Stakeholder 11]	[Stakeholder 12]

Executive Summary

[Elaborate on the project in brief; incorporate information from the Project Charter if necessary. Provide a summary of the assessment and the assessment plan.]

Assessment Management Plan Approval

We, the undersigned, acknowledge that we have reviewed *Version [Version Number]* of Assessment Management Plan for *[Name of Project]* and that we approve of and agree with the approach and information that it presents.

Any changes to this Project Management Plan will be carried out as described in the Issues and Change Management Section.

Any newer versions of the Assessment Management Plan, once approved, supersedes all older versions.

Authorization 1 of 3:

Signature	
Full Name (Print)	
Date	
Title	
Role	

Authorization 2 of 3:

Signature	
Full Name (Print)	
Date	
Title	
Role	

Authorization 3 of 3:

Signature	
Full Name (Print)	
Date	
Title	
Role	

[Add or remove as many signatories as necessary.]

Contents

Introduction .... *LXXXIX*
Scope and Cost .... *LXXXIX*
Schedule .... *LXXXIX*
Stakeholder Management .... *LXXXIX*
Stakeholder Analysis LXXXIX
Stakeholder Management Plan LXXXIX
Assessment Team Management .... *LXXXIX*
Communication Management .... *XC*
Communication Interactions XC
Forms of Communication XC
Risk Management .... *XC*
Risk Analysis XC
Risk Management Plan XC
Quality Management .... *XC*
Issue and Change Management .... *XC*
Issue Management Plan XC
Change Management Plan XC
Closing .... *XC*

Introduction

[Provide an introduction and background information on the client organization as well as any other information that may serve to introduce the assessment plan.]

Scope and Cost

[The Scope and Cost Section determines and documents a list of specific assessment goals, deliverables, features, functions, tasks, deadlines and associated costs. These should be clearly listed.]

[A basic table or spreadsheet can be used to display and demonstrate what the costs of the assessment are.]

Schedule

[The schedule is a listing of the assessment's milestones, activities and deliverables usually with intended start and finish dates.]

[To develop the schedule, a work breakdown structure is created based on the requirements or the project. A timeline with milestones, activities, and deliverables dates is then formulate; a Gantt chart can be used in this case.]

Stakeholder Management

Stakeholder Analysis

[Outline who the stakeholders are and determine level of interest and influence.]

Stakeholder Management Plan

[Describe how stakeholders will be managed based on influence and level of interest.]

Assessment Team Management

[Formulate who will be a part of the assessment team based on the requirements of the project. Describe reporting structure, roles and responsibilities.]

Communication Management

Communication Interactions

[Describe who communicates with whom.]

Forms of Communication

[Describe what kind of communications will be used and with who.]

Risk Management

Risk Analysis

[Identify and categorize risks.]

Risk Management Plan

[Describe how risk will be managed, i.e. what measures will be taken for each risk.]

Quality Management

[Determine what are the quality standards being used and describe how quality will be maintained.]

Issue and Change Management

Issue Management Plan

[Describes how issues will be communicated and managed.]

Change Management Plan

[Describes how changes will communicated and managed.]

Closing

[Provides a sequence of steps that must be taken to close the assessment successfully. Most of these steps are defined in the Assessment Management Methodology but may vary from assessment to assessment.]

Appendix G: Information and Communications Technology Inventory Control Template

[Name of Project]

Information and Communications Technology Inventory Control

Principal deliverable of the cyber security assessment.

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver’s Name	Approver’s Signature	Approval Date

Contents

About This Document .... *XCV*
Inventory .... *XCVI*
Notes .... *XCVII*

About This Document

This document provided a listing of all Information and Communications Technology Equipment (ICT) that the assessment team has identified as being pertinent to the results of the assessment.

These form the core of the assessment of cyber threat at the organization.

Inventory

The following table is a listing of all information and communications technology equipment related to the assessment:

Workstation/Functional Area	Device Description	Model/Make	Serial No.	Status/Comment

Notes

[List important notes and other information here.]

Appendix H: Cyber Security Risk Analysis Template

[Name of Project]

Cyber Security Risk Analysis

Principal deliverable of the cyber security assessment

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Contents

About This Document ... *CII*

Risk and Observation Tables ... *CIII*

Identify ... CIV

Protect ... CV

Detect ... CVII

Respond ... CVII

Recover ... CVIII

Risk Categorization ... *CIX*

Risk Response ... *CX*

High Risk ... CX

Moderate Risk ... CX

Low Risk ... CX

About This Document

Risk analysis is a key part of a cyber security strategy. This document lays out a cyber security risk analysis of *[Name of Client Organization]* that complements the Current and/or Target Cyber Security Profiles that are a part of *[Name of Project]*.

[Insert any other pertinent information.]

Risk and Observation Tables

The observation tables are used to make note of and categorize risk in line with the guidelines set out by the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. The information gathered can be used in other parts of the assessment and as a part of the final assessment report.

The following legend is used as guidance for the five subsequent sections of this document representing the Identify, Protect, Detect, Respond and Recover functions:

Function	Aggrupation of subcategorizes to be analyzed.
Category	Categorization of functions.
Subcategory	Particular action to be taken or issue to be addressed.
Probability	A numerical value that represents the likelihood that an adverse event in the particular subcategory will occur. See Probability Levels Table.
Impact	A numerical value that represents the (typically negative) effect that the particular subcategory. See Impact Levels Table.
Risk (PxI)	Numerical valuation of the probability that event will occur multiplied by impact of said event.
Reference	Guideline, standard or practice will be use to address the particular need.
Comment/Observations	Any comment or note with regards to the subcategory.

The following table represents levels of probabilities and their numerical equivalent for the five sections representing the Identify, Protect, and Detect, Respond and Recover functions:

Probability of Occurrence Levels		
Numerical Equivalent	**Likelihood**	**Description**
0.1	**Negligible**	Unlikely ever to occur.
0.28	**Very Low**	Likely to occur two/three times every five years.
0.46	**Low**	Likely to occur once every year or less.
0.64	**Medium**	Likely to occur once every six months or less.
0.82	**High**	Likely to occur once per month or less.
1.0	**Very High**	Likely to occur multiple times per month.

The following table represents levels of impact severity and their numerical equivalent for the five sections representing the Identify, Protect, Detect, Respond and Recover functions:

Impact Severity Levels		
Numerical Equivalent	**Likelihood**	**Description**
0.1	**Insignificant**	Little or no impact.
0.28	**Minor**	Minimal effort to repair, restore or reconfigure.
0.46	**Significant**	Small but tangible harm, maybe noticeable by a limited audience, some embarrassment, some effort to repair.
0.64	**Damaging**	Damage to reputation, loss of confidence, significant effort to repair.
0.82	**Serious**	Considerable system outage, loss of connected customers, business confidence, compromise of large amount information.
1.0	**Critical**	Extended outage, permanent loss of resource, triggering business continuity procedures, complete compromise of information.

Identify

The Identify Function develops the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.

The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
IDENTIFY (ID)	**ID.AM**	**ID.AM-1**				
		ID.AM-2				
		ID.AM-3				
		ID.AM-4				
		ID.AM-5				
		ID.AM-6				
	ID.BE	**ID.BE-1**				

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
		ID.BE-2				
		ID.BE-3				
		ID.BE-4				
		ID.BE-5				
	ID.GV	ID.GV-1				
		ID.GV-2				
		ID.GV-3				
		ID.GV-4				
	ID.RA	ID.RA-1				
		ID.RA-2				
		ID.RA-3				
		ID.RA-4				
		ID.RA-5				
		ID.RA-6				
	ID.RM	ID.RM-1				
		ID.RM-2				
		ID.RM-3				

Protect

The Protect Function develops and implements the appropriate safeguards to ensure delivery of critical infrastructure services.

It supports the ability to limit or contain the impact of a potential cyber security event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
PROTECT (PR)	PR.AC	PR.AC-1				
		PR.AC-2				
		PR.AC-3				
		PR.AC-4				

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
		PR.AC-5				
	PR.AT	PR.AT-1				
		PR.AT-2				
		PR.AT-3				
		PR.AT-4				
		PR.AT-5				
	PR.DS	PR.DS-1				
		PR.DS-2				
		PR.DS-3				
		PR.DS-4				
		PR.DS-5				
		PR.DS-6				
		PR.DS-7				
	PR.IP	PR.IP-1				
		PR.IP-2				
		PR.IP-3				
		PR.IP-4				
		PR.IP-5				
		PR.IP-6				
		PR.IP-7				
		PR.IP-8				
		PR.IP-9				
		PR.IP-10				
		PR.IP-11				
		PR.IP-12				
	PR.MA	PR.MA-1				
		PR.MA-2				
	PR.PT	PR.PT-1				
		PR.PT-2				
		PR.PT-3				
		PR.PT-4				

Detect

The Detect Function develops and implements the appropriate activities to identify the occurrence of a cyber security event.

It enables timely discovery of cyber security events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
DETECT (DE)	DE.AE	DE.AE-1				
		DE.AE-2				
		DE.AE-3				
		DE.AE-4				
		DE.AE-5				
	DE.CM	DE.CM-1				
		DE.CM-2				
		DE.CM-3				
		DE.CM-4				
		DE.CM-5				
		DE.CM-6				
		DE.CM-7				
		DE.CM-8				
	DE.DP	DE.DP-1				
		DE.DP-2				
		DE.DP-3				
		DE.DP-4				
		DE.DP-5				

Respond

Develop and implements the appropriate activities to take action regarding a detected cyber security event.

It supports the ability to contain the impact of a potential cyber security event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
RESPOND (RS)	RS.RP	RS.RP-1				
	RS.CO	RS.CO-1				
		RS.CO-2				
		RS.CO-3				
		RS.CO-4				
		RS.CO-5				
	RS.AN	RS.AN-1				
		RS.AN-2				
		RS.AN-3				
		RS.AN-4				
	RS.MI	RS.MI-1				
		RS.MI-2				
		RS.MI-3				
	RS.IM	RS.IM-1				
		RS.IM-2				

Recover

The Recover Function develops and implements the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.

It supports timely recovery to normal operations to reduce the impact from a cyber security event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
RECOVER (RC)	RC.RP	RC.RP-1				
	RC.IM	RC.IM-1				
		RC.IM-2				
	RC.CO	RC.CO-1				
		RC.CO-2				
		RC.CO-3				

Risk Categorization

The following table further categorizes cyber security risks in terms their levels (high, moderate, low):

		Probability of Occurrence					
		Negligible (0.10)	Very Low (0.28)	Low (0.46)	Medium (0.64)	High (0.82)	Very High (1.00)
Impact Severity	Critical (1.00)	Low	Moderate	High	High	High	High
	Serious (0.82)	Low	Moderate	High	High	High	High
	Damaging (0.64)	Low	Moderate	Moderate	High	High	High
	Significant (0.46)	Low	Low	Moderate	Moderate	High	High
	Minor (0.28)	Low	Low	Low	Moderate	Moderate	Moderate
	Insignificant (0.10)	Low	Low	Low	Low	Low	Low

The follow tables show the numeric values that corresponds to each level (high, moderate, low):

		Probability of Occurrence					
		Negligible (0.10)	Very Low (0.28)	Low (0.46)	Medium (0.64)	High (0.82)	Very High (1.00)
Impact Severity	Critical (1.00)	0.10	0.28	0.46	0.64	0.82	1.00
	Serious (0.82)	0.082	0.2296	0.3372	0.5248	0.6724	0.82
	Damaging (0.64)	0.064	0.1792	0.2944	0.4096	0.5248	0.64
	Significant (0.46)	0.046	0.1288	0.2116	0.2944	0.3772	0.46
	Minor (0.28)	0.028	0.0784	0.1288	0.1792	0.2296	0.28
	Insignificant (0.10)	0.010	0.028	0.046	0.064	0.082	0.10

Risk Response

Risk/Solution pairs are formulated in the following tables in order to formulate a solution to the risk.

High Risk

Function	Category	Subcategory	Risk Description	Solution Description

Moderate Risk

Function	Category	Subcategory	Risk Description	Solution Description

Low Risk

Function	Category	Subcategory	Risk Description	Solution Description

Appendix I: Cyber Security Master Profile

[Name of Project]

Cyber Security Profile

Proposed cyber security stance of the organization based on existing and expected conditions.

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity	**Client Organization**
[Name of Contact Person]	*[Name of Contact Person]*
[Name of Organization]	*[Name of Organization]*
[Address Line 1]	*[Address Line 1]*
[Address Line 2]	*[Address Line 2]*
[Telephone]	*[Telephone]*
[Email Address]	*[Email Address]*

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Contents

About This Document .... *CXV*
1. IDENTIFY (ID) .... *CXVI*
1.1 Asset Management (ID.AM) CXVI
1.2 Business Environment (ID.BE) CXVI
1.3 Governance (ID.GV) CXVII
1.4 Risk Assessment (ID.RA) CXVII
1.5 Risk Management Strategy (ID.RM) CXVII
2. PROTECT (PR) .... *CXVIII*
2.1 Access Control (PR.AC) CXVIII
2.2 Awareness and Training (PR.AT) CXVIII
2.3 Data Security (PR.DS) CXVIII
2.4 Information Protection Processes and Procedures (PR.IP) CXIX
2.5 Maintenance (PR.MA) CXX
2.6 Protective Technology (PR.PT) CXX
3. DETECT (DE) .... *CXX*
3.1 Anomalies and Events (DE.AE) CXX
3.2 Security Continuous Monitoring (DE.CM) CXXI
3.3 Detection Processes (DE.DP) CXXI
4. RESPOND (RS) .... *CXXII*
4.1 Response Planning (RS.RP) CXXII
4.2 Communications (RS.CO) CXXII
4.3 Analysis (RS.AN) CXXII
4.4 Mitigation (RS.MI) CXXII
4.5 Improvements (RS.IM) CXXIII
5. RECOVER (RC) .... *CXXIII*
5.1 Recovery Planning (RC.RP) CXXIII
5.2 Improvements (RC.IM) CXXIII
5.3 Communications (RC.CO) CXXIII

About This Document

This document describes the Cyber Security Profile of *[Name of Client Organization]* as carried out in *[Name of Project]* and is one of the objectives or deliverables as agreed upon at the initiation of the assessment.

A profile represents the functions, categories and subcategories prioritized by an organization based on business needs and can be used to measure the organization's progress toward the it cyber security readiness target.

[Insert any other pertinent information.]

1. IDENTIFY (ID)

1.1 Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to business objectives and the organization's risk strategy.

