

Université du Québec en Outaouais

**Integrating Governance, Risk, and Compliance
Management to Enhance Requirements
Engineering in Information Technology Projects**

By

Richard Bett, M.Sc. PM, PMP

A thesis submitted to the Graduate Faculty of
Université de Québec in partial fulfillment of the
requirements for the Degree of Master of Science

PROJECT MANAGEMENT

Université du Québec
en Outaouais

- 4 FEV. 2009

Bibliothèque

January 2009

PERSONAL BIOGRAPHY

Richard Bett is certified as a Project Management Professional (PMP) since December 2001. Richard completed an Honors degree in Commerce with Management Information System courses, at Laurentian University in Sudbury, Ontario. He has been operating his own consulting firm during the last seven years. He has been instrumental in building network infrastructures, installing computer information systems and implementing management information systems at the local and national level. Richard has five years of teaching experience in project management at the college level as well as industry.

Once Richard receives his M.Sc. PM, he will be interested in teaching at the university level on a part-time basis and author articles in academic journals. His goal is to teach project management at the international level.

ACKNOWLEDGEMENTS

I dedicate my thesis to my lovely wife Gisèle and our two beautiful daughters Stéphanie and Maxine, for whom I love very much. I say thank you for your patience and understanding which permitted me to complete my thesis.

I wish to express my gratitude to the members of the Jury Dr. Michal Iglewski and Dr. Véronique Nabelsi for their participation and suggestions in making this thesis possible.

I wish to say thank you to Dr. Stéphane Gagnon, my thesis director who gave me direction and provided valuable insight and support.

TABLE OF CONTENTS

LIST OF TABLES - GENERAL.....	vi
LIST OF TABLES – CASE STUDIES	vii
LIST OF FIGURES.....	viii
ABSTRACT	ix
INTRODUCTION	10
1.0 RESEARCH OBJECTIVES.....	12
1.1. Challenges and Success Factors as to Practicing RE in Information Technology (IT) Projects	12
1.2. Relevance of GRCM for RE.....	16
2.0 PERFORMING REQUIREMENTS ENGINEERING	18
2.1. Overview of Requirements Engineering (RE).....	18
2.2. Requirement Engineering Process	19
2.2.1. Elicitation.....	20
2.2.2. Analysis.....	21
2.2.3. Prioritization	22
2.2.4. Validation.....	22
2.2.5. Documentation	22
2.2.6. Requirements Management	23
2.3. RE in General	25
2.3.1. Various Types of Requirements.....	25
2.3.2. Design and Development Issues with RE.....	27
2.3.3. Type of RE Problems.....	29
2.3.4. Trends Affecting RE Processes and Practices	29
2.4. RE Capability Measurement Framework	33
3.0 GOVERNANCE, RISK AND COMPLIANCE MANAGEMENT (GRCM)	37
3.1. Foundations of GRCM as Best Practices.....	37
3.2. Governance	38
3.2.1. Overview of IT Governance	39
3.2.2. IT Governance Focus Areas.....	41
3.2.3. IT Governance Tools	42
3.2.3.1. COBIT.....	43
3.2.3.2. ITIL	44
3.2.3.3. ISO 17799	45
3.3. Risk Management	46
3.3.1. Overview of Risk Management	47
3.3.2. Project Risk Management.....	51
3.3.3. Minimize Risks	52
3.4. Compliance	53

3.4.1.	Overview of Compliance	53
3.4.2.	Compliance with Legal Requirements.....	56
3.4.3.	Reviews of Security Policy and Technical Compliance	58
3.5	System Audit Consideration.....	60
3.6	Relating GRCM to Other SE Practices.....	62
3.7	GRCM Measurement Framework	63
3.8	Measuring the Level of Capability in the Organizational Context.....	68
4.0	RESEARCH METHODOLOGY	71
4.1	Positivist Case Study Research.....	71
4.2.	Research Process	73
4.2.1.	Design of the Case Study	73
4.2.2.	Conduct of the Case Study.....	78
4.2.3.	Analysis of the Case Study Evidence	80
4.2.4.	Writing up the Case Study Report	82
4.3.	Case Profiles	84
5.0	DATA ANALYSIS.....	87
5.1.	Capability Measurement Framework for GRCM and RE	87
5.2.	Within-Case Analysis to Identify Key Relationships between GRCM and RE.....	90
5.3.	Cross-Case Analysis to Identify Key Relationships between GRCM and RE....	90
6.0	CONCLUSION	98
	APPENDIX A - Case Study A: Registration of Businesses on the Web.....	101
	APPENDIX B - Case Study B: Corporate Intranet Revamp Project.....	119
	APPENDIX C - Case Study C: Travel Automation Information System	136
	APPENDIX D - Case Study D: Financial Management Information System (FMIS).....	151
	REFERENCES	168

LIST OF TABLES - GENERAL

Table 2-1: RE Process Using “Requirements” Fundamental Activities.....	23
Table 2-2: RE Operationalization and Theoretical Justification.....	34
Table 2-3: Dashboard Indicating the RE Level of Capability.....	35
Table 2-4: Rating Guidelines for RE Capability.....	35
Table 3-1: IT Governance Characteristics.....	40
Table 3-2: Risk Management Roles and Responsibilities	50
Table 3-3: Compliance with Legal Requirements.....	57
Table 3-4: Reviews of Security Policy and Technical Compliance.....	59
Table 3-5: System Audit Considerations	61
Table 3-6: GRCM Operationalization and theoretical Justification.....	64
Table 3-7: Dashboard Indicating the GRCM Level of Capability.....	67
Table 3-8: Rating Guidelines for GRCM Capability.....	68
Table 3-9: OC Operationalization and Theoretical Justification.....	69
Table 3-10: Dashboard Indicating the OC Level of Capability	69
Table 3-11: Rating Guidelines for OC Capability.....	70
Table 4-1: Sources of Evidence in Case Research: Strengths and Weaknesses.....	78
Table 4-2: Application of the Positivist Case Study Research	83
Table 4-3: Case Profile Summary.....	85
Table 5-1: GRCM Capability Measurement Framework.....	88
Table 5-2: RE Capability Measurement Framework.....	89
Table 5-3: OC Capability Measurement Framework.....	89