ID.AM-1
Physical devices and systems within the organization are inventoried.
ID.AM-2
Software platforms and applications within the organization are inventoried.
ID.AM-3
Organizational communication and data flows are mapped.
ID.AM-4
External information systems are catalogued.
ID.AM-5
Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality and business value.
ID.AM-6
Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.

1.2 Business Environment (ID.BE)

The organization's mission, objectives, stakeholders and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities and risk management decisions.

ID.BE-1
The organization's role in the supply chain is identified and communicated.
ID.BE-2
The organization's place in critical infrastructure and its industry sector is identified and communicated.
ID.BE-3
Priorities for organizational mission, objectives and activities are established and communicated.
ID.BE-4
Dependencies and critical functions for delivery of critical services are established.
ID.BE-5
Resilience requirements to support delivery of critical services are established.

1.3 Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental and operational requirements are understood and management are informed of cyber security risk.

ID.GV-1
Organizational information security policy is established.
ID.GV-2
Information security roles & responsibilities are coordinated and aligned with internal roles and external partners.
ID.GV-3
Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed.
ID.GV-4
Governance and risk management processes address cyber security risks.

1.4 Risk Assessment (ID.RA)

The organization understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals.

ID.RA-1
Asset vulnerabilities are identified and documented.
ID.RA-2
Threat and vulnerability information is received from information sharing forums and sources.
ID.RA-3
Threats, both internal and external, are identified and documented.
ID.RA-4
Potential business impacts and likelihoods are identified.
ID.RA-5
Threats, vulnerabilities, likelihoods and impacts are used to determine risk.
ID.RA-6
Risk responses are identified and prioritized.

1.5 Risk Management Strategy (ID.RM)

The organization’s priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.

ID.RM-1
Risk management processes are established, managed and agreed to by organizational stakeholders.
ID.RM-2
Organizational risk tolerance is determined and clearly expressed.

ID.RM-3
The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

2. PROTECT (PR)

2.1 Access Control (PR.AC)

Access to assets and associated facilities is limited to authorized users, processes, or devices and to authorized activities and transactions.

PR.AC-1
Identities and credentials are managed for authorized devices and users.
PR.AC-2
Physical access to assets is managed and protected.
PR.AC-3
Remote access is managed.
PR.AC-4
Access permissions are managed, incorporating the principles of least privilege and separation of duties.
PR.AC-5
Network integrity is protected, incorporating network segregation where appropriate.

2.2 Awareness and Training (PR.AT)

The organization’s personnel and partners are provided with cyber security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-1
All users are informed and trained.
PR.AT-2
Privileged users understand roles & responsibilities.
PR.AT-3
Third-party stakeholders (e.g., suppliers, customers, and partners) understand roles & responsibilities.
PR.AT-4
Senior executives understand roles & responsibilities.
PR.AT-5
Physical and information security personnel understand roles & responsibilities.

2.3 Data Security (PR.DS)

Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity and availability of information.

PR.DS-1
Data-at-rest is protected.
PR.DS-2
Data-in-transit is protected.
PR.DS-3
Assets are formally managed throughout removal, transfers and disposition.
PR.DS-4
Adequate capacity to ensure availability is maintained.
PR.DS-5
Protections against data leaks are implemented.
PR.DS-6
Integrity checking mechanisms are used to verify software, firmware and information integrity.
PR.DS-7
The development and testing environment(s) are separate from the production environment.

2.4 Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-1
A baseline configuration of information technology/industrial control systems is created and maintained.
PR.IP-2
A System Development Life Cycle to manage systems is implemented.
PR.IP-3
Configuration change control processes are in place.
PR.IP-4
Backups of information are conducted, maintained and tested periodically.
PR.IP-5
Policy and regulations regarding the physical operating environment for organizational assets are met.
PR.IP-6
Data is destroyed according to policy.
PR.IP-7
Protection processes are continuously improved.
PR.IP-8
Effectiveness of protection technologies is shared with appropriate parties.
PR.IP-9
Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
PR.IP-10
Response and recovery plans are tested.
PR.IP-11

Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening).

PR.IP-12

A vulnerability management plan is developed and implemented.

2.5 Maintenance (PR.MA)

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

PR.MA-1

Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools.

PR.MA-2

Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access.

2.6 Protective Technology (PR.PT)

Technical security solutions are managed to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements.

PR.PT-1

Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

PR.PT-2

Removable media is protected and its use restricted according to policy.

PR.PT-3

Access to systems and assets is controlled, incorporating the principle of least functionality.

PR.PT-4

Communications and control networks are protected.

3. DETECT (DE)

3.1 Anomalies and Events (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

DE.AE-1

A baseline of network operations and expected data flows for users and systems is established and managed.

DE.AE-2

Detected events are analyzed to understand attack targets and methods.

DE.AE-3

Event data are aggregated and correlated from multiple sources and sensors.
DE.AE-4
Impact of events is determined.
DE.AE-5
Incident alert thresholds are established.

3.2 Security Continuous Monitoring (DE.CM)

The information system and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures.

DE.CM-1
The network is monitored to detect potential cyber security events.
DE.CM-2
The physical environment is monitored to detect potential cyber security events.
DE.CM-3
Personnel activity is monitored to detect potential cyber security events.
DE.CM-4
Malicious code is detected.
DE.CM-5
Unauthorized mobile code is detected.
DE.CM-6
External service provider activity is monitored to detect potential cyber security events.
DE.CM-7
Monitoring for unauthorized personnel, connections, devices, and software is performed.
DE.CM-8
Vulnerability scans are performed.

3.3 Detection Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

DE.DP-1
Roles and responsibilities for detection are well defined to ensure accountability.
DE.DP-2
Detection activities comply with all applicable requirements.
DE.DP-3
Detection processes are tested.
DE.DP-4
Event detection information is communicated to appropriate parties.
DE.DP-5
Detection processes are continuously improved.

4. RESPOND (RS)

4.1 Response Planning (RS.RP)

Response processes and procedures are executed and maintained to ensure timely response to detected cyber security events.

RS.RP-1
Response plan is executed during or after an event.

4.2 Communications (RS.CO)

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

RS.CO-1
Personnel know their roles and order of operations when a response is needed.
RS.CO-2
Events are reported consistent with established criteria.
RS.CO-3
Information is shared consistent with response plans.
RS.CO-4
Coordination with stakeholders occurs consistent with response plans.
RS.CO-5
Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness.

4.3 Analysis (RS.AN)

Analysis is conducted to ensure adequate response and support recovery activities.

RS.AN-1
Notifications from detection systems are investigated.
RS.AN-2
The impact of the incident is understood.
RS.AN-3
Forensics is performed.
RS.AN-4
Incidents are categorized consistent with response plans.

4.4 Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.

RS.MI-1
Incidents are contained.
RS.MI-2
Incidents are mitigated.
RS.MI-3
Newly identified vulnerabilities are mitigated or documented as accepted risks.

4.5 Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RS.IM-1
Response plans incorporate lessons learned.
RS.IM-2
Response strategies are updated.

5. RECOVER (RC)

5.1 Recovery Planning (RC.RP)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cyber security events.

RC.RP-1
Recovery plan is executed during or after an event.

5.2 Improvements (RC.IM)

Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.IM-1
Recovery plans incorporate lessons learned.
RC.IM-2
Recovery strategies are updated.

5.3 Communications (RC.CO)

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

RC.CO-1
Public relations are managed.

RC.CO-2

Reputation after an event is repaired.

RC.CO-3

Recovery activities are communicated to internal stakeholders and executive and management teams.

Appendix J: Final Assessment Report Template

[Name of Project]

Final Assessment Report

Principal deliverable of the cyber security assessment.

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Contents

About This Document ..... *CXXIX*
Introduction ..... *CXXX*
Scope ..... *CXXX*
Methodology ..... *CXXX*
Results ..... *CXXX*
Conclusion ..... *CXXX*
Recommendations ..... *CXXX*
Supporting Documents ..... *CXXX*

About This Document

This document is the main deliverable of *[Name of Project]* along with any other objectives or deliverables as agree upon at the initiation of the assessment.

[Insert any other pertinent information.]

Introduction

[Provide a brief introduction and background information on the organization, its environment, and about the assessment itself.]

[Mention the methodology and the main reference standards, norms and/or frameworks that were used.]

Scope

[Provide an overview of the scope of the project as well a detailed description of objectives.]

Methodology

[Give a sequential rundown of the actions taken to carry out the assessment; describe how the results were obtained.]

Results

[Give a forward to the results and how it ties into the framework being used. The results are essentially divided into two parts: the Cyber Security Risk Analysis and the Cyber Security Profile.]

[The Cyber Security Profile is a complete study of the future, desired state of cyber security readiness at the target (client) organization. This is based on the client's requirements as well as the nature of the organization, the environment, and expert input from the assessment team.]

[The Cyber Security Risk Analysis is a study of the various cyber security risks and how they would impact the organization. This is essentially based on the Cyber Security Profile.]

Conclusion

[The conclusion is derived from the results. It is a presentation of key points and final outcomes. It should synthesize the results and answer the main questions about the assessment.]

Recommendations

[Contains all the recommendations, suggestions and limitations there were observed during the assessment. This is to assist the client to make decisions moving forward.]

Supporting Documents

[Provides a listing and description of all supporting documents, archived and files that is included as a part of the assessment.]

Appendix K: Assessment Closure Document Template

[Name of Project]

Assessment Closure Document

To officially formalize the completion of the cyber security assessment.

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity	**Client Organization**
[Name of Contact Person]	*[Name of Contact Person]*
[Name of Organization]	*[Name of Organization]*
[Address Line 1]	*[Address Line 1]*
[Address Line 2]	*[Address Line 2]*
[Telephone]	*[Telephone]*
[Email Address]	*[Email Address]*

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date

Contents

About This Document .... *CXXXV*
Introduction .... *CXXXVI*
Assessment Scope .... *CXXXVI*
Cost and Resources .... *CXXXVI*
Schedule and Milestones .... *CXXXVI*
Accounting Summary .... *CXXXVI*
Recommendations .... *CXXXVI*
Supporting Documents .... *CXXXVI*
Points of Contact .... *CXXXVI*
Acceptance .... *CXXXVII*

About This Document

This document serves to mark the official completion of *[Name of Project]*. It gives an overview of the deliverables and objectives that are being handed over. It also provides additional information, insights and recommendations that may be useful to the client.

Its key purpose is to formalize the completion of the assessment.

Introduction

[Provide a brief introduction and background information on the organization, its environment and information about the assessment itself.]

Assessment Scope

[Provide an overview of the scope of the project as well as a detailed description of objectives that were delivered. This is the most detailed and important part of this document. All products and deliverables are being handed over must be listed in detail here.]

[During the closing meeting, this document is delivered with the final assessment report in order to successfully close the assessment.]

Cost and Resources

[Provide an overview of the cost incurred and any other resources used (such as human resources) during the course of the project.]

Schedule and Milestones

[Provide an overview of the schedule and major milestones and events that occurred during the execution of the assessment.]

Accounting Summary

[Provide a summary of payments and other financial information that occurred during the assessment as well as information about balance owing and any other contractual arrangement that may be pending, such as final payment for successful completion of the assessment.]

Recommendations

[Provide an overview of all recommendations, suggestions and limitations there were observed during the assessment. This is to assist the client to make decisions moving forward.]

Supporting Documents

[Provide a listing and description of all supporting documents, archived and files that is included.]

Points of Contact

[Provides contact information in case the assessment needs to be discussed further or repeated and to also maintain a clear channel of communication for any other purposes.]

Acceptance

By signing below, I, ____, in my capacity as ______________________________, of ____ acknowledge the completion of this assessment as outlined in this Assessment Closure Document.

Signature	**Signature (witness)**
Full Name	**Full Name**
Date	**Date**

Appendix L: Archive Listing Document Template

[Name of Project]

Archive Listing Document

For the delivery of assessment documentation to client on assessment completion.

Version *[X.X] – [DD/MM/YYYY]*

Executing Entity
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Client Organization
[Name of Contact Person]
[Name of Organization]
[Address Line 1]
[Address Line 2]
[Telephone]
[Email Address]

Version History

[This section provides information on how this document has developed or changed. Use the table below to provide the version number, the author implementing the version or changes, the date of the version, the name of the person approving the version, the date that particular version was approved, finalized or accepted and a brief description of the changes.]

Version Number	**Author/Editor**	**Edits/Changes**	**Approver's Name**	**Approver's Signature**	**Approval Date**

Contents

About This Document .... *CXLII*
Archive Listing .... *CXLIII*
Acceptance .... *CXLIV*

About This Document

This document prefaces all documents that are handed over to the client on completion of *[Name of Project]*. It contains a listing of all documents, archives and files that are attached to it.

It also serves to acknowledge formal verification and acceptance of these documents, archive and files.

Archive Listing

The following table lists all documents that were delivered to client:

Archive	Description	Version Number

Acceptance

By signing below, I, ____, in my capacity as _______________________________, of ____ acknowledge receipt of the archives, documents and files listed in and delivered with this *Archive Listing Document*.

Signature	**Signature (witness)**
Full Name	**Full Name**
Date	**Date**

Appendix 8: Implementation of Cyber Security Assessment of NEMC

CSA - NEMC

Final Assessment Report

Principal deliverable of the cyber security assessment

Version 1.0 – 01/10/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	This is a first iteration of the Final Assessment Report after completion of the assessment.	Douglas Westby		01/10/2018

Contents

About This Document .... *CXLIX*
Introduction .... *CL*
Scope .... *CL*
Methodology .... *CL*
Results .... *CLI*
Conclusion .... *CLII*
Recommendations .... *CLII*
Supporting Documents .... *CLII*

About This Document

This document is the main deliverable of *Cyber Security Assessment of NEMC* along with any other objectives or deliverables as agree upon at the initiation phase of the assessment.

There are various attachments or annexes to this document. Because of this, most of the data found in these annexes are not repeated in this report. In order to get a full picture of the assessment, these documents must be reviewed and used as references.

Introduction

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

The Ministry of Health has a small Information Technology Unit that is unable to provide adequate services to the whole Ministry. Because of this, some units like NEMC have been lagging behind terms of adequate service provision in this area.

Due to the lack of good overall Information Technology (IT) support, it has been surmised that the security aspect of the Information Technology and Communication (ICT) infrastructure of NEMC as well as other areas of the Ministry is lacking.

In order to get a good handle on where NEMC stands in terms of cyber security, it was necessary to implement an assessment of its current ICT infrastructure. Base on this information, was possible to determine the required or target cyber security stance (Cyber Security Profile) of the unit using a risk-based approach. The information gathered will assist the Ministry in being prepared from a broader perspective and will allow for evidence-based decision-making to be made in terms of future investments in ICT costs.