LIST OF TABLES – CASE STUDIES

Table A-1: GRM an Independent Variable with its Constructs and Measures.....	109
Table A-2: GRM Detailed Observations and Estimated Level of Capability.....	111
Table A-3: RE a Dependent Variable with its Constructs and Measures	115
Table A-4: RE Detailed Observations and Estimated Level of Capability	116
Table A-5: OC an Independent Variable with its Construct and Measure.....	118
Table A-6: OC Detailed Observations and Level of Capability.....	118
Table B-1: GRM an Independent Variable with its Constructs and Measures.....	126
Table B-2: GRM Detailed Observations and Estimated Level of Capability.....	128
Table B-3: RE a Dependent Variable with its Constructs and Measures	132
Table B-4: RE Detailed Observations and Estimated Level of Capability	133
Table B-5: OC an Independent Variable with its Construct and Measure.....	135
Table B-6: OC Detailed Observations and Level of Capability.....	135
Table C-1: GRM an Independent Variable with its Constructs and Measures.....	142
Table C-2: GRM Detailed Observations and Estimated Level of Capability.....	144
Table C-3: RE a Dependent Variable with its Constructs and Measures	148
Table C-4: RE Detailed Observations and Estimated Level of Capability	149
Table C-5: OC an Independent Variable with its Construct and Measure.....	150
Table C-6: OC Detailed Observations and Level of Capability.....	150
Table D-1: GRM an Independent Variable with its Constructs and Measures.....	158
Table D-2: GRM Detailed Observations and Estimated Level of Capability.....	160
Table D-3: RE a Dependent Variable with its Constructs and Measures	164
Table D-4: RE Detailed Observations and Estimated Level of Capability	165
Table D-5: OC an Independent Variable with its Construct and Measure	167
Table D-6: OC Detailed Observations and Level of Capability.....	167

LIST OF FIGURES

Figure 2-1: RE Process Decomposition and its Fundamental Activities.....	20
Figure 4-1: Research Conceptual Framework	75
Figure 4-2: Main Components of a Case Study Protocol	78
Figure 4-3: Qualities of a Case Study Report.....	82

ABSTRACT

Richard Bett, Integrating Governance, Risk, and Compliance Management (GRCM) to Enhance Requirements Engineering in Information Technology Projects. (Under the direction of Dr. Stéphane Gagnon.)

A typical Information Technology (IT) project involves a number of disciplines working concurrently throughout a Systems Development Lifecycle (SDLC). Requirements Engineering (RE) is one of the key project activities in the front-end of the lifecycle, generally performed jointly by Business and Systems Analysts.

Several studies of IT project failures have revealed that key factors include a lack of proper IT project management methods, and especially the absence of a well-defined RE process. While PM best practices, both generic and IT-focused, are highly evolved and sufficient to deal with the first factor, there is still a lack of standardized RE framework to serve as a guide for IT projects.

We propose to explore an opportunity to enhance the RE process by integrating emerging best practices in a related discipline, namely Governance, Risk, and Compliance Management (GRCM). Founded on the concepts of Strategic Management, Corporate Governance, and Policy Deployment, GRCM provides a framework for managing organization-wide risks, meet regulatory compliance imposed by the organization's environment, and establish a governance infrastructure to deploy risk management policies and ensuring compliance across multiple projects.

The objective of this thesis is to see if a new GRCM discipline could be integrated in a standard SDLC. It could provide a new basis to improve Software Engineering methods in order to ensure the organization has enterprise-wide coherence into performing RE activities in every IT projects.

The research methodology used in this paper is based on the academic journal entitled "Investigating Information Systems with Positivist Case Study Research" authored by Guy Paré.

We performed a comparative analysis of RE activities in four key enterprise-wide IT projects. Data analysis is performed to see if the two following objectives can be fulfilled.

- a. Develop and validate a new GRCM and RE capability measurement framework
- b. Explore to what extent GRCM capabilities are correlated with RE capabilities

We concluded with a future research section, where examples of moving the GRCM and RE disciplines forward in IT projects are given.

INTRODUCTION

The purpose of this thesis is to explore opportunities that may exist to enhance the RE process, by integrating and applying best practice such as Governance, Risk and Compliance Management (GRCM) in a related discipline. We therefore believe this thesis warrants an empirical approach to see how the RE process can be enhanced.

This paper has six distinctive chapters which includes a conclusion and future research study suggestions. Chapter 1 provides information to situate the reader “in context”. The information includes challenges and success factors to practicing RE in Information Technology Projects, the relevance of Governance, Risk and Compliance Management (GRCM) for RE and concludes with the thesis objectives. Chapter 2 describes (RE) as a process, outlines the various types of requirements, design and development issues with RE, the types of RE problems, the trends affecting the RE process and practices and concludes with the RE capability measurement framework. Chapter 3 explains GRCM as key to an organization, system audit considerations, relates GRCM to other SE practices and concludes with the GRCM capability measurement framework. It also look sat the Organizational Context (OC) as an important factor. Chapter 4 describes the positivist case study research in which this thesis is based on, the research process considered, and the case profiles. Chapter 5 identifies how the research data was collected, gathered and analyzed. It explains how the GRCM and RE capability measurement frameworks are used as instruments as part of the data analysis and how the with-in case and cross- case analysis are performed to identify key relationships between GRCM and RE. In

conclusion, Chapter 6 summarizes the results to support the two research objectives; it identifies the limitations of this study, and possible future research studies.

1.0 RESEARCH OBJECTIVES

Chapter 1 looks at the challenges and success factors identified in the literature as to practicing RE in Information Technology projects, the relevance of GRCM for RE, and concludes with two research objectives that need to be fulfilled as part of this research.

1.1. Challenges and Success Factors as to Practicing RE in Information Technology (IT) Projects

Information Technology projects are implemented on a daily basis, worldwide. Every project is expected to be implemented successfully by the people who sponsor them. High expectations are set and the projects needs to meet them.

Every IT project is different whether it is for an organization or for government. Numerous types of IT projects are implemented to support their business needs. These projects can be the installation of a new network infrastructure, upgrade or purchase of hardware equipment, upgrade or purchase of Commercial off the Shelf (COTS) software, installation of a highly integrated enterprise application such as SAP or the development of an application in house.

From the perspective of software engineering (SE), RE is the first activity of the software process and it is intended to establish what services are required from the system and the constraints on the system's operation and development (Sommerville 2001).

According to the literature review there are challenges and success factors as to practicing RE in IT projects. Getting requirements right might be the single most important and difficult part of a software project (Hofmann 2001). Many

organizations are interested in improving their RE practices and defining RE processes, because of their confidence that RE can be the key to developing successful systems (Kauppinen 2004). As Wiegers points out improving an organization's RE processes is not trivial, and haphazard approaches to process improvement do not often lead to sustainable success (Wiegers 1999).

One of the challenge organization faces is the people's resistance to change (Curtis 1997), (Diaz 1997), (McFeeley 1996), (Zahran 1998). Another challenge is the lack of user involvement. Implementing RE processes throughout the organization, and convincing people to apply RE practices in high-pressure projects can be a considerable challenge (Kauppinen 2004). Another challenge is the lack of resources. Traditionally, RE receives a relatively small percentage of project resources throughout the software life cycle. Project teams expended on average 15.7 percent of project effort on RE activities. Successful projects allocate a significant higher amount of resources to RE (28%) than the average project (Hofmann 2001).

Despite some of the challenges in executing the RE activities there are success factors that are identified as to practicing RE in IT projects.

(Kauppinen 2004) found eight papers (Calvo-Manzano Villalón 2002), (Claus 1999), (Damian 2002), (Hutchings 1995), (Jacobs 1999), (Kauppinen 2001), (Kauppinen 2002), (Salo 1998) that deal with issues relating to the success of RE process improvement. In addition to these eight papers, they also used as reference sources two RE books (Sommerville 1997), (Wiegers 1999) that offer guidance on process improvement.

The following concepts identified by (Kauppinen 2004) summarizes the most frequently identified factors that affect the success of RE process improvement. The frequency of occurrence is cited in the brackets. The concepts are presented in the order of the number of references to them found in the studied RE literature. Each concept is further discussed.

- User involvement [6]
- Benefits of the RE process [6]
- Cultural change [5]
- Continuous RE process improvement [5]
- Evolutionary RE process improvement [4]
- Pilot projects [4]
- Training and education [4]
- Simplicity of the RE process [4]

User involvement – one of the main factors contributing to the institutionalization of a process is the involvement of future process users and management in development of the process from the very beginning (Claus 1999).

Benefits of the RE process – Sommerville and Sawyer argue that one should always try to introduce techniques where everyone involved (not just managers) sees some benefits (Sommerville 1997).

Cultural change – The results of four case studies (Claus 1999), (Hutchings 1995), (Jacobs 1999), (Kauppinen 2001), show that the introduction of RE involves not just a change of process or technology, but also a change in culture.

Continuous RE process improvement – Calvo-Manzano Villalon et al. Encourage companies to manage process evolution by expert support and the application of metrics and corrective actions (Calvo-Manzano Villalón 2002).

Evolutionary RE process improvement – Sommerville and Sawyer recommend organizations to introduce small-scale improvements with a high benefit/cost ratio before expensive new techniques (Sommerville 1997). Wiegers aligns with these statements and argues that instead of aiming for perfection, it is important to develop a few improved procedures and to get started with implementation (Wiegers 1999) .

Pilot projects – According to Claus et al. One of the main success factors of process definition is that at least one software development project is involved from the start of the process improvement initiative and applies the new processes (Claus 1999).

Sommerville and Sawyer also point out that it is important to introduce process changes in pilot projects in order to find out the advantages and disadvantages of the change (Sommerville 1997).

Training and Education – Damian et al. Report that once the RE process was revised, training and leadership was essential for change management (Damian 2002) . In addition Jacobs reports that training only a few persons and hoping in the multiplier-effect is likely to fail (Jacobs 1999). He points out that all parties to be involved in RE have therefore to participate in adequate training (Kauppinen 2004).

Simplicity of the RE process – According to Salo and Kakola, the presence of multiple stakeholders from several functional organizations, some of whom participate in requirements processes in a minor role, implies that these processes, methods and tools should be as simple as possible (Salo 1998).

1.2. Relevance of GRCM for RE

Due to the lack of information in the literature this is an opportunity to seek an answer in regards to the relevance of GRCM for RE. In other words can GRCM be used to enhance the RE process or activities. Even though research on RE has been active throughout the 1990's, there are not many studies concerning RE process improvement (Kauppinen 2004).

To be able to come up with an answer, the need for a new Capability Measurement Framework is required. Actual relationships between GRCM and RE also need to be defined. To proclaim that GRCM has some relevancy with RE, a Capability Measurement Framework needs to be created. This framework should be simple as possible for researchers and practitioners to utilize. The framework should be able to measure the level of capability for both GRCM and RE. Once this is achieved the next step is to actually identify key relationships between the GRCM elements and RE activities. If relationships exist between the GRCM elements and RE activities then it will support GRCM is relevant for RE. To support the possibility that integrating GRCM can enhance RE two research objectives have been identified during the literature review.

- a. Develop and validate a new GRCM and RE capability measurement framework
- b. Explore to what extent GRCM capabilities are correlated with RE capabilities.

These two objectives will be the drivers for this research.

As seen in this chapter there are challenges and success in practicing RE in Information Technology projects. If this paper can support the two research objectives, this will indicate that GRCM can enhance RE and be considered as a success factor in practicing RE in Information Technology projects.

The next chapter describes the RE process, various types of requirements, design and development issues with RE, the types of RE problems, trends, and the new proposed RE capability measurement framework.