This document provided an overview of the Cyber Security Assessment that was carried out. It contains insights and recommendations on what to do to improve the cyber security. It is expected that the reader will review accompanying documents for more information and details.

Scope

In general terms, the assessment covers the National Engineering & Maintenance Center and its respective ICT infrastructure. This includes physical ICT infrastructure to include computers, networks and other electronic equipment, especially those that connect to any network that the Center has.

The scope is defined in more detailed the agreed upon *Statement of Work* that is included as an annex to this document.

Methodology

The complete methodology use can be found as an attachment to this document. The methodology is well described and contains templates that were used as the basis for most of the documentation produced during the assessment.

The following is a sequential listing of the main tasks that were performed:

1. A *Basic Cyber Security Survey* and an *Initial Cyber Security Assessment Report* was carried

out. This was done to gather initial information for decision making, to present the case for the assessment, as well as formatting the *Statement of Work* and related documents.

2. An *Information and Communications Technology Inventory Control* process was carried out to determine the technology that would form the main part of the assessment.
3. Various interview with staff members and visitors as well as site visits for information gathering were done. This was in order to gather insight and formation about the state of cyber security readiness of the organization.
4. A *Cyber Security Profile* was formulated based on information gathered.
5. A *Cyber Security Risk Analysis* based on the same profile was carried out. The risks were then classified using a weighted classification system based on probability of occurrence and impact should the particular risk manifest itself.
6. The risks were further grouped in three categories: high, moderate, or low – this was with the intention of giving the client the ability to know which aggrupation of risks needed to be addressed and in what order.

Results

The principal results are essentially divided into two main parts: The *Cyber Security Profile* and the *Cyber Security Risk Analysis*.

The *Cyber Security Profile* is a breakdown of the stance that the organization should have based on its functions, environment and needs.

To create the *Cyber Security Profile*, subcategories from the *NIST Cybersecurity Framework* were removed if they are not relevant to the business needs, environment and requirements of the organization being assessed. This then reduces the Framework to a target profile that fits the organization.

The *Cyber Security Risk Analysis* is a study of the various cyber security risks and how they would impact the organization. This analysis is done on the *Cyber Security Profile* of the organization and is essentially looks at what needs to be done to obtain what is expected in terms of cyber security within the scope of the assessment.

After completing the analysis, the results are three separated into Risk Response tables:

a. High Risks – must be addressed immediately.
b. Moderate Risks – must be addressed in the medium term.
c. Low Risks – are not that critical but must be addressed at some point.

The *Risk Response* tables also provide practical solutions to addressing these risks. The solutions are either based on ISO 27000 family as a first choice, then the NIST Standards and so forth. The reason for basing solutions primarily on the ISO 27000 family is that it is expected that this will be the more prevalent standard in Belize and more than likely the one that the Government will adopt.

The full *Cyber Security Risk Analysis* with the *Risk Response* tables section can be found attached. Other important results such as the *Initial Cyber Security Assessment Report* as well the *Information and Communications Technology Inventory Control* are also a part of the results of the assessment and are included.

Conclusion

The main conclusion is that the unit is unprepared in terms of cyber security. In short, nothing has been done in terms of information technology support at NEMC except occasional responsive maintenance from both internal and external sources.

The staff are not trained or versed in information technology, and there appear to be limited resources allocated these activities.

Recommendations

Key recommendations are as follows:

1. All risks (gaps) should be address, especially those that are considered high risk.
2. In order to implement and maintain cyber security solutions, staff must be hired for this particular purpose. Existing IT staff can perform these tasks; however, there may not be sufficient human resources available at the Ministry.
3. The assessment should be repeated at least every year to assess changes in stance and to look at improvement, if any, to cyber security at the organization.

Supporting Documents

All supporting documents are included and listed in the *Archive Listing Document*, including the ones that are of importance to complement this report.

Assessment Charter

Project Identification

Name	*Cyber Security Assessment of the National Engineering & Maintenance Center of the Ministry of Health, Belize*
Description	*Project to carry out a cyber security assessment of the National Engineering & Maintenance Center of the Ministry of Health, Belize.*
Sponsor	*Ministry of Health*
Start Date	*August 6, 2018*
End Date	*October 8, 2018*
Project Manager	*Douglas Westby, P.Eng.*

Background

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

The Ministry of Health has a small Information Technology Unit that is unable to provide adequate services to the whole Ministry. Because of this, some units like NEMC have been lagging behind terms of adequate service provision in this area.

Due to the lack of good overall Information Technology (IT) support, it has been surmised that the security aspect of the Information Technology and Communication (ICT) infrastructure of NEMC is lacking. This may also true for various other units and parts of the Ministry and the wider Government Infrastructure.

In order to get a good handle on where NEMC stands in terms of cyber security, it is necessary to implement an assessment of its current ICT infrastructure. Base on this information, it will be possible to determine the required or target cyber security stance of the unit. This information gather will assist the Ministry in being prepared from a broader perspective and will allow for evidence-based decision making to be made in terms of future investments in ICT costs.

Justification

The primary objective of this endeavor is to carry out a cyber security assessment of NEMC with the objective of determining the existing or current stance or level of preparedness as well as determined the target or future baseline level of preparedness that is required.

Justification

The main benefit of carrying out such an assessment that there will be data available that can be used to make evidence-based decisions on steps that need to be taken to harden IT infrastructure of the unit. Furthermore, the results can be used to justify carrying out the same assessments for other units and parts of the Ministry.

There are other benefits such as having information and inventories about available ICT equipment and devices at unit. Furthermore, the main benefit to the unit is that its members will be aware of what needs to be done in order to strengthen their stance in terms of cyber security.

Scope

In general terms, the assessment will cover the National Engineering & Maintenance Center and its respective ICT infrastructure and functions.

This includes physical ICT infrastructure to include computers, networks and other electronic equipment.

Objectives

The main objective of the assessment is to provide a comprehensive report of the actual cyber security stance of the unit as well as to propose solutions to fill risk gaps based on a weighted risk analysis.

Key Deliverables

Name	Description
Initial Assessment Report	An initial and basic survey of the existing ICT infrastructure in order to better understand schedule, scope and cost and to be able to formulate and better plan the statement of work and the assessment itself.
Final Assessment Report	A report that gives an overview of the main finding and is comprise of the Information and Communications Inventory Control, the Cyber Security Profile and the Cyber Security Risk Analysis of the organization being assessed.
Information and Communications Technology Inventory Control	A log or control of all the equipment and relevant technologies that forms the core of the cyber security needs of the client organization.
Cyber Security Profile	A description of where the organization should be in terms of cyber

Key Deliverables

Name	Description
	security within the framework of its needs and functions.
Cyber Security Risk Analysis	A risk analysis of existing cyber security issues (based on the Cyber Security Profile).

Milestones

Milestone	Date
Delivery of Initial Cyber Security Assessment Report	August 17, 2018
Project Launch Meeting	September 3, 2018
Delivery of Final Report & Supporting Documents	October 1, 2018
Carry Out Closure Meeting	October 8, 2018

Success Criteria

In order for the assessment to be successful, all objectives must be completed as agreed and delivered within the required timeframe. The normal day-to-day functions of the client should be minimally affected.

Resources Required

Human Resources	Other Resources
1. Engineer (Assessor/Project Manager/Team Lead) with technical background in Cyber Security 2. IT/Network Technician (Assistant Assessor) 3. Equipment Auditor	No other major resource is required for this project.

Budget

Since all resource will be source in-house, no budget has been allocated.

Assumptions

1. Employees will be open to the idea of having the assessment done.
2. All the resources required to carry out the assessment will be provided in-house.

Assumptions

3. All the information needed is will be attainable in-house.
4. All permissions to use sensitive or confidential information will be provided.

Constraints

Project must be completed within the allotted timeframe and/or as quickly as possible.

All resources must be acquired in- house (project cost should be minimal or near zero).

Risks

Description	Severity
The information required will not be readily available.	Low
Some members of the unit may not be readily available for interviews.	Medium
Natural disasters (and other force majeure) may hinder or disrupt project.	Medium

Authorization

Sponsor		Project Manager	
Signature		**Signature**	
Full Name	Froylan Uk	**Full Name**	Douglas Westby, P.Eng.
Title	Technical Supervisor, NEMC	**Title**	Technical Advisor, NEMC

Business Case

Project Identification	
Name of Organization	*National Engineering & Maintenance Center, Ministry of Health*
Author	*Douglas Westby, P.Eng.*
Sponsor	*Ministry of Health*
Start Date	*August 6, 2018*
End Date	*October 8, 2018*
Project Manager	*Douglas Westby, P.Eng.*

Executive Summary

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

The Ministry of Health has a small Information Technology Unit that is unable to provide adequate services to the whole Ministry. Because of this, some units like NEMC have been lagging behind terms of adequate service provision in this area.

Due to the lack of good overall Information Technology (IT) support, it has been surmised that the security aspect of the Information Technology and Communication (ICT) infrastructure of NEMC is lacking. This may also true for various other units and parts of the Ministry and the wider Government Infrastructure.

In order to get a good handle on where NEMC stands in terms of cyber security, it is necessary to implement an assessment of its current ICT infrastructure. Base on this information, it will be possible to determine the required or target cyber security stance of the unit. This information gather will assist the Ministry in being prepared from a broader perspective and will allow for evidence-based decision making to be made in terms of future investments in ICT costs.

Justification

The primary objective of this endeavor is to carry out a cyber security assessment of NEMC with the objective of determining the existing or current stance or level of preparedness as well as determined the target or future baseline level of preparedness that is required.

The main benefit of carrying out such as assessment is that there will be data available that can be used to make evidence-based decisions on steps that need to be taken to harden IT infrastructure of the unit, specifically in terms of cyber security. Furthermore, the results can be used to justify carrying out the same assessments for other units and parts of the Ministry.

There are other benefits such as having information and inventories about available ICT equipment and devices at the unit. Furthermore, the main benefit to the unit is that its members will be aware of what needs to be done in order to strengthen their stance in terms of cyber security.

Expected Outcomes

The short-term outcome of the project is having a report that details the cyber security profile of the unit as well as having potential solutions to fill the current cyber security gaps that are perceived to be critical to the safety of the organization.

The long terms outcome is that this information from the assessment will be acted up to strengthen the cyber security stance of the client organization. The information gathered will be disseminated further to the Ministry and Government, primarily to be used as model assessment use case that can be carried out elsewhere.

If the assessment is not carried out, the potential risks will remain undiscovered which will leave the unit and by extension the Ministry vulnerable.

Time, Cost and Scope

The assessment is expected to last for six to eight weeks approximately. The time may vary based on the level of detail that is required.

In terms of scope, the project will cover the National Engineering & Maintenance Center and its ICT respective infrastructure.

The cost is expected to be minimal as resources (primarily human resources) will redistributed internally to carry out assessment. Due the scope of the project, no external consultants or additional resources are required.

Major Risks

The only major risk associated with this project is that the information required will not be readily available. This is primarily because members of the unit may not be available to provide the information needed or they may not have the technical knowledge to do so.

Other risks include the availability of staff to provide information due to existing work commitments, as well as the possible occurrence of natural disasters (and other force majeure) may hinder or disrupt the project.

Approvals

The following (signed) approvals are required for this document:

Name	Title	Signature	Date
Froylan Uk	Technical Supervisor, NEMC		06/08/18

Distribution

This document has been distributed to those listed below:

Name	Title	Signature	Date
Froylan Uk	Technical Supervisor, NEMC		06/08/18

CSA - NEMC

Basic Cyber Security Survey

A preliminary survey to determine initial requirements for cyber security assessment plan

Version 1.0 – 07/08/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	Information from interview process, no changes.	Douglas Westby		07/08/2018

Contents

Confidentiality Statement .... *CLXIII*

Introduction .... *CLXIII*

Instructions .... *CLXIII*

Organization Identification .... *CLXIV*

Scope .... *CLXIV*

Firewall and Gateways .... *CLXV*

Secure Configuration .... *CLXV*

Access Control .... *CLXVI*

Malware Protection .... *CLXVI*

Patch Management .... *CLXVII*

Other Information .... *CLXVII*

Confidentiality Statement

All information gathered by this survey will be used for the sole purpose of designing an appropriate Project Management Plan and/or Statement of Work in order to carry out a full cyber security assessment at the business or organization in question and within the defined scope.

No personal, confidential, privileged or proprietary information will be released, disclosed, reproduced or otherwise used.

Introduction

This survey is comprised of a series of questions in six different subject areas related to business function and cyber security. It is designed to:

1. Determine the state of readiness of the business or organization, or its state of readiness in terms of cyber security.
2. The size of the business and organization and its resources.

This information will then be used to generate an Initial Assessment Report which will then be used to design an appropriate Statement of Work and Project Management Plan.

This most of the questions and subsections in this survey are based on or taken from the *Cyber Essentials Common Questionnaire V1.1.*

Instructions

1. This survey is designed to gather information from IT personnel who have knowledge of the information technology being used and the cyber security policies and practices of the organization.
2. It is important that answers are presented as accurately and as completely as possible.
3. Only answer questions that are applicable to the organization.

Organization Identification

Organization Name	*National Engineering & Maintenance Center*
Parent Organization Name	*Ministry of Health*
Brief Description	*Engineering and maintenance unit of the Ministry of Health*
Product or Services Offered	*Biomedical engineering, building services, transportation and other related technical support services*
No. of Employees	*18*
Contact Person Name	*Froylan Uk*
Contact Person Job Title	*Technical Supervisor*
Contact Person Email Address	*froylan.uk@health.gov.bz*
Contact Person Telephone Number	*+501-652-3453*

Scope

Identify the scope of the systems or subsystems to be assessed under this survey, including locations, network boundaries, management and ownership. Where possible include IP addresses and/or ranges.

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Service and other related technical support services.

The major components of the unit's ICT infrastructure in confined within the main NEMC building in Belize City. However, some users log in remotely from around the country or from home to gain access to information related to work.

The following is a preliminary listing ICT equipment and services:

1. Cloud server for file sharing
2. Workstations and other devices
3. 18 desktops (not all are functional)
4. 3 laptops
5. Various portable devices
6. Various personal (staff) devices
7. 3 network printers
8. 1 fax machine
9. 1 PBX system with various extensions and 2 lines
10. 1 DSL system with router
11. 1 network projector

Scope

Other resources:

1. Various staff email accounts.
2. Various staff accounts connected to information servers and other services.
3. Various pieces of biomedical equipment are connected to the network from time to time.
4. Various remote login service such as Team Viewer, ssh, etc.

In terms of interconnection with the outside world and interchange of information, the unit has a DSL modem, portable media is also used to interchange information.