2.0 PERFORMING REQUIREMENTS ENGINEERING

This chapter gives an overview of Requirements Engineering (RE), describes the requirements engineering process or activities, identifies the various types of requirements, design and development issues with RE, the types of RE problems, trends affecting RE processes and practices, and describes the new proposed RE capability measurement framework.

2.1. Overview of Requirements Engineering (RE)

"Requirements are considered the heart of system engineering" and that the systems engineering skill of being able to "technically coordinate multiple disciplines" is necessary to requirements engineering work (Gonzales 2005).

We must see requirements engineering as a sociotechnical discipline that requires diverse skills and knowledge (Robertson 2005).

From the perspective of software engineering (SE), RE is the first activity of the software process, and it is intended to establish what services are required from the system and the constraints on the system's operation and development. RE is a particularly critical stage of the software process as errors at the stage inevitably lead to later problems in the system design and implementation (Sommerville 2001).

Requirements engineering (RE) is about defining precisely the problem that the software is to solve (i.e. defining what the software is to do) (Cheng 2007). It's about identifying, communicating and documenting the requirements that the system will need to satisfy.

RE involves understanding the needs of users, customers, and other stakeholders; understanding the contexts in which the to-be-developed software will be used; modeling, analyzing, negotiating, and documenting the stakeholders' requirements; validating that the documented requirements match the negotiated requirements; and managing requirements evolution (Alfonso 2004).

Identifying requirements is a must for all projects despite the type or size of the project. The requirements need to be necessary, unambiguous, concise, consistent, complete, measurable, reachable and verifiable.

2.2. Requirement Engineering Process

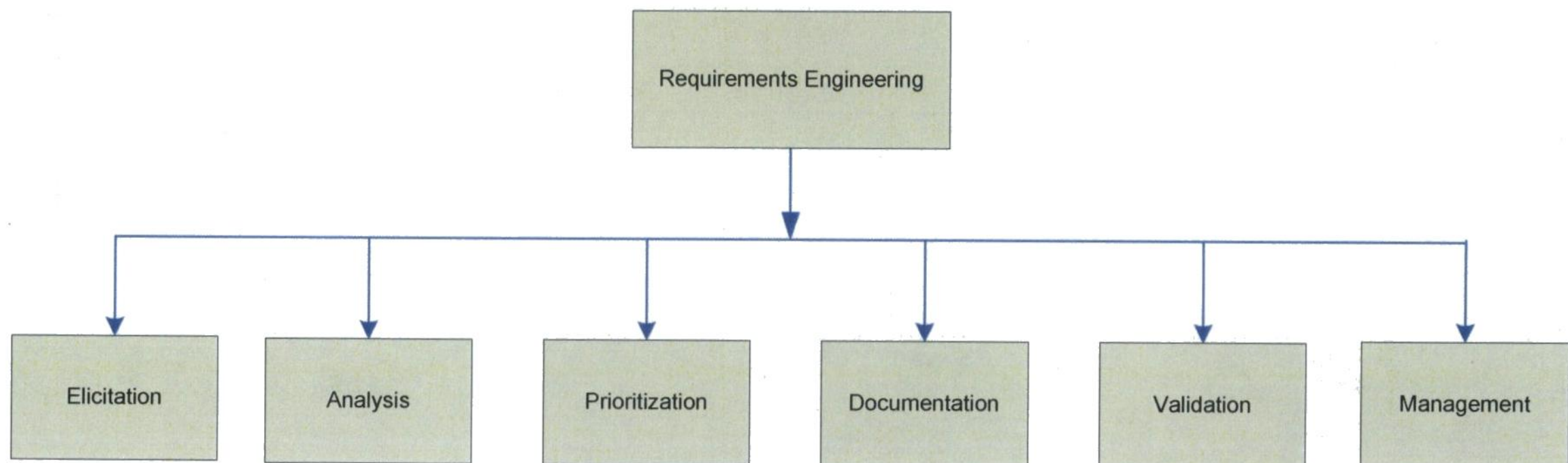
RE is the process by which the requirements are determined. The RE process varies immensely depending the type of application being developed, the size and culture of the companies involved, and the software acquisition processes used (Sommerville 2005).

For large systems such as the military the formal RE stage is built in the system engineering which has many documents in regards to the system and software requirements. For smaller organizations the RE process might consist of work sessions or brainstorming sessions. Despite the size of the organization or system basic RE process activities can be identified.

According to the literature review the requirement engineering process vary from one author to another. Figure 2-1 identifies the RE process decomposition and its

fundamental activities as viewed by the author. Information from various authors (Table 2-1) was gathered to assist the author in drawing Figure 2-1.

Figure 2-1 RE Process Decomposition and its Fundamental Activities



Each of the fundamental activities of the RE process including the methodologies, strategies, techniques, analyses and tools are describe next.

2.2.1. Elicitation

Elicitation is where stakeholders, contextual requirements, metaphors and personas are identified. This is where the system requirements are defined, what problem needs to be solved and the system boundaries to set. It comprises activities that enable the understanding of the goals, objectives and motives for building a proposed software system (Cheng 2007).

To perform this activity, techniques, analyses and tools such as questionnaires, surveys, interviews, brainstorming sessions, focus groups, JAD sessions, analysis of existing documents, prototyping and animation are used.

2.2.2. Analysis

The analysis checks to ensure the requirements are a necessity and not a nice to have or a desire. It ensures the requirements are consistent, clear, complete and feasible (within budget and available development schedule). Any conflicts in requirements are resolved by negotiating with the stakeholders and then requirements are prioritized. The analysis also looks if the requirements can be aligned with Commercial of the Shelf (COTS) if applicable.

Some analysis look for well-formedness errors in requirements, where an “error” can be ambiguity ((Berry 2004),(Feathers 2004), (Kaiya 2006), (Sawyer 2005), (Wasson 2006), inconsistency (Campbell 2002), (Engels 2001), (Nentwich 2003) or incompleteness.