Firewall and Gateways

1. Have you installed firewalls or similar devices at the boundaries of the networks in the scope?

No.

2. Have the default usernames/passwords on all boundary firewalls (or similar devices) been changed to a strong passwords?

No.

3. Have all open ports and services on each firewall (or similar device) been subject to justification and approval by an appropriately qualified and authorized business representative and has this approval been properly documented?

No.

4. Have all commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOS, tftp, RPC, rlogin, rsh, rexec) been disabled or blocked by default at the boundary firewalls?

No.

5. Confirm that there is a corporate policy requiring all firewall rules that are no longer required to be removed or disabled in a timely manner and that this policy has been adhered to (meaning that there are currently no open ports or services that are not essential for the business).

There is no corporate policy in this regard.

6. Confirm that any remote administrative interfaces has been disabled on all firewall (or similar) devices.

No.

7. Confirm that where there is no requirement for a system to have Internet access, a Default Deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the Internet.

This is not being done.

Secure Configuration

1. Have all unnecessary or default user accounts been deleted or disabled?

No.

2. Confirm that all accounts have passwords, and that any default passwords have been changed to strong passwords.

Some accounts have passwords, but not all of them.

3. Has all unnecessary software, including OS utilities, services and applications, been removed or

disabled?

No, OS installations have all default software.

4. Has the Autorun (or similar service) been disabled for all media types and network file shares?

No.

5. Has a host based firewall been installed on all desktop PCs or laptops and is this configured to block unapproved connections by default?

There is a host based firewall on each computer but it cannot be confirmed that it is being used.

6. Is a standard build image used to configure new workstations, does this image include the policies, controls and software required to protect the workstation, and is the image kept up-to-date with corporate policies?

No.

7. Do you have a backup policy in place and are backups regularly taken to protect against threats such as ransomware?

No.

8. Are security and event logs maintained on servers, workstations and laptops?

No.

Access Control

1. Are user account requests subject to proper justification, provisioning and an approvals process and assigned to named individuals?

No.

2. Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?

No.

3. Are accounts removed or disabled when no longer required?

Not regularly.

4. Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorized individuals?

No.

5. Are special access privileges documented and reviewed regularly (e.g. quarterly)?

No.

6. Are all administrative accounts only permitted to perform administrator activity with no Internet or external email permissions?

There are no restrictions.

7. Does your password policy enforce changing administrator passwords at least every 60 days to a complex password?

No, not at all.

Malware Protection

1. Please confirm that malware protection software has been installed on at least all computers with an ability to connect outside of the network(s) in the scope of this survey.

Yes, for the most part, but this is not checked regularly.

2. Does corporate policy require all malware protection software to have all engine updates applied, and

Malware Protection

is this applied rigorously?

No, there is no policy on this.

3. Have all malware signature files been kept up to date (through automatic updates or through centrally managed deployment)?

For the most part, yes, antiviruses are configured to auto update and scan. However this is not regularly checked by anyone.

4. Has malware been configured for on-access scanning and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning?

For the most part, no.

5. Has malware protection software been configured to run regular (at least daily) scans?

In some cases yes, this is determined by users, there is no policy.

6. Are users prevented from running executable code or programs from any media to which they also have write access?

Almost all users have administrative accounts, so the answer would be no.

7. Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function?

This function does not exist.

Patch Management

1. Is all software installed on computers and network devices in the scope licensed and supported?

No, not always. Most of the major software is licensed, but some of them are not. In some cases, software in installed by users.

2. Are all operating system security patches applied within 14 days of release?

No, not always. In fact, almost never.

3. Are all application software security patches applied within 14 days of release?

No, not always. Almost never unless the software is preconfigured to work this way.

4. Is all legacy or unsupported software isolated, disabled or removed from devices within the scope?

No. This is not being done systematically, unless it affects the functions of the unit.

5. Is a mobile working policy in force that requires mobile devices (including BYOD) to be kept up to date with vendor updates and app patches?

No. In some cases, the devices are unknown.

Other Information

Include any other information that may be pertinent to this survey or that can assist with clarifying any matter related to the cyber security within the business.

Notable points:

1. Most users connect to social media on the network during the course of the day.
2. There are possibilities that outside personnel are connecting the Wi-Fi, especially from hospital that is located in the same compound.
3. Users something log in with other users credentials.

Other Information

Include any other information that may be pertinent to this survey or that can assist with clarifying any matter related to the cyber security within the business.

4. Wi-Fi access is left on at night.

The general conclusion is that good cyber security practices are not being implemented at the National Engineering & Maintenance Center.

CSA - NEMC

Initial Cyber Security Assessment Report

A preliminary report to determine initial requirements for cyber security assessment plan.

Version 1.0 – 17/08/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	Information from interview process, no changes.	Douglas Westby		17/08/2018

Contents

Confidentiality Statement .... *CLXXII*
Introduction .... *CLXXII*
Organization Identification .... *CLXXIII*
Scope .... *CLXXIII*
Firewalls and Gateways .... *CLXXIV*
Secure Configuration .... *CLXXIV*
Access Control .... *CLXXV*
Malware Protection .... *CLXXV*
Patch Management .... *CLXXVI*
Other Information .... *CLXXVI*

Confidentiality Statement

All information gathered by this survey will be used for the sole purpose of designing an appropriate Project Management Plan and/or Statement of Work in order to carry out a full cyber security assessment at the business or organization in question and within the defined scope.

No personal, confidential, privileged or proprietary information will be released, disclosed, reproduced or otherwise used.

Introduction

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

This Initial Assessment Report is a basic analysis of where the unit stands in terms of cyber security. It is not a complete analysis but rather, it lays the groundwork to justify and design a more comprehensive future assessment.

This Initial Assessment Report is based on a survey that was comprised of a series of questions in six different subject areas related to business function and cyber security. It is designed to:

1. Determine the state of readiness of the business or organization or its state of readiness in terms of cyber security.
2. The size of the business and organization and its resources.

This information in this Initial Assessment Report will be used to design a Statement of Work and Assessment Management Plan.

Organization Identification

Organization Name	*National Engineering & Maintenance Center*
Parent Organization Name	*Ministry of Health*
Brief Description	*Engineering and maintenance unit of the Ministry of Health*
Product or Service	*Biomedical engineering, building services, transportation and other related technical support services*
No. of Employees	*18*
Contact Person Name	*Froylan Uk*
Contact Person Job Title	*Technical Supervisor*
Contact Person Email Address	*froylan.uk@health.gov.bz*
Contact Person Telephone Number	*+501-652-3453*

Scope

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Service and other related technical support services.

The major components of the unit's ICT infrastructure in confined within the main NEMC building in Belize City. However, some users log in remotely from around the country or from home to gain access to information related to work.

The following is a preliminary listing ICT equipment and services:

1. Cloud server for file sharing
2. Workstations and other devices
3. 18 desktops (not all are functional)
4. 3 laptops
5. Various portable devices
6. Various personal (staff) devices
7. 3 network printers
8. 1 fax machine
9. 1 PBX system with various extensions and 2 lines
10. 1 DSL system with router
11. 1 network projector

Other resources:

1. Various staff email accounts.

Scope

2. Various staff accounts connected to information servers and other services.
3. Various pieces of biomedical equipment are connected to the network from time to time.

Various remote login service such as Team Viewer, ssh, etc.

In terms of interconnection with the outside world and interchange of information, the unit has a DSL modem, portable media is also used to interchange information.

Firewalls and Gateways

There are no installed firewalls or similar devices at the boundaries of the network in question. Because of this, the answers to the rest of this section are irrelevant.

On a scale of zero to ten, with ten being the highest in terms of readiness in this area (Firewalls and Gateways) and zero implying that there is no implementation of the technology or action does not exist, this section would scores zero out of ten (0/10).

Secure Configuration

For the most part, no unnecessary or default user accounts were deleted or disabled.

Some accounts have passwords, and that some default passwords have been changed to strong passwords.

No unnecessary software, OS utilities, services and applications have been removed or disabled.

Autorun (or similar service) has not been disabled for all media types and network file shares.

There are some host based firewall installed on desktop PCs or laptops but it is uncertain if they are configured to block unapproved connections by default.

A standard build image is not being used to configure new workstations. There are different version of OS's and software on various workstations.

There is no backup policy in place and backups are not being done. Backup of information is at the will of the users of the systems.

There are no security and event logs maintained on servers, workstations and laptops.

On a scale of zero to ten, with ten being the highest in terms of readiness in this area (Secure Configuration) and zero implying that there is no implementation of the technology or action does not exist, this section would scores two out of ten (2/10).

Access Control

User account requests are not subject proper justification, provisioning and an approvals process and assigned to named individuals.

Users are not required to authenticate with a unique username and strong password before being granted access to computers and applications.

Accounts are not regularly removed or disabled when no longer required.

There are no defined restrictions on elevated or special access privileges, such as system administrator accounts.

Special access privileges are not documented and reviewed regularly

Administrative accounts are not required to perform administrator activity with no Internet or external email permissions.

There is no password policy that enforces changing administrator passwords.

On a scale of zero to ten, with ten being the highest in terms of readiness in this area (Access Control) and zero implying that there is no implementation of the technology or action does not exist, this section would scores one out of ten (1/10).

Malware Protection

Malware protection software has been installed on most computers with an ability to connect outside of the network(s) in the scope of this survey.

No policy exists that requires that all malware protection software engine are updated regularly.

In some cases, malware signature files been kept up to date but not through a centrally managed system. Furthermore, only some of the computers are kept up to date. Some antivirus software is configured to auto update and scan.

Malware been configured for on-access scanning when downloading or opening files, opening folders on removable or remote storage and web pages.

For the most part, malware protection software not been configured to run regularly. In some cases this is being done but this is determined by users, there is no policy.

Users are not prevented from running executable code or programs from any media to which they

Malware Protection

also have write access. Almost all users have administrative accounts.

No blacklisting functions exist that prevent users from accessing known malicious web sites.

This function does not exist. On a scale of zero to ten, with ten being the highest in terms of readiness in this area (Malware Protection) and zero implying that there is no implementation of the technology or action does not exist, this section would scores two out of ten (2/10).

Patch Management

Most of the major software are licensed, but some of them are not. In some cases, software in installed by users who use pirated versions.

Operating system security patches applied unless necessary to make a certain application function.

Application software security patches are not always applied within 14 days of release. Patching is almost never unless the software is preconfigured to work this way.

Legacy or unsupported software isolated are not disabled or removed from devices. This is not done unless it affects the functions of the unit.

There are no mobile working policy in force that requires mobile devices (including BYOD) to be kept up to date with vendor updates and app patches.

On a scale of zero to ten, with ten being the highest in terms of readiness in this area (Patch Management) and zero implying that there is no implementation of the technology or action does not exist, this section would scores one out of ten (1/10).

Other Information

Notable points:

1. Most users connect to social media on the network during the course of the day.
2. There are possibilities that outside personnel are connecting the Wi-Fi, especially from hospital that is located in the same compound.
3. Users something log in with other users credentials.
4. Wi-Fi access is left on at night.

The general conclusion is that good cyber security practices are not being implemented at the National Engineering & Maintenance Center.

CSA - NEMC

Statement of Work

Agreement #1 to provide Cyber Security Assessment Services to the National Engineering & Maintenance Center of the Ministry of Health.

Version 1.0 – 03/09/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	Statement of work information, used information from Project Charter, etc.	Douglas Westby		03/09/2018

Contents

Introduction .... *CLXXX*

Background Information .... *CLXXX*

Current Information and Communications Technology Environment CLXXX

Goals and Objectives CLXXXI

Scope of Work .... *CLXXXI*

Deliverables CLXXXI

Milestones CLXXXII

Period of Performance .... *CLXXXII*

Place of Performance .... *CLXXXII*

Applicable Standards .... *CLXXXII*

Specific Requirements .... *CLXXXIII*

Resource Requirements .... *CLXXXIII*

Human Resources CLXXXIII

Other Resources CLXXXIII

Service Provider Responsibilities .... *CLXXXIII*

Client Responsibilities .... *CLXXXIII*

Risks .... *CLXXXIV*

Assumptions .... *CLXXXIV*

Completion Criteria .... *CLXXXIV*

Change Control Procedure .... *CLXXXIV*

Contracting and Payment Procedures .... *CLXXXV*

Other Information and Supporting Documents .... *CLXXXV*

Points of Contact .... *CLXXXV*

Introduction

In order to conduct a cyber security assessment of the National Engineering & Maintenance Center, it is necessary to define assessment-specific activities, deliverables and timelines of the services that will be provided.

This document provided and formalizes the scope of proposed assessment as we all more detailed information in terms of obligations from client as well as service providers and expands on the charter previously created for this assessment.

Formal acceptance of this document by authorized signature implies that the assessment will proceed as defined in this document.

Background Information

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

The Ministry of Health has a small Information Technology Unit that is unable to provide adequate services to the whole Ministry. Because of this, some units like NEMC have been lagging behind terms of adequate service provision in this area.

Due to the lack of good overall Information Technology (IT) support, it has been surmised that the security aspect of the Information Technology and Communication (ICT) infrastructure of NEMC is lacking. This may also true for various other units and parts of the Ministry and the wider Government Infrastructure.

In order to get a good handle on where NEMC stands in terms of cyber security, it is necessary to implement an assessment of its current ICT infrastructure. Base on this information, it will be possible to determine the required or target cyber security stance of the unit using a risk-based approach. The information gathered will assist the Ministry in being prepared from a broader perspective and will allow for evidence-based decision making to be made in terms of future investments in ICT costs.

Current Information and Communications Technology Environment

NEMC is composed of a single location in Belize City. In terms of physical infrastructure, there is a main building and some adjoining support services building.

In terms of ICT infrastructure, most functions are confined to the main building except in cases where communications occur from outside (elsewhere). This would normally be information via email as well as data exchange from field technicians and maintenance staff located in major public health facilities in various locations around the country.

NEMC offers critical maintenance services to all public health facilities. In this regard, equipment and information passes in and out of the facility frequently.

Goals and Objectives

The main goal is to carry out a cyber security assessment of NEMC. The objective is to prepare comprehensive reports of the current and target stance of cyber security readiness of the unit.

The current and future stance are the actual cyber security state of the unit as well as a proposed baseline that is improved and consistent with the functions of the unit and how it fits into the broader Ministry of Health functions.

Scope of Work

In general terms, the assessment will cover the National Engineering & Maintenance Center and its ICT respective infrastructure. This includes physical ICT infrastructure to include computers, networks and other electronic equipment.

Deliverables

The follow table lists all major deliverables for this assessment:

Name	Description
Initial Assessment Report	An initial and basic survey of the existing ICT infrastructure in order to better understand schedule, scope and cost and to be able to formulate and better plan the statement of work and the assessment itself.
Final Assessment Report	A report that gives an overview of the main finding and is comprise of the Information and Communications Inventory Control, the Cyber Security Profile and the Cyber Security Risk Analysis of the organization being assessed.
Information and Communications Technology Inventory Control	A log or control of all the equipment and relevant technologies that forms the core of the cyber security needs of the client organization.
Cyber Security Profile	A description of where the organization should be in terms of cyber security within the framework of its needs and functions.
Cyber Security Risk Analysis	A risk analysis of existing cyber security issues (based on the Cyber Security Profile).

Milestones

The follow table lists all major milestone for this assessment:

Milestone	Estimated Delivery Date
Delivery of Initial Cyber Security Assessment Report	August 17, 2018
Project Launch Meeting	September 3, 2018
Delivery of Final Report & Supporting Documents	October 1, 2018
Carry Out Closure Meeting	October 8, 2018

Period of Performance

This initial stages of the assessment commenced on August 1, 2018. During this time, the following document and tasks were performed:

1. Creation of a Business Case Document
2. Creation of an Assessment Charter
3. Basic Cyber Security Survey
4. Initial Cyber Security Assessment

Upon signing of this Statement of Work, the actual Cyber Security Assessment will commence on the September 3, 2018.

The main deliverables, the Final Reports, are expected to be delivered on October 1, 2018.

The Assessment officially closes on the October 8, 2018 with the Closure Meeting to be hold on the same day.

Place of Performance

The Assessment will be performed in and near to the NEMC main offices in Belize City.

Applicable Standards

The main standards that will be adhered to are:

1. The NIST Cyber Security Framework and supporting documents.
2. The Project Management Institute Body of Knowledge and supporting documents.
3. Any other standard that may become relevant and necessary to use during the course of the Assessment.

Specific Requirements

There are no specific or special requirements for this project except for those that are already outlined in this Statement of Work.

Resource Requirements

Based on the scope of the project, the resource requirements are not significant. They are described the following subsections.

Human Resources

Name	Title	Knowledge/Skills
Douglas Westby	Engineer (Assessor/Project Manager/Team Lead)	Information Technology, Computer Networks, Cyber Security, Project Management
James Castillo	IT/Network Technician (Assistant Assessor)	Information Technology, Computer Networks, Cyber Security, Project Management
Brent Hernandez	Equipment Auditor	Inventory Keeping, Institutional Regulations, Information Technology

Other Resources

Resources
1. Network analyzers.
2. Computers and other devices to record data.
3. Assessment software and tools.

Service Provider Responsibilities

The following are a list of activities that the Service Provider is responsible for:

1. Provide an in-depth assessment of the National Engineering and Maintenance Center based on the NIST Cyber Security Framework.
2. Provide deliverables as agreed in the *Statement of Work*.
3. Protect the confidentiality of the Client.
4. Response in a timely and professional manner.

Client Responsibilities

The following are a list of activities that the Client is responsible for:

1. Provide access to information by assessors.

2. Provide physical access and access to hardware as needed.
3. Provide access to staff for interviewing and information exchange.
4. Response in a timely and professional manner.

Risks

Risk	Severity
The information required will not be readily available.	Low
Some members of the unit may not be readily available for interviews.	Medium
Natural disasters (and other force majeure) may hinder or disrupt project.	Medium

Assumptions

1. Employees will be open to the idea of having the assessment done.
2. All the resources required to carry out the assessment will be provided in-house.
3. All the information needed is will be attainable in-house.
4. All permissions to use sensitive or confidential requirements will be provided.

Completion Criteria

In order for the assessment to be successful, the final report must be delivered within the required timeframe. The normal day-to-day functions of the unit should be minimally affected.

Change Control Procedure

The change control procedures in this section describes the management of changes to this Statement of Work as well as any changes or issues that must be managed during the course of the assessment.

Changes to the Statement of Work or any other aspect of the assessment can occur when both Client and Service Provider agree that it is necessary.

The following outlines the Change Control Procedure.

1. Points of Contact from both sides will contact each other via email provided for any issue or any change requests.
2. Response will be within one working day (24 hours) and agreement (or no objection) is to be obtained within one working day (24 hours) via email (those provided in *Points of Contact* section).
3. Modified Statement of Work reflecting agreed upon changes is to be updated and re-signed within one working day (24 hours). A newer Statement of Work supersedes any older statement of work.

Contracting and Payment Procedures

Since the assessment will be implemented internally, there is no specific contracting and payment procedure except for any already establish allowances for subsistence and overtime as well as exemption from normal day-to-day activities by assessors as needed.

Other Information and Supporting Documents

The Assessment Management Plan that includes the tentative Work Breakdown Structure, Schedule will be provide after this document is officially approved. These documents are subject to changes base on Change Control Procedure outlined in this Statement of Work.

Points of Contact

Name	Role	Contact information
Douglas Westby	Assessor/Project Manager/Team Lead	Douglas Westby +501-610-6465 dwestby@health.gov.bz
Froylan Uk	Client's Focal Point	Froylan Uk +501-223-0511/223-5223 nemc@health.gov.bz

Acceptance

By initialing each page and signing below, I, ___Froylan Uk___, in my capacity as ___Technical Supervisor___, of the ___National Engineering and Maintenance Center, Ministry of Health___ agree to and accept the terms set forth in this *Statement of Work*.

Signature	**Signature (witness)**
Froylan Uk, Technical Supervisor	Anika Perez, First Class Clerk
Full Name	**Full Name**
03/09/18	03/09/18
Date	**Date**

CSA - NEMC

Cyber Security Assessment Management Plan

Project Management Plan to Cyber Security Assessment Services to the National Engineering & Maintenance Center of the Ministry of Health

Version 1.0 – 03/09/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	First iteration of the assessment management plan.	Douglas Westby		03/09/2018

Distribution History

This table provides information on the distribution of the various versions of the *Assessment Management Plan*.

Version Number	[Stakeholder 1]	[Stakeholder 2]	[Stakeholder 3]	[Stakeholder 4]	[Stakeholder 5]	[Stakeholder 6]	[Stakeholder 7]	[Stakeholder 8]	[Stakeholder 9]	[Stakeholder 10]	[Stakeholder 11]	[Stakeholder 12]
1.0												

Executive Summary

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

The Ministry of Health has a small Information Technology Unit that is unable to provide adequate services to the whole Ministry. Because of this, some units like NEMC have been lagging behind terms of adequate service provision in this area.

Due to the lack of good overall Information Technology (IT) support, it has been surmised that the security aspect of the Information Technology and Communication (ICT) infrastructure of NEMC is lacking. This may also true for various other units and parts of the Ministry and the wider Government Infrastructure.

In order to get a good handle on where NEMC stands in terms of cyber security, it is necessary to implement an assessment of its current ICT infrastructure. Base on this information, it will be possible to determine the required or target cyber security stance of the unit. This information gather will assist the Ministry in being prepared from a broader perspective and will allow for evidence-based decision making to be made in terms of future investments in ICT costs.

Assessment Management Plan Approval

We, the undersigned, acknowledge that we have reviewed Version 1.0 of *Assessment Management Plan* for *Cyber Security Assessment of NEMC* and that we approve of and agree with the approach and information that it presents.

Any changes to this project management plan will be carried out as described in the Issues and Change Management Section.

Any newer versions of the *Assessment Management Plan*, once approved, supersedes all older versions.

Authorization 1 of 3:

Signature	
Full Name (Print)	
Date	
Title	
Role	

Authorization 2 of 3:

Signature	
Full Name (Print)	
Date	
Title	
Role	

Authorization 3 of 3:

Signature	
Full Name (Print)	
Date	
Title	
Role	

Contents

Introduction .... *CXCII*

Scope and Cost .... *CXCII*

Scope........ CXCII

Cost CXCIII

Schedule .... *CXCIII*

Work Breakdown Structure CXCIV

Timeline CXCVI

Stakeholder Management .... *CXCVI*

Stakeholder Analysis........ CXCVI

Stakeholder Management Plan CXCVII

Assessment Team Management........ *CXCVII*

Assessment Team Requirements CXCVII

Assessment Team Management Plan........ CXCVIII

Communication Management .... *CXCVIII*

Communication Interactions CXCVIII

Forms of Communication CXCVIII

Risk Management .... *CXCIX*

Risk Analysis........ CXCIX

Risk Management Plan CXCIX

Quality Management........ *CC*

Issue and Change Management........ *CC*

Issue Management Plan CC

Change Management Plan........ CC

Closing........ *CC*

Introduction

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

The Ministry of Health has a small Information Technology Unit that is unable to provide adequate services to the whole Ministry. Because of this, some units like NEMC have been lagging behind terms of adequate service provision in this area.

Due to the lack of good overall Information Technology (IT) support, it has been surmised that the security aspect of the Information Technology and Communication (ICT) infrastructure of NEMC is lacking. This may also true for various other units and parts of the Ministry and the wider Government Infrastructure.

In order to get a good handle on where NEMC stands in terms of cyber security, it is necessary to implement an assessment of its current ICT infrastructure. Base on this information, it will be possible to determine the required or target cyber security stance of the unit using a risk-based approach. The information gathered will assist the Ministry in being prepared from a broader perspective and will allow for evidence-based decision making to be made in terms of future investments in ICT costs.

This document provided a roadmap to successfully execute, monitor and control and close the proposed Cyber Security Assessment. Please refer to Statement of Work (attached copy) for more information.

Formal acceptance of this document by authorized signature implies that the assessment will proceed as defined in this document.

Scope and Cost

Scope

The scope of the project is to conduct a Cyber Security Assessment based as defined in the *Statement of Work*. The scope is further broken down as follows base Basic Cyber Security Survey that was previously done:

The major components of the unit’s ICT infrastructure in confined within the main NEMC building in Belize City. However, some users log in remotely from around the country or from home to gain access to information related to work.

The following is a preliminary listing ICT equipment and services:

1. Cloud server for file sharing
2. Workstations and other devices
3. 18 desktops (not all are functional)
4. 3 laptops
5. Various portable devices
6. Various personal (staff) devices
7. 3 network printers
8. 1 fax machine
9. 1 PBX system with various extensions and 2 lines
10. 1 DSL system with router
11. 1 network projector

Other resources:

1. Various staff email accounts.
2. Various staff accounts connected to information servers and other services.
3. Various pieces of biomedical equipment are connected to the network from time to time.
4. Various remote login service such as Team Viewer, ssh, etc.

In terms of interconnection with the outside world and interchange of information, the unit has a DSL modem, portable media is also used to interchange information.

Cost

The Assessment will be implemented internally; cost will be absorbed in operational costs. Any already establish allowances for subsistence and overtime as well as exemption from normal day-to-day activities by assessors as needed will be provided based on already established Government compendium of allowances.

Schedule

The assessment is broken down and placed in a timeline. The Work Breakdown Structure give a detailed breakdown of how work is divided. The Schedule outlines the sequence of events that will carried to complete the project.

Work Breakdown Structure

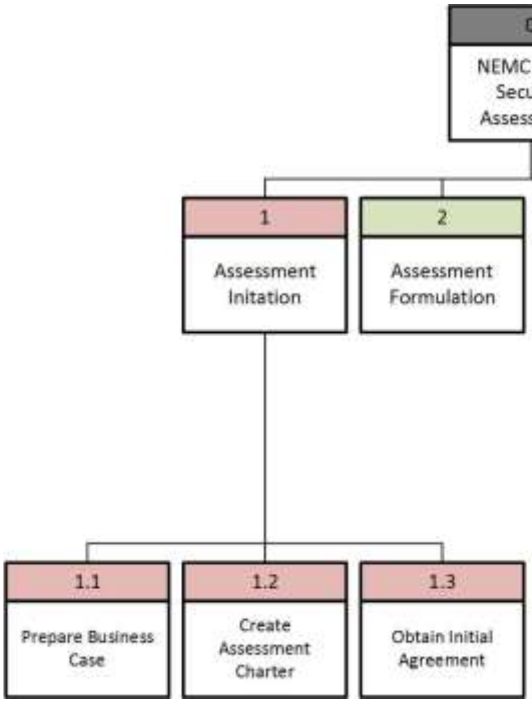


Figure 9 Assessment Initiation breakdown.

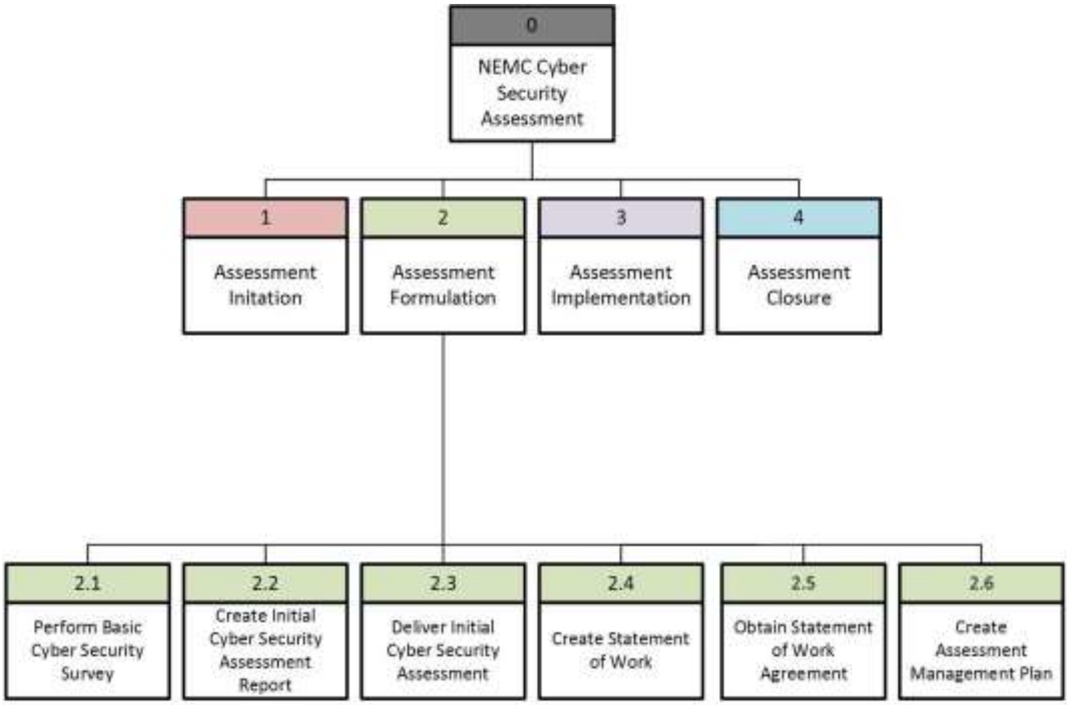

0
NEMC Cyber Security Assessment
1
Assessment Initation
2
Assessment Formulation
3
Assessment Implementation
4
Assessment Closure
2.1
Perform Basic Cyber Security Survey
2.2
Create Initial Cyber Security Assessment Report
2.3
Deliver Initial Cyber Security Assessment
2.4
Create Statement of Work
2.5
Obtain Statement of Work Agreement
2.6
Create Assessment Management Plan

Figure 10 Assessment Formulation breakdown.