Other analyses look for anomalies, such as unknown interactions among requirements (Carlshamre 2001),(Hausmann 2002), (Robinson 2003), possible obstacles to requirements satisfaction (Lutz 2006), (van Lamsweerde 2000), or missing assumptions (Baker 2005). Both types of analyses reveal misunderstanding or questions about the requirements that usually call for further elicitation (Cheng 2007).

To perform this activity, techniques, analyses and tools such creating a checklist, consistency checking, inspections, risk management, impact analysis and requirements selection are applied.

2.2.3. Prioritization

Some projects may have constraints such as budget, limited resources and schedule. The client selects features providing the greatest benefit to users with the highest priority.

Requirements need to be prioritized by the client and developer to respect the constraints.

As per (Firesmith 2004) an activity is required for the prioritization and classification of requirements. The main focus of this activity is to ensure the requirements are prioritized and classified.

2.2.4. Validation

Validation is a task where requirements identified by the stakeholders are what they really need (Ryan 1993). To perform this task or activity, techniques, analyses and tools such as requirement reviews, requirement testing, simulation, animation and model checking are used. Requirement validation usually results in stakeholders sign-off.

2.2.5. Documentation

A Functional Requirement Document (FRD) including use-cases is usually created by a business analyst, accepted by the stakeholders and approved by the business client. This process is iterative if the IT technology project deals with software improvement. The documents need to ensure the requirements interpretation are clear for stakeholders and software developers (IEEE 1984).

2.2.6. Requirements Management

All requirements are stored, captured and managed during the project. Other activities such as scenario management, feature management, global RE and control of requirements and changes are considered. To perform this task, techniques, analyses and tools such traceability and stability are practiced.

Table 2-1 describes activities that are fundamental to most RE processes. Included in this table are the methodologies and strategies for each RE activity supported by various authors (column A), and techniques, analyses and tools and supported by various authors (column B).

Table 2-1: RE Process Using “Requirements” Fundamental Activities

RE Activities	Methodologies, Strategies	Authors (A)	Techniques, Analyses and Tools	Authors (B)
Elicitation	<ul style="list-style-type: none"> Identify Stakeholders 	(Sharp 1999), (Daniela 1999)	<ul style="list-style-type: none"> Questionnaires Surveys Interviews 	(Nuseibeh 2000)
	<ul style="list-style-type: none"> Identify Contextual Requirements 	(Cohene 2005), (Sutcliffe 2006)	<ul style="list-style-type: none"> Analyse existing documents 	(Nuseibeh 2000)
	<ul style="list-style-type: none"> Identify Methaphors and Personas 	(Pisan 2000), (Potts 2001), (Aoyana 2005)	<ul style="list-style-type: none"> Brainstorming Sessions 	(Nuseibeh 2000), (Maiden 2005)
	<ul style="list-style-type: none"> What the system requirements are? 	(Cohene 2005), (Sutcliffe 2006),	<ul style="list-style-type: none"> Focus Groups/JAD sessions 	(Maiden 1996)
	<ul style="list-style-type: none"> What problem needs to be solved, identify system boundaries 	(Nuseibeh 2000)	<ul style="list-style-type: none"> Prototyping Animation 	(Davis 1992) (Magee 2000)

Table 2-1: RE Process Using “Requirements” Fundamental Tasks (cont.)

RE Activities	Methodologies, Strategies	Authors (A)	Techniques, Analyses and Tools	Authors (B)	
Analysis	<ul style="list-style-type: none"> Negotiation 	(Easterbrook 1994), (Sommerville 1997)	<ul style="list-style-type: none"> Checklist 	(Wasson 2005)	
	<ul style="list-style-type: none"> Aligning requirements with COTS 	(Alves 2002), (Rolland 2001)	<ul style="list-style-type: none"> Consistency Checking 	(Engels 2001), (Heitmeyer 1996)	
	<ul style="list-style-type: none"> Conflict Management 		(Robinson 2003), (Sommerville 1997)	<ul style="list-style-type: none"> Inspections 	(Fagan 1986), (Parnas 1987)
				<ul style="list-style-type: none"> Risk Management 	(Feathers 2004)
				<ul style="list-style-type: none"> Impact Analysis 	(Krishnamurthi 2005)
				<ul style="list-style-type: none"> Requirements selection 	(Regnell 2003), (Sutcliffe 2003)
Prioritization	<ul style="list-style-type: none"> Prioritization and classification of requirements 	(Firesmith 2004)	<ul style="list-style-type: none"> Ensure requirements are prioritized and classified 	(Moreira 2005)	
Validation	<ul style="list-style-type: none"> Verify with stakeholders the requirements - what they really need. 	(Ryan 1993)	<ul style="list-style-type: none"> Simulation 	(Thompson 1999)	
			<ul style="list-style-type: none"> Animation 	(Heidenheimer 1998)	
			<ul style="list-style-type: none"> Model Checking 	(Chan 1998), (Easterbrook 2001)	
Documentation	<ul style="list-style-type: none"> Requirement interpretation is clear for stakeholders and software developers 	(IEEE 1984)			

Table 2-1: RE Process Using “Requirements” Fundamental Tasks (cont.)

RE Activities	Methodologies, Strategies	Authors (A)	Techniques, Analyses and Tools	Authors (B)
Requirements Management	• Scenario management	(Alspaugh 2001)	• Traceability Information	(Cleland-Huang 2004), (Hayes 2006)
	• Feature management	(Weber 2002)	• Stability Analysis	(Bush 2003)
	• Global RE	(Damian 2006)		
	• Control of Requirements and Changes	(Sommerville 2005)		

N.B. This table was compiled using references from well-known authors.

2.3. RE in General

This section looks at various types of requirements, the design and development issues with RE, the types of RE problems, the trends affecting the RE processes and practices and the RE capability measurement framework/instrument.

2.3.1. Various Types of Requirements

Requirements can be identified at several levels such as functional requirements, non-functional requirements and technical (Build) requirements.