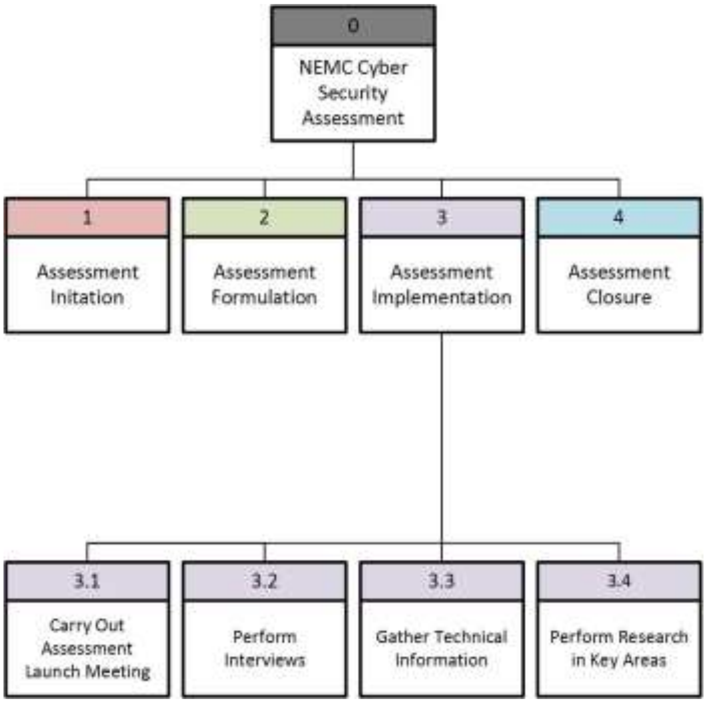

0
NEMC Cyber Security Assessment
1
Assessment Initation
2
Assessment Formulation
3
Assessment Implementation
4
Assessment Closure
3.1
Carry Out Assessment Launch Meeting
3.2
Perform Interviews
3.3
Gather Technical Information
3.4
Perform Research in Key Areas

Figure 11 Assessment Implementation breakdown.

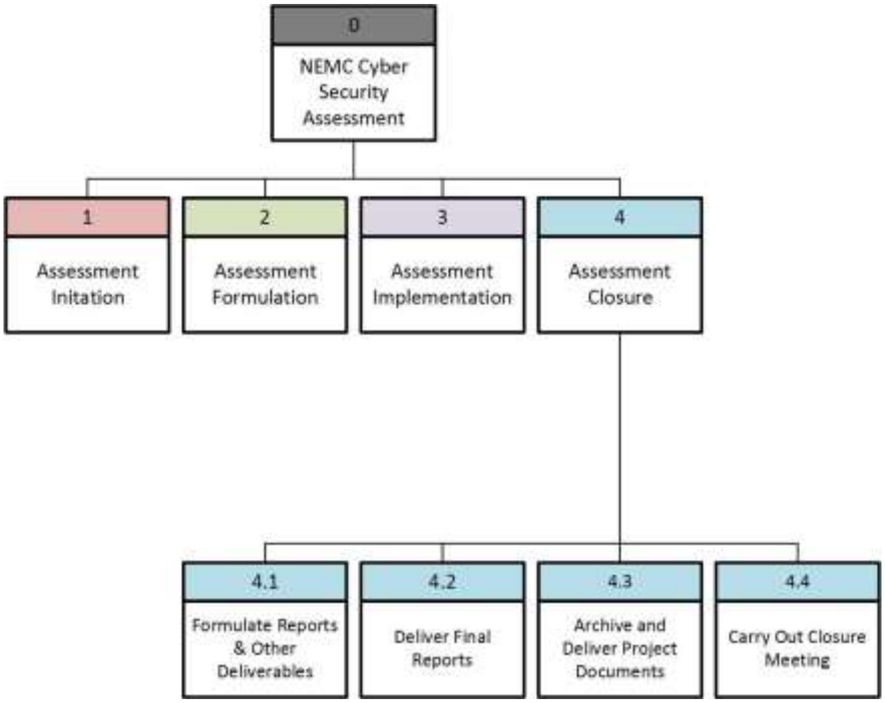

0
NEMC Cyber Security Assessment
1
Assessment Initation
2
Assessment Formulation
3
Assessment Implementation
4
Assessment Closure
4.1
Formulate Reports & Other Deliverables
4.2
Deliver Final Reports
4.3
Archive and Deliver Project Documents
4.4
Carry Out Closure Meeting

Figure 12 Assessment Closure breakdown.

Timeline

A more detailed schedule of the assessment is Microsoft Project format is available to all relevant stakeholders. The schedule will be updated as required and relevant stakeholders will be apprised. The table below shows major milestones of this project.

Milestone	Dates
Delivery of Initial Cyber Security Assessment Report	August 17, 2018
Project Launch Meeting	September 3, 2018
Deliver Final Reports	October 1, 2018
Carry Out Closure Meeting	October 8, 2018

Stakeholder Management

Stakeholder Analysis

The following table outlines the major stakeholders in involved in the assessment and their roles:

Stakeholder	Role
Senior Management Team, MoH	Project Sponsors.
Technical Supervisor, NEMC	Represents the interest of NEMC and Ministry.
NEMC Staff (all)	Provide information to the assessment team.
Assessor (also Project Manager/Team Lead)	Spearhead the assessment.
Project Team	Assist in carrying out the assessment.

The follow table outlines the Power-Interest level for each stakeholder identified:

Stakeholder	Power	Interest
Senior Management Team, MoH	High	Low
Technical Supervisor, NEMC	High	High
NEMC Staff (all)	Low	Low
Assessor (also Project Manager/Team Lead)	High	High
Project Team	Low	High

Stakeholder Management Plan

A study was done of the stakeholders involved in the assessment process. The following matrix shows stakeholders divided by quadrants base on interests and power:

Power	**High**	Senior Management Team, MoH	Technical Supervisor, NEMC Assessor (also Project Manager/Team Lead)
	Low	NEMC Staff (all)	Project Team
		Low	**High**
		Interest	

A lot of attention should be paid to the stakeholders in the upper left quadrant (high power, high interest). Stakeholders in the upper right quadrant is critical at the beginning of the project. The stakeholder on the lower right quadrant is important but they can be managed as they have high interest in seeing the assessment through. The lower left quadrant is not critical.

The most important interactions will be between the Technical Supervisor and the Assessor and this where most stakeholder management will take place during the course of the assessment.

Assessment Team Management

Assessment Team Requirements

Based on the scope of work of this project, the assessment team will be chosen from the human resources available at the Ministry, the required human resources are listed as follows:

1. Assessor (Project Manager/Team Lead) – officer with a background in Information and Communications Technology and is familiar with the standards that will be implemented.
2. Assistant Assessor – officer with a background in Information and Communications Technology who is able to assist the Assessor in carrying out the assessment.
3. Equipment Auditor – officer with a background in inventory keeping who will assist with the information gathering, especially with the taking of inventory.

All tasks and responsibilities required to carrying out the assessment will be responsibility of the assessment team.

Assessment Team Management Plan

Both Assistant and Equipment Auditor reports the Assessor. The assessor is responsible to assign tasks in order to carry out the assessment successfully.

All internal rules, regulations and policies of the Ministry of Health regarding employee reporting, behavior, etc. remain in effect.

Communication Management

The interactions and forms of communications outlined in this section are planned or proposed based on the parameters of the assessment are subject to changes and should be taken as guidelines.

Communication Interactions

The below table outlines typical communications interactions and purposes:

Interactions	Purpose
Service Provider's Representative – Client's Representative	Official channel of interaction between client and service provider.
Assessment Team – Members of the Unit (NEMC)	Communication is primarily to gather information for the assessment.
Between Assessment Team Members	Communications between assessment team, critical to carry out the assessment.

Forms of Communication

The below table describes the proposed forms of communications and their typical purposes:

Forms of Communication	Purpose
Verbal	For face-to-face interactions during meetings, etc.
Written	For official and unofficial correspondence, most importantly, as a form of documentation.
Electronic mail	For official and unofficial correspondence, most importantly, as a form of documentation.
Portable media and file sharing	For sharing information, especially large amounts of information, including confidential information that is based share using this medium.

Risk Management

Risk Analysis

The following table is a listing of risks that have been identified for this assessment:

ID	Risk Description	Probability	Impact	P	I	PxI
1	Low quality of information during assessment	High	High	1.00	1.00	1.00
2	Restricted access to critical information	Medium	High	0.45	1.00	0.45
3	Inexperience from team members	High	Medium	1.00	0.45	0.45
4	Delays due to internal processes and red tape	Medium	Medium	0.45	0.45	0.20
5	Delays in decision-making	High	Low	1.00	0.10	0.10
6	Force Majeure (e.g. act of nature) impacts project	Medium	High	0.45	1.00	0.45
7	Failure to follow methodology	Medium	High	0.45	1.00	0.45
8	Failure to understand frameworks and standards	Medium	High	0.45	1.00	0.45
9	Stakeholders become disengaged with the project	Low	Medium	0.10	0.45	0.05
10	Internal changes in organization disrupts project	Low	High	0.10	1.00	0.10

The above listing is not exhaustive as unidentified risks might occur during the course of the assessment.

The below matrix shows the categorization of the risk that have been identified based on the probability of occurrence (high = 1.0, medium = 0.45, and low = 0.1) as well as the impact they will have on the project (high = 1.0, medium = 0.45, and low = 0.1).

Probability	**High (1.0)**		3,	1,
	Med. (0.45)		4,	2,6,7,8
	Low (0.1)	5,	9	10
		Low (0.1)	**Med. (0.45)**	**High (1.0)**
		Impact		

Risk Management Plan

Identified risk as per risk register will be managed as follows:

1. All medium and low probability risks that have medium or low impact will be monitored in order to determine if adjustments need to be made to in order to mitigate them. These correspond to Risks 5, 4, and 9.
2. For Risk 1, Assessment team are instructed to start gathering any information from outside the organization that may help to mitigate any lack of information quality during the assessment.
3. Risk 10 is to be ignored as it has a very low probability of occurrence.

4. All medium probability, high impact risks will be handled on a case-by-case basis by Assessor if they occur. Team members are ask monitor and report any of these as they occur.

Any unplanned risk that occur during the assessment will be managed under the *Issue and Change Management* section.

Quality Management

The quality of the project will be determined by adherence to standards as defined in the *Statement of Work*, *Applicable Standards* section.

All other underlying requirements for quality are determined by the Ministry of Health's internal policies and guidelines.

Issue and Change Management

Issue Management Plan

All issues will be communicated officially via email as provisioned by Statement of Work, *Change Control Procedure* section.

Change Management Plan

Any changes that are perceived to be necessary will be communicated with the Client's representation as defined in the Statement of Work, *Change Control Procedure* section.

All changes to any project document will be updated in *Version History* section of each document and approved by the Project Manager (Douglas Westby) after seeking appropriate approvals.

Closing

The closing procedure is defined as follows:

1. Delivery of the final reports on the 1st of October, 2018. The delivery of the report one week in advance of the closing meeting allows for the findings to be reviewed and relevant queries be formulated.
2. Conduct Closing Meeting on the 8th of October, 2018. The purpose of the meeting to clarify and information that may have come up from the Final Report and to conduct a technical consultation workshop on the way forward to close any gaps. It will address how to implement any changes that may be required as well as to determine the high-level scope of work for future implementation of recommendations. This meeting will last anywhere between a few hours to a day.

CSA - NEMC

Information and Communications Technology Inventory Control

Principal deliverable of the cyber security assessment.

Version 1.0 – 01/10/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	James Castillo	First iteration of the listing of ICT equipment at NEMC.	Douglas Westby		01/10/2018

Contents

About This Document .... *CCIV*

Inventory .... *CCV*

Notes .... *CCVI*

About This Document

This document provided a listing of all Information and Communications Technology Equipment (ICT) that the assessment team has identified as being pertinent to the results of the assessment. These form the core of the assessment of cyber threat at the organization.

Inventory

The following table is a listing of all information and communications technology equipment related to the assessment:

Workstation/Functional Area	Device Description	Model/Make	Serial No.	Status/Comment
Technical Supervisor	Desktop Computer	Dell Inspiron Desktop	FLPD4HAO46850	Functional
	Printer	HP Deskjet D1460	GCVRA-702	Functional
	Laptop	Dell 3540	AYKS4HAO784521	Functional
Transport Officer	Desktop Computer	Dell Inspiron Desktop	CH-D8XROV-72872-IAV	Functional
Storekeeper	Desktop Computer	Dell Inspiron Desktop	7862CPL	Functional
Second Class Clerk	Desktop Computer	Dell Inspiron Desktop	CH-012MWY-64180-364	Functional
Main Office	printer	HP Laser jet pro 500 Color MFP	BOICB-1200-00	Functional
Conference Room	Television	Toshiba	DO9254CO543DI	Functional
	projector	EpsonH552A	TUAF48163IL	Functional
Biomedical Technician	Desktop Computer	Generic Brand	N/A	Functional
	Laptop	Dell 3540	GYHG4HAO45218	Functional
Biomedical Technician	Desktop Computer	Dell Inspiron Desktop	D2PTBX010473	Functional
Technical Advisor	Desktop Computer	Dell D07D	7018337593	Functional
	Printer	HP Deskjet Link Advantage 4615	CN2AB24424	Functional
	Camera DVR	Provisual	2641650-P	Functional
Entranceway	Attendance Terminal	Unknown	3359761260103	Functional
Storeroom	Printer	HP Laser jet pro 500 Color MFP	CN59DCB829	Not functional
	Printer	HP Office Jet 8610	CN51HEX2CT	Functional
	Printer	HP Deskjet Link Advantage 4615	CN2AB2442F	Not functional

Notes

1. There are about 16 Android phones and 2 iPhones being used by employees at any given time. These are personal properly but they connect to the network in the main building at NEMC. This is not done in a controlled manner.
2. Employees bring other devices at work from time to time; these devices are not monitored and controlled.
3. A scan shows unknown or unaccounted devices connected to the wireless network from time to time.
4. The wireless network is left turned on after hours.
5. All operating systems for workstations are Microsoft Windows based.
6. There is no physical access control for most of the devices.