Functional requirements indicate what the system shall do. It describes the functions that the system is to execute; for example, software for a humidifier that records the humidity in the air. These requirements are part of the users/customers (Standish 2003)

responsibility to define, even though they may abdicate the initial specifications to the development team. Functional requirements are independent on any design constraints or technical implementations.

The functional requirements consist of business requirements, user requirements and functional requirements itself. The following describes the functional requirements at a high level.

Business requirements are higher-level statements of the goals, objectives, or needs of the enterprise. They describe such things the reasons why a project is initiated, the things that the project will achieve, and the metrics which will be used to measure its success (IIBA 2006).

User requirements are statements of the needs of a particular stakeholder or class of stakeholders. They describe the needs that a given stakeholder has and how that stakeholder will interact with a solution. User Requirements serve as a bridge between Business Requirements and the various classes of solution requirements (IIBA 2006). They are gathered during the elicitation task.

The next level of requirements to be considered is the non-functional requirements.

Non Functional requirements represent how the software must perform once it is developed. Systems qualities are often expressed as non-functional requirements, also called quality attributes (Boehm) . These requirements address the ilities : (suitability, accuracy, interoperability, compliance, security, reliability, efficiency, maintainability,

portability and quality in use as described by the ISO (International Organization for Standardization) standards in (ISO/IEC 9126) and performance criteria.

Another level of requirements to be considered is the Technical (Build) Requirements

Technical (Build) Requirements - These project requirements are defined by how the software will be developed or built to satisfy the functional and non-functional requirements. Technical requirements include the physical implementation characteristics of the project and include for example, programming language, CASE or other tools, methods, work breakdown structure, etc. (Dekkers 2005). It would also include a platform such as UNIX, Linux or Windows.

It becomes quite difficult to analyze the functional and non-functional requirements in a single module because the target users of each requirement might be different. (Ranjan 2006)

2.3.2. Design and Development Issues with RE

In the traditional RE, requirements are typically prioritized once. All stakeholders involved in the RE process get together at the beginning of the definition project phase to identify, analyze, prioritize and negotiate the requirements. A requirements document is then created and distributed to the stakeholders for review and acceptance. Once the requirements document is accepted and approved the requirements are baselined. The designers and developers can then start to design and build the software according to the requirements.

Traditional approaches try to produce enough documentation to be able to answer all questions in the future. To be able to do so, they need (1) anticipate future questions and (2) answer them in a concise and understandable manner. Both things are difficult – this is why writing good requirements documents is so hard (Paetsch 2003).

The client is mainly involved in the early stage of the project and not throughout the whole development process. The bulk of the effort of RE does occur early in the lifetime of a project, motivated by the evidence that requirement errors, such as misunderstood or omitted requirements, are more expensive to fix later in the project lifecycles (Boehm 1981) (Nakajo 1991).

RE uses interviews to identify and gather information on requirements. The interviewee may respond according to his perception of how he or she see things and not necessarily communicate on how the organization sees it as a whole. This may lead to requirements misunderstanding.

This software process is time consuming and expensive. It may take some time before all or most requirements are nailed down before development can begin. If a requirement change is necessary during the development stage this will cause project delays.

RE relies on extensive rigorous documentation to ensure everyone is on the same page when it comes to deliverables. One change in the process requires many changes in the documentation. This is particular an issue when the software needs to be maintained in the long run.

In traditional RE, many factors drive requirements prioritization—for example, business value, risks, cost, and implementation dependencies. Clients identify the features that provide them the greatest benefit; developers identify technical risks or implementation difficulties.

2.3.3. Type of RE Problems

When asked about general problems practitioners are having in software development, all focus groups indicated RE. A project manager states “I don’t believe that we spend enough time up front of the project doing all the work, understanding exactly what we need to do and consequently we learn as we go through and have to keep changing the requirements” (Beecham 2003).

The types of RE problems practitioners are experiencing are organizational and technical RE problems. An analysis suggest a need to help practitioners manage organizational activities along with technical aspects of the RE process (Beecham 2003).

2.3.4. Trends Affecting RE Processes and Practices

Major challenges may arise from emerging trends in software systems. According to (Cheng 2007) trends reflect changes in stakeholders’ needs, and as such they directly affect RE processes and practices. The following are some of the pressing needs and challenges in RE.

1. **Scale.** Software systems are increasing in size. This means it is becoming more complex and requires more attention to ensure the requirements are well defined.

More stakeholders will be involved in defining requirements thus requiring better techniques to merge various types of requirements into a single coherent story (Cheng 2007).

2. **Security.** As computing systems becomes more pervasive and portables carry more and more consumer or personnel related information they will become the centre of attacks. The security will pose challenges to RE that may exceed other non-functional requirements (Cheng 2007).
3. **Tolerance.** The SE and RE community will need to be more tolerant when it comes to security and correctness expectations. (Shaw 2002) discusses the need to accept “sufficient correctness” for complex systems, instead of striving for absolute correctness that may lead to brittle systems.
4. **Increased Reliance on the Environment.** There is a rise of systems of systems, consisting of hardware, software and people all of which may be loosely or tightly joined together. The RE technologies and tools for reasoning about the integration of physical environment, human behaviour, interface devices and software system are not yet mature (Cheng 2007).
5. **Self-management.** There is a growing interest in self-managing systems, in which the software system is aware of its context and is able to react and adapt to changes in either its environment or its requirements (Kramer 2007). These systems require different perspectives on the types of requirement information in contrast to

traditional approaches which typically focus on static goals or functionality (Cheng 2007).

6. **Globalization.** Global software development is an emerging paradigm shift towards globally distributed development teams (Herbsleb 2007). This shift is motivated by the desire to exploit a 24-hour work day, to capitalize on global resource pools, decrease costs, and be geographically closer to the end-consumer (Damian 2006).

This poses two main challenges to RE.