CSA - NEMC

Cyber Security Profile

Proposed cyber security stance of the organization based on existing and expected conditions.

Version 1.0 – 01/10/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	Cyber security profile of NEMC, based on assessments and on-the-ground information.	Douglas Westby		01/10/2018

Contents

About This Document ... *CCX*

1. IDENTIFY (ID) ... *CCXI*

1.1 Asset Management (ID.AM) ... CCXI

1.2 Business Environment (ID.BE) ... CCXI

1.3 Governance (ID.GV) ... CCXI

1.4 Risk Assessment (ID.RA) ... CCXI

1.5 Risk Management Strategy (ID.RM) ... CCXII

2. PROTECT (PR) ... *CCXII*

2.1 Access Control (PR.AC) ... CCXII

2.2 Awareness and Training (PR.AT) ... CCXII

2.3 Data Security (PR.DS) ... CCXII

2.4 Information Protection Processes and Procedures (PR.IP) ... CCXIII

2.5 Maintenance (PR.MA) ... CCXIII

2.6 Protective Technology (PR.PT) ... CCXIII

3. DETECT (DE) ... *CCXIV*

3.1 Anomalies and Events (DE.AE) ... CCXIV

3.2 Security Continuous Monitoring (DE.CM) ... CCXIV

3.3 Detection Processes (DE.DP) ... CCXIV

4. RESPOND (RS) ... *CCXIV*

4.1 Response Planning (RS.RP) ... CCXIV

4.2 Communications (RS.CO) ... CCXV

4.3 Analysis (RS.AN) ... CCXV

4.4 Mitigation (RS.MI) ... CCXV

4.5 Improvements (RS.IM) ... CCXV

5. RECOVER (RC) ... *CCXVI*

5.1 Recovery Planning (RC.RP) ... CCXVI

5.2 Improvements (RC.IM) ... CCXVI

5.3 Communications (RC.CO) ... CCXVI

About This Document

This document describes the Cyber Security Profile of National Engineering & Maintenance Center as carried out in *Cyber Security Assessment of NEMC* and is one of the objectives or deliverables as agreed upon at the initiation of the assessment.

A profile represents the functions, categories and subcategories prioritized by an organization based on business needs and can be used to measure the organization's progress toward the it cyber security readiness target.

1. IDENTIFY (ID)

1.1 Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to business objectives and the organization's risk strategy.

ID.AM-1
Physical devices and systems within the organization are inventoried.
ID.AM-2
Software platforms and applications within the organization are inventoried.

1.2 Business Environment (ID.BE)

The organization's mission, objectives, stakeholders and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities and risk management decisions.

ID.BE-4
Dependencies and critical functions for delivery of critical services are established.
ID.BE-5
Resilience requirements to support delivery of critical services are established.

1.3 Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and management are informed of cyber security risk.

ID.GV-1
Organizational information security policy is established.

1.4 Risk Assessment (ID.RA)

The organization understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals.

ID.RA-1
Asset vulnerabilities are identified and documented.
ID.RA-2
Threat and vulnerability information is received from information sharing forums and sources.
ID.RA-3
Threats, both internal and external, are identified and documented.

1.5 Risk Management Strategy (ID.RM)

The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.

ID.RM-1
Risk management processes are established, managed and agreed to by organizational stakeholders.

2. PROTECT (PR)

2.1 Access Control (PR.AC)

Access to assets and associated facilities is limited to authorized users, processes, or devices and to authorized activities and transactions.

PR.AC-1
Identities and credentials are managed for authorized devices and users.
PR.AC-2
Physical access to assets is managed and protected.
PR.AC-3
Remote access is managed.

2.2 Awareness and Training (PR.AT)

The organization's personnel and partners are provided with cyber security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-1
All users are informed and trained.
PR.AT-2
Privileged users understand roles & responsibilities.

2.3 Data Security (PR.DS)

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity and availability of information.

PR.DS-1
Data-at-rest is protected.
PR.DS-3
Assets are formally managed throughout removal, transfers and disposition.

2.4 Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

PR.IP-4
Backups of information are conducted, maintained and tested periodically.
PR.IP-7
Protection processes are continuously improved.
PR.IP-9
Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

PR.IP-10
Response and recovery plans are tested.
PR.IP-11
Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening).

2.5 Maintenance (PR.MA)

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

PR.MA-1
Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools.
PR.MA-2
Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access.

2.6 Protective Technology (PR.PT)

Technical security solutions are managed to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements.

PR.PT-2
Removable media is protected and its use restricted according to policy.
PR.PT-4
Communications and control networks are protected.

3. DETECT (DE)

3.1 Anomalies and Events (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

DE.AE-2
Detected events are analyzed to understand attack targets and methods.
DE.AE-4
Impact of events are determined.

3.2 Security Continuous Monitoring (DE.CM)

The information system and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures.

DE.CM-1
The network is monitored to detect potential cyber security events.
DE.CM-7
Monitoring for unauthorized personnel, connections, devices, and software is performed.
DE.CM-8
Vulnerability scans are performed.

3.3 Detection Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

DE.DP-1
Roles and responsibilities for detection are well defined to ensure accountability.
DE.DP-2
Detection activities comply with all applicable requirements.
DE.DP-3
Detection processes are tested.
DE.DP-4
Event detection information is communicated to appropriate parties.

4. RESPOND (RS)

4.1 Response Planning (RS.RP)

Response processes and procedures are executed and maintained to ensure timely response to detected cyber security events.

RS.RP-1
Response plan is executed during or after an event.

4.2 Communications (RS.CO)

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

RS.CO-1
Personnel know their roles and order of operations when a response is needed.
RS.CO-4
Coordination with stakeholders occurs consistent with response plans.

4.3 Analysis (RS.AN)

Analysis is conducted to ensure adequate response and support recovery activities.

RS.AN-1
Notifications from detection systems are investigated.
RS.AN-2
The impact of the incident is understood.
RS.AN-3
Forensics are performed.
RS.AN-4
Incidents are categorized consistent with response plans.

4.4 Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.

RS.MI-1
Incidents are contained.
RS.MI-2
Incidents are mitigated.

4.5 Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RS.IM-1
Response plans incorporate lessons learned.
RS.IM-2
Response strategies are updated.

5. RECOVER (RC)

5.1 Recovery Planning (RC.RP)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cyber security events.

RC.RP-1

Recovery plan is executed during or after an event.

5.2 Improvements (RC.IM)

Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.IM-1

Recovery plans incorporate lessons learned.

RC.IM-2

Recovery strategies are updated.

5.3 Communications (RC.CO)

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

RC.CO-3

Recovery activities are communicated to internal stakeholders and executive and management teams.

CSA - NEMC

Cyber Security Risk Analysis

Principal deliverable of the cyber security assessment.

Version 1.0 – 01/10/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	First iteration of the risk analysis for CSA of NEMC, MoH, Belize.	Douglas Westby		01/10/2018

Contents

About This Document .... *CCXX*
Risk and Observation Tables .... *CCXXI*
Identify CCXXII
Protect CCXXIII
Detect CCXXIII
Respond CCXXIV
Recover CCXXV
Risk Categorization .... *CCXXV*
Risk Response .... *CCXXVI*
High Risk CCXXVI
Moderate Risk CCXXVII
Low Risk CCXXX

About This Document

A risk analysis is a key part of a cyber security strategy. This document lays out a cyber security risk analysis of that complements the Cyber Security Profile of the National Engineering and Maintenance Center of the Ministry of Heath as a part of the current Cyber Security Assessment of the unit.

Risk and Observation Tables

The observation tables are used to make note of and categorize risk in line with the guidelines set out by the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. The information gathered can be used in other parts of the assessment and as a part of the final assessment report.

The following legend is used as guidance for the five subsequent sections of this document representing the Identify, Protect, Detect, Respond and Recover functions:

Function	Aggrupation of subcategorizes to be analyzed.
Category	Categorization of functions.
Subcategory	Particular action to be taken or issue to be addressed.
Probability	A numerical value that represents the likelihood that an adverse event in the particular subcategory will occur. See Probability Levels Table.
Impact	A numerical value that represents the (typically negative) effect that the particular subcategory. See Impact Levels Table.
Risk (PxI)	Numerical valuation of the probability that event will occur multiplied by impact of said event.
Reference	Guideline, standard or practice will be use to address the particular need.
Comment/Observations	Any comment or note with regards to the subcategory.

The following table represents levels of probabilities and their numerical equivalent for the five sections representing the Identify, Protect, Detect, Respond and Recover functions:

Probability of Occurrence Levels		
Numerical Equivalent	**Likelihood**	**Description**
0.1	**Negligible**	Unlikely ever to occur.
0.28	**Very Low**	Likely to occur two/three times every five years.
0.46	**Low**	Likely to occur once every year or less.
0.64	**Medium**	Likely to occur once every six months or less.
0.82	**High**	Likely to occur once per month or less.
1.0	**Very High**	Likely to occur multiple times per month.

The following table represents levels of impact severity and their numerical equivalent for the five sections representing the Identify, Protect, Detect, Respond and Recover functions:

Impact Severity Levels		
Numerical Equivalent	Likelihood	Description
0.1	**Insignificant**	Little or no impact.
0.28	**Minor**	Minimal effort to repair, restore or reconfigure.
0.46	**Significant**	Small but tangible harm, maybe noticeable by a limited audience, some embarrassment, some effort to repair.
0.64	**Damaging**	Damage to reputation, loss of confidence, significant effort to repair.
0.82	**Serious**	Considerable system outage, loss of connected customers, business confidence, compromise of large amount information.
1.0	**Critical**	Extended outage, permanent loss of resource, triggering business continuity procedures, complete compromise of information.

Identify

The Identify Function develops the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.

The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cyber security risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
IDENTIFY (ID)	ID.AM	ID.AM-1	0.64	0.82	0.52	Done but not updated regularly.
		ID.AM-2	0.82	0.46	0.38	Not formalized.
	ID.BE	ID.BE-4	0.46	0.46	0.21	
		ID.BE-5	0.46	0.46	0.21	
	ID.GV	ID.GV-1	0.46	0.46	0.21	
	ID.RA	ID.RA-1	0.82	0.64	0.52	
		ID.RA-2	0.46	0.28	0.13	To a certain degree, but not formalized.
		ID.RA-3	0.64	0.1	0.06	
	ID.RM	ID.RM-1	0.64	0.28	0.18	

Protect

The Protect Function develops and implements the appropriate safeguards to ensure delivery of critical infrastructure services.

It supports the ability to limit or contain the impact of a potential cyber security event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
PROTECT (PR)	PR.AC	PR.AC-1	0.82	0.46	0.38	To a certain degree, but not formalized.
		PR.AC-2	0.82	0.46	0.38	
		PR.AC-3	0.82	0.46	0.38	
	PR.AT	PR.AT-1	0.64	0.28	0.18	Only some users, based on their technical knowledge.
		PRAT-2	0.82	0.28	0.23	To some extent, yes.
	PR.DS	PR.DS-1	0.82	0.46	0.38	To a certain degree, but not formalized.
		PR.DS-3	0.64	0.46	0.29	
	PR.IP	PR.IP-4	0.64	0.28	0.18	
		PR.IP-7	0.82	0.28	0.23	
		PR.IP-9	0.82	0.28	0.23	
		PR.IP-10	0.82	0.28	0.23	
		PR.IP-11	0.82	0.28	0.23	
	PR.MA	PR.MA-1	0.64	0.28	0.18	
		PR.MA-2	0.64	0.28	0.18	
	PR.PT	PR.PT-2	0.64	0.28	0.18	
		PR.PT-4	0.64	0.28	0.18	Not beyond built-in capabilities.

Detect

The Detect Function develops and implements the appropriate activities to identify the occurrence of a cyber security event.

It enables timely discovery of cyber security events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
DETECT (DE)	DE.AE	DE.AE-2	0.46	0.46	0.21	
		DE.AE-4	0.82	0.28	0.23	
	DE.CM	DE.CM-1	0.64	0.64	0.41	
		DE.CM-7	0.64	0.46	0.29	Only when it is suspected.
		DE.CM-8	0.64	0.46	0.29	
	DE.DP	DE.DP-1	0.64	0.64	0.41	
		DE.DP-2	0.82	0.46	0.38	
		DE.DP-3	0.82	0.64	0.52	
		DE.DP-4	0.82	0.64	0.52	

Respond

Develop and implements the appropriate activities to take action regarding a detected cyber security event.

It supports the ability to contain the impact of a potential cyber security event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
RESPOND (RS)	RS.RP	RS.RP-1	0.82	0.46	0.38	
	RS.CO	RS.CO-1	0.64	0.46	0.29	
		RS.CO-4	0.64	0.46	0.29	
	RS.AN	RS.AN-1	0.82	0.46	0.38	
		RS.AN-2	0.82	0.28	0.23	
		RS.AN-3	0.82	0.28	0.23	
		RS.AN-4	0.64	0.28	0.18	
	RS.MI	RS.MI-1	0.46	0.46	0.21	
		RS.MI-2	0.64	0.28	0.18	
	RS.IM	RS.IM-1	0.82	0.46	0.38	
		RS.IM-2	0.82	0.46	0.38	Some action is taken, but not always adequate

Recover

The Recover Function develops and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.

It supports timely recovery to normal operations to reduce the impact from a cyber security event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

Function	Category	Subcategory	Probability	Impact	Risk (PxI)	Comments/Observations
RECOVER (RC)	RC.RP	RC.RP-1	0.82	0.28	0.23	
	RC.IM	RC.IM-1	0.82	0.28	0.23	
		RC.IM-2	0.82	0.28	0.23	
	RC.CO	RC.CO-3	0.64	0.1	0.06	To a certain degree, yes.

Risk Categorization

The following table further categorizes cyber security risks in terms their levels (high, moderate, low):

		Probability of Occurrence					
		Negligible (0.10)	Very Low (0.28)	Low (0.46)	Medium (0.64)	High (0.82)	Very High (1.00)
Impact Severity	Critical (1.00)	Low	Moderate	High	High	High	High
	Serious (0.82)	Low	Moderate	High	High	High	High
	Damaging (0.64)	Low	Moderate	Moderate	High	High	High
	Significant (0.46)	Low	Low	Moderate	Moderate	High	High
	Minor (0.28)	Low	Low	Low	Moderate	Moderate	Moderate
	Insignificant (0.10)	Low	Low	Low	Low	Low	Low

The follow tables show the numeric values that corresponds the levels (high, moderate, low):

		Probability of Occurrence					
		Negligible (0.10)	Very Low (0.28)	Low (0.46)	Medium (0.64)	High (0.82)	Very High (1.00)
Impact Severity	Critical (1.00)	0.10	0.28	0.46	0.64	0.82	1.00
	Serious (0.82)	0.082	0.2296	0.3372	0.5248	0.6724	0.82
	Damaging (0.64)	0.064	0.1792	0.2944	0.4096	0.5248	0.64
	Significant (0.46)	0.046	0.1288	0.2116	0.2944	0.3772	0.46
	Minor (0.28)	0.028	0.0784	0.1288	0.1792	0.2296	0.28
	Insignificant (0.10)	0.010	0.028	0.046	0.064	0.082	0.10

Risk Response

Risk/Solution pairs are formulated in the following tables in order to propose a solution to fill cyber security gap. The purpose of the solution is to fill the gap in order to reduce risk and ensure that the organization is up to par with its proposed Cyber Security Profile.

High Risk

Function	Category	Subcategory	Risk Description	Response Description
IDENTIFY (ID)	ID.AM	ID.AM-1	Physical devices and systems within the organization are not inventoried.	Implement **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
IDENTIFY (ID)	ID.RA	ID.RA-1	Asset vulnerabilities are not identified and documented.	Implement **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3
DETECT (DE)	DE.DP	DE.DP-3	Detection processes are not tested.	Implement **ISO/IEC 27001:2013** A.14.2.8
DETECT (DE)	DE.DP	DE.DP-4	Event detection information is not communicated to appropriate parties.	Implement **ISO/IEC 27001:2013** A.16.1.2
DETECT (DE)	DE.CM	DE.CM-1	The network is not monitored to detect potential cyber security events.	Implement **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DETECT (DE)	DE.DP	DE.DP-1	Roles and responsibilities for detection are not well defined to ensure accountability.	Implement **ISO/IEC 27001:2013** A.6.1.1

Function	Category	Subcategory	Risk Description	Response Description
IDENTIFY (ID)	ID.AM	ID.AM-2	Software platforms and applications within the organization are not inventoried.	Implement **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
PROTECT (PR)	PR.AC	PR.AC-1	Identities and credentials are managed for authorized devices and users.	Implement **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
PROTECT (PR)	PR.AC	PR.AC-2	Physical access to assets is not managed and protected.	Implement **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
PROTECT (PR)	PR.AC	PR.AC-3	Remote access is not managed.	Implement **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1
PROTECT (PR)	PR.DS	PR.DS-1	Data-at-rest is not protected.	Implement **ISO/IEC 27001:2013** A.8.2.3
DETECT (DE)	DE.DP	DE.DP-2	Detection activities do not comply with all applicable requirements.	Implement **ISO/IEC 27001:2013** A.18.1.4
RESPOND (RS)	RS.RP	RS.RP-1	Response plan is not executed during or after an event.	Implement **ISO/IEC 27001:2013** A.16.1.5
RESPOND (RS)	RS.AN	RS.AN-1	Notifications from detection systems are not investigated.	Implement **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5
RESPOND (RS)	RS.IM	RS.IM-1	Response plans do not incorporate lessons learned.	Implement **ISO/IEC 27001:2013** A.16.1.6
RESPOND (RS)	RS.IM	RS.IM-2	Response strategies are not updated.	Implement **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Moderate Risk

Function	Category	Subcategory	Risk Description	Response Description
PROTECT (PR)	PR.DS	PR.DS-3	Assets are not formally managed throughout removal, transfers and disposition.	Implement **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
DETECT (DE)	DE.CM	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is not performed.	Implement **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DETECT (DE)	DE.CM	DE.CM-8	Vulnerability scans are not performed.	Implement **ISO/IEC 27001:2013** A.12.6.1

Function	Category	Subcategory	Risk Description	Response Description
RESPOND (RS)	**RS.CO**	**RS.CO-1**	Personnel do not know their roles and order of operations when a response is needed.	Implement **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1
RESPOND (RS)	**RS.CO**	**RS.CO-4**	Coordination with stakeholders is not consistent with response plans.	Implement **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
PROTECT (PR)	**PR.AT**	**PR.AT-2**	Privileged users do not understand roles & responsibilities.	Implement **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
PROTECT (PR)	**PR.IP**	**PR.IP-7**	Protection processes are not continuously improved.	Implement **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PROTECT (PR)	**PR.IP**	**PR.IP-9**	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are not in place and managed.	Implement **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2
PROTECT (PR)	**PR.IP**	**PR.IP-10**	Response and recovery plans are not tested.	Implement **ISO/IEC 27001:2013** A.17.1.3
PROTECT (PR)	**PR.IP**	**PR.IP-11**	Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening).	Implement **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4
DETECT (DE)	**DE.AE**	**DE.AE-4**	Impact of events are not determined.	Implement **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
RESPOND (RS)	**RS.AN**	**RS.AN-2**	The impact of the incident is not understood.	Implement **ISO/IEC 27001:2013** A.16.1.6
RESPOND (RS)	**RS.AN**	**RS.AN-3**	Forensics are not performed.	Implement **ISO/IEC 27001:2013** A.16.1.7
RECOVER (RC)	**RC.RP**	**RC.RP-1**	Recovery plan is not executed during or after an event.	Implement **ISO/IEC 27001:2013** A.16.1.5
RECOVER (RC)	**RC.IM**	**RC.IM-1**	Recovery plans do not incorporate lessons learned.	Implement **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**RC.IM**	**RC.IM-2**	Recovery strategies are not updated.	Implement **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
IDENTIFY (ID)	**ID.BE**	**ID.BE-4**	Dependencies and critical functions for delivery of critical services are not established.	Implement **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3

Function	Category	Subcategory	Risk Description	Response Description
IDENTIFY (ID)	**ID.BE**	**ID.BE-5**	Resilience requirements to support delivery of critical services are not established.	Implement **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
IDENTIFY (ID)	**ID.GV**	**ID.GV-1**	Organizational information security policy is not established.	Implement **ISO/IEC 27001:2013** A.5.1.1
DETECT (DE)	**DE.AE**	**DE.AE-2**	Detected events are analyzed to understand attack targets and methods.	Implement **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4
RESPOND (RS)	**RS.MI**	**RS.MI-1**	Incidents are not contained.	Implement **ISO/IEC 27001:2013** A.16.1.5
IDENTIFY (ID)	**ID.RM**	**ID.RM-1**	Risk management processes are not established, managed and agreed to by organizational stakeholders.	Implement **ISO/IEC 27001:2013** A.16.1.5
PROTECT (PR)	**PR.AT**	**PR.AT-1**	All users are not informed and trained.	Implement **ISO/IEC 27001:2013** A.7.2.2
PROTECT (PR)	**PR.IP**	**PR.IP-4**	Backups of information are not conducted, maintained and tested periodically.	Implement **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
PROTECT (PR)	**PR.MA**	**PR.MA-1**	Maintenance and repair of organizational assets are not performed and logged in a timely manner, with approved and controlled tools.	Implement **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5
PROTECT (PR)	**PR.MA**	**PR.MA-2**	Remote maintenance of organizational assets is not approved, logged and performed in a manner that prevents unauthorized access.	Implement **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1
PROTECT (PR)	**PR.PT**	**PR.PT-2**	Removable media is not protected and its use restricted according to policy.	Implement **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
PROTECT (PR)	**PR.PT**	**PR.PT-4**	Communications and control networks are not protected.	Implement **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1

Function	Category	Subcategory	Risk Description	Response Description
RESPOND (RS)	**RS.AN**	**RS.AN-4**	Incidents are not categorized consistent with response plans.	Implement **ISO/IEC 27001:2013** A.16.1.4
RESPOND (RS)	**RS.MI**	**RS.MI-2**	Incidents are not mitigated.	Implement **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5

Low Risk

Function	Category	Subcategory	Risk Description	Response Description
IDENTIFY (ID)	**ID.RA**	**ID.RA-2**	Threat and vulnerability information is not received from information sharing forums and sources.	Implement **ISO/IEC 27001:2013** A.6.1.4
IDENTIFY (ID)	**ID.RA**	**ID.RA-3**	Threats, both internal and external, are not identified and documented.	Implement **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
RECOVER (RC)	**RC.CO**	**RC.CO-3**	Recovery activities are not communicated to internal stakeholders and executive and management teams.	Implement **NIST SP 800-53 Rev. 4** CP-2, IR-4

CSA - NEMC

Assessment Closure Document

To officially formalize the completion of the cyber security assessment.

Version 1.0 – 08/10/2018

Executing Entity
Douglas Westby
NEMC
Lottie Waight Street
Belize City, Belize
+501-610-6465
dwestby@health.gov.bz

Client Organization
Froylan Uk
NEMC
Lottie Waight Street
Belize City, Belize
+501-223-0511/223-5223
nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	First iteration of the assessment closure document that serves to formalize the completion of the assessment.	Douglas Westby		08/10/2018

Contents

About This Document .... *CCXXXIV*
Introduction .... *CCXXXV*
Assessment Scope .... *CCXXXV*
Cost and Resources .... *CCXXXV*
Schedule and Milestones .... *CCXXXV*
Accounting Summary .... *CCXXXVI*
Recommendations .... *CCXXXVI*
Supporting Documents .... *CCXXXVI*
Points of Contact .... *CCXXXVI*
Acceptance .... *CCXXXVII*

About This Document

This document serves to mark the official completion of *Cyber Security Assessment of NEMC*. It gives an overview of the deliverables and objectives that are being handed over. It also provides additional information, insights and recommendations that may be useful to the client.

Its key purpose is to formalize the completion of the assessment. This document can be used as a guide for the final meeting to formalize the completion of the project.

Introduction

The National Engineering & Maintenance Department (NEMC) is one of various technical units of the Ministry of Health. The purpose of the unit is to provide technical support in the areas of Biomedical Engineering, Transportation, Building Services and other related technical support services.

In order to get a good handle on where NEMC stands in terms of cyber security, it was necessary to implement an assessment of its current ICT infrastructure. Base on this information, it was be possible to determine the required or target cyber security stance of the unit using a risk-based approach. The information gathered will assist the Ministry in being prepared from a broader perspective and will allow for evidence-based decision making to be made in terms of future investments in ICT costs.

This document provided a summary of the assessment and is presented at the final meeting between the service provider and client.

Assessment Scope

The purpose of the assessment was to provide an in-depth analysis of the cyber security readiness of the National Engineering and Maintenance Center.

More detailed information about the scope of the assessment can be found in the Statement of Work as well as the *Assessment Management Plan*.

Cost and Resources

The resources required for this project include some human as well as material resources. All resources were obtained in-house. More information on resource usage can be found in the *Statement of Work*.

Schedule and Milestones

Milestone along with delivery dates are listed in the following table.

Milestone	Date
Delivery of Initial Cyber Security Assessment Report	August 17, 2018
Project Launch Meeting	September 3, 2018
Deliver Final Reports	October 1, 2018
Carry Out Closure Meeting	October 8, 2018

All milestones were met and all deliverables were on time or completed before the required deadlines.

Accounting Summary

No payment or financial information is provide since the assessment was conducted internally.

Recommendations

Please see *Recommendations* Section of the *Final Assessment Report*.

Supporting Documents

There are no supporting documents apart from those being delivered and listing the *Archive Listing Document.*

Points of Contact

Contact information is provided in case the assessment needs to be discussed further or repeated and to also maintain a clear channel of communication for any other purposes. The contact persons remain the same those provided in the *Statement of Work* and are listed in the following table:

Name	Role	Contact information
Douglas Westby	Assessor	Douglas Westby +501-610-6465 dwestby@health.gov.bz
Froylan Uk	Client Focal Point	Froylan Uk +501-223-0511/223-5223 nemc@health.gov.bz

Acceptance

By signing below, I, Froylan Uk, in my capacity as Technical Supervisor, of National Engineering and Maintenance Center, Ministry of Health acknowledge the completion of this assessment as outlined in this *Assessment Closure Document*.

Signature	**Signature (witness)**
Froylan Uk	Douglas Westby, P.Eng.
Full Name	**Full Name**
08/10/18	08/10/18
Date	**Date**

CSA - NEMC

Archive Listing Document

For the delivery of assessment documentation to client on assessment completion

Version 1.0 – 08/10/2018

Executing Entity	**Client Organization**
Douglas Westby	Froylan Uk
NEMC	NEMC
Lottie Waight Street	Lottie Waight Street
Belize City, Belize	Belize City, Belize
+501-610-6465	+501-223-0511/223-5223
dwestby@health.gov.bz	nemc@health.gov.bz

Version History

Version Number	Author/Editor	Edits/Changes	Approver's Name	Approver's Signature	Approval Date
1.0	Douglas Westby	First iteration of the listing of documents and files to be delivered to client.	Douglas Westby		08/10/2018

Contents

About This Document .... *CCXLI*
Archive Listing .... *CCXLII*
Acceptance .... *CCXLIII*

About This Document

This document prefaces all documents that are handed over to the client on completion of *Cyber Security Assessment of NEMC.* It contains a listing of all documents, archives and files that are attached to it.

It also serves to acknowledge formal verification and acceptance of these documents, archive and files.

Archive Listing

The following table lists all documents that were delivered to client:

Description	Version Number
CSA - NEMC - Assessment Closure Document.docx	1.0
CSA - NEMC - Archive Listing Document.docx	1.0
CSA - NEMC - Assessment Charter.docx	1.0
CSA - NEMC - Basic Cyber Security Survey.docx	1.0
CSA - NEMC - Business Case.docx	1.0
CSA - NEMC - Cyber Security Profile.docx	1.0
CSA - NEMC - Cyber Security Risk Assessment.docx	1.0
CSA - NEMC - Final Assessment Report.docx	1.0
CSA - NEMC - Information and Communications Technology Inventory Control.docx	1.0
CSA - NEMC - Initial Cyber Security Assessment Report.docx	1.0
CSA - NEMC - Assessment Management Plan.docx	1.0
CSA - NEMC - Schedule.mpp	1.0
CSA - NEMC - Statement of Work.docx	1.0

Acceptance

By signing below, I, Froylan Uk, in my capacity as Technical Supervisor, of National Engineering and Maintenance Center, Ministry of Health acknowledge receipt of the archives, documents and files listed in and delivered with this *Archive Listing Document*.

Signature	**Signature (witness)**
Froylan Uk	Douglas Westby, P.Eng.
Full Name	**Full Name**
08/10/18	08/10/18
Date	**Date**