- First - New or extended RE techniques are needed to support outsourcing of downstream development tasks, such as design, coding and testing.
 - Second - To enable effective distributed RE. Future requirement activities will be globally distributed. The requirement analyst will likely be working with geographically distributed stakeholders and distributed development teams may work with in-house customers. It is not just geographically distributed, but distributed in terms of time zone, culture and language (Cheng 2007).
7. **Methodologies, Patterns and Tools.** More work is required on how to interconnect various types of requirements models. Well-defined approaches to interrelating requirement, goals, scenarios, data, functions, state-based behaviour and constraints are needed to address this problem. (Cheng 2007). More requirements management tools such as Requisite Pro from the Rational Unified Process (RUP) suite or

Dynamic Object Oriented Requirement System (DOORS) by Telelogic should be used to identify, control, track and manage requirements.

8. **Requirements Reuse.** Reuse existing requirements artefacts. One of the most strategic forms of requirement reuse is product lining, where related products are considered as a product family, and their co-development is planned from the beginning. Common requirements are collected from the family of products in reusable templates that can be adapted to derive the requirements for an individual product.

Development of reference models for specifying requirements will become more evident in many domains of application. The development of requirements models from scratch is reduced. (Cheng 2007) This will help move many software projects from being creative design to being normal design (Maibaum 2000).

9. **Richer models.** Required for capturing and analysing non-functional requirements.

These are also known as “ilities” and have defied clear characteristics for decades (Maibaum 2000).

10. **Effectiveness of RE Technologies.** Practitioners need hard evidence that new-technology is cost-effective, in order to justify the overhead in training and in process documentation of changing their development process (Cheng 2007).

According to the SWEBOK “requirements will change and this change must be managed by continuing to “do” requirements engineering throughout the life-cycle of the project. It is time to admit it is not “ideal” or even “rational” to start with a detailed requirements definition at the beginning of a software development process; the requirements specification should be developed as on-going part of the project (Poppendieck).

Today the business environment is dynamic and organizations needs to keep up with changes to remain competitive. IT plays an important role in ensuring the business is operating and is able to do what is suppose to do by ensuring the proper application software is available and maintained. More software development approaches are being sought by organizations including government to ensure their processes are adaptable to changes.

2.4. RE Capability Measurement Framework

This section partly covers the first objective identified in section 1.2 of this paper. To build the RE capability measurement framework, RE constructs are used. Table 2-2 outlines the RE activities, the operationalization statements or constructs which indicates how each activity should be practiced, the metrics used to measure the construct level of integration (Fully Integrated “FI”, Semi Integrated “SI”, and Not Integrated “NI”) and references from re-known authors to support the constructs.

Table 2-2 outlines the RE activities, constructs, the measures and authors.

Table 2-2: RE Operationalization and Theoretical Justification

RE - Activities	Operationalization (Constructs)	Measure (FI,SI,NI)	Author
Elicitation	<ul style="list-style-type: none"> All requirements need to be identified by some means. 		(Nuseibeh 2000)
	<ul style="list-style-type: none"> The client needs to be involved 		(Crawford 1994)
Analysis	<ul style="list-style-type: none"> Negotiation and conflict management is important. 		(Easterbrook 1994), (Sommerville 1997)
Prioritization	<ul style="list-style-type: none"> The requirements need to be prioritized and classified. 		Firesmith 2004)
Validation	<ul style="list-style-type: none"> The requirements need to be validated by the client. 		(Ryan 1993)
Documentation	<ul style="list-style-type: none"> The requirements need to be clear so there are no misinterpretations of requirements by the developer. 		(IEEE 1984)
Management	<ul style="list-style-type: none"> Requirement changes need to be managed 		(Sommerville 2005)

As a result of Table 2-2 an “RE Capability Measurement Framework” is created.

Table 2-3 displays the “RE Capability Measurement Framework” in a dashboard format.

The framework is used to identify the RE activity as well as its level of capability. The level of capability for each activity is represented by a number and color for visual effect.


In this instance  represents a high level of capability for each RE activity. This is the optimum level of capability an organization can achieve. In this paper it is considered the baseline.

Table 2-3: Dashboard Indicating the RE Level of Capability

Requirements	Level of Capability
Elicitation	3
Analysis	3
Prioritization	3
Validation	3
Documentation	3
Management	3

Table 2-4 “Rating Guidelines for RE capability” gives the significance of the numbering and the color coding.

Table 2-4: Rating Guidelines for RE Capability

RATING GUIDELINES			
Capability Categories	Green (3) Meets requirements	Yellow (2) Warning Zone	Red (1) Intervention Required
1. Requirements management Deals with the gathering and approval of the functions and features to be implemented in the proposed solution.	The RE process is in line with the baseline. <ul style="list-style-type: none"> • Elicitation • Analysis • Prioritization • Validation • Documentation • Management Constructs are achieved.	The RE process is not in line with the baseline and may impact the project such as scope, schedule or costs.	One or more RE activity does not meet the baseline thus needs to be intervened by senior management.

As seen in this chapter, six activities were identified as part of the RE process. These activities were considered to build the RE capability measurement framework. Metrics were used to indicate the level of capability for each RE activity. This framework will indicate which RE activity is acceptable and which ones require more attention. To meet objective (a) identified in section 1.2 a GRCM capability measurement framework will need to be identified.

The next chapter discusses governance, risk, compliance management and system audit consideration. It also relates GRCM to other SE practices and describes the proposed GRCM capability measurement framework.

3.0 GOVERNANCE, RISK AND COMPLIANCE MANAGEMENT (GRCM)

This chapter identifies some of the elements that are part of GRCM. It looks at IT governance, tools such as COBIT, ITIL and ISO 17799, risk management, project risk management, minimizing risks, compliance, compliance with legal requirements, security policy and technical compliance. It considers system audits; it relates GRCM to other SE practices and describes a new GRCM capability measurement framework.

3.1. Foundations of GRCM as Best Practices

Due to the Sarbanes-Oxley Act (SOX) of 2002, board members and senior managers have been required to focus more consistently and more carefully than ever before with matters of governance, risk management and compliance. Governance, Risk and Compliance management must be treated as a separate area of concern by boards and management. Even though GRCM touches everything across the organization; it still needs to be treated by management as a unique set of objectives and interrelated processes.

“Organizations recognize the importance of implementing good corporate governance, risk management, compliance and ethics into business operations, but often struggle, with how to put these principles into practice” (Mitchell 2005).

Sarbanes –Oxley (SOX) requires something like Control Objectives for Information and Related Technology (COBIT), a set of best practices for IT governance, or The

Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework, a framework better suited for risk evaluation/management.

The next section defines what Governance, Risk Management and Compliance means in an IT perspective as well as the standards and best practices used.

3.2. Governance

The word governance is a derivative of the verb “to govern”. According to the Concise Oxford dictionary “govern” has many meanings. To rule with authority, to sway, rule, influence, regulate or determine (person, his acts, course or issue of events).

Since the collapse of large corporations such as Enron, WorldCom, Adelphia Communications, Global Crossing and Tyco International the concepts of governance have moved into the spotlight.

The corporate governance structure of an organization is defined by its corporate charter, bylaws and formal policy. The importance of good corporate governance increasingly is recognized worldwide as a best practice (OECD 2000).

“Corporate governance initiatives aim to create boards that are more responsive to shareholders by attempting to balance the CEO’s power with the board’s ability to act as genuine custodians of the organization” (Conger 2001).

Governance helps leaders maintain organizations that are sustainable, accountable to shareholders, capable of returning profit to them, and worthy on the marketplace.

3.2.1. Overview of IT Governance

The Information Technology Governance Institute defines IT governance as “the leadership, organizational structures and process that ensure that the enterprise’s IT sustains and extends the enterprise’s strategies and objectives.” (Larsen 2006)

A primary proponent of IT governance is the Information Systems Audit and Control Association (ISACA) which in 1998 created the IT Governance Institute (ITGI). The institute was created to clarify and provide guidance on existing and future issues concerning governance, security and assurance.

IT governance provides the structure that links IT processes IT resources and information to enterprise strategies and objectives. IT governance integrate optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring and evaluating IT performance. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage (ITGI 2005)

Table 3-1 describes the IT Governance Characteristics.

Table 3-1: IT Governance Characteristics

Primary Proponent	<ul style="list-style-type: none"> • Information Systems Audit and Control Association - ISACA
Refers to the working of	<ul style="list-style-type: none"> • Board of directors • Executive Team • Rest of organization
Core Principles	<ul style="list-style-type: none"> • Align with corporate strategy • Provide good IT value • Manage IT risks
Intent	<ul style="list-style-type: none"> • Ensure integrity of IT systems • Inclusion of independent audit • Have appropriate controls for: <ul style="list-style-type: none"> - Monitoring IT risk - Controlling IT assets - Compliance with laws and regulations • Records management • Enable the enterprise by exploiting opportunities and maximizing benefits of IT • Ensure resources are used responsibly
Driving Factors	<ul style="list-style-type: none"> • Growth in complexity of the organization • Globalization • Rapid advance of technology • Accelerated decision making • More proactive board • Shareholders activism • Increase news coverage • Increased competition • Recent scandals • Increased emphasis on accountability • Need to manage the management process • Need for meaningful communication • Focus on organizational capital, value and balance • Expanding role of IT <ul style="list-style-type: none"> - Corporate/enterprise governance support - Strategic initiatives - Knowledge management - Privacy/security/continuity • Proliferation of technology “solutions”
Key elements	<ul style="list-style-type: none"> • IT strategic planning • IT control framework • IT project management • IT asset management • IT policies/standards/processes <ul style="list-style-type: none"> - Corporate - Business units - Information services

Source: (Hamaker 2003)

Even though Information Technology is managed by the director of information services the overlying responsibility lies with the board of directors and the senior management team.

3.2.2. IT Governance Focus Areas

Organizations and government need to focus on specific areas if they want to implement IT Governance in their environment. According to (ISACA 2007) the focus areas that needs to be considered are the following:

Strategic Alignment:

- ensuring the business and IT plans are linked
- maintaining the IT value proposition
- aligning IT operations with enterprise operations

Value Delivery:

- executing the value proposition throughout the delivery cycle
- ensuring that IT delivers the promised benefits against the strategy
- concentrating on optimizing costs and proving the intrinsic value of IT

Resource Management:

- optimal investment in critical IT resources: process, people, applications, infrastructure and information.

Risk Management:

- requires risk awareness by senior corporate officers
- a clear understanding of the enterprise's appetite for risk
- transparency about the significant risks to the enterprise
- embedding of risk management responsibilities into the organization

Performance Management:

- tracks and monitors strategy implementation
- project completion
- resource usage
- process performance and service delivery

3.2.3. IT Governance Tools

By adopting a standard IT governance framework, organizations may realize a number of benefits (Spafford 2003). The use of standards and best practices is being driven by the client requirement for improved performance, value transparency and increased control over IT activities.

If we focus on IT standards, three standards exist that seem to be at the forefront today.

They are: COBIT, ITIL and ISO 17799.

3.2.3.1. COBIT

Control Objectives for Information and related Technology (COBIT) is the world's leading IT governance and control framework. It is based on established frameworks such as the Capability Maturity Model (CMM), ISO 9000, ITIL and ISO 17799. COBIT was first published by ITGI in April 1996. ITGI's latest update is COBIT 4.1.

COBIT does not include process steps and tasks because, although it is oriented toward IT processes, it is a control and management framework rather than a process framework (OGC 2005).

COBIT is an IT governance framework and supporting tool set that allow managers to bridge the gap between control requirements, technical issues and business risks. The COBIT framework is comprised of 34 high-level control objectives and 318 detailed control objectives that have been designed to help businesses maintain effective control over IT.

COBIT enables clear policy development and good practice for IT control throughout organizations. It emphasizes regulatory compliance and assists organizations in increasing the value attained from IT. COBIT has become the integrator for IT best practices and the umbrella framework for IT governance because it is harmonized with other standards such as ITIL for service management and ISO 17799 for security and is continuously kept up to date.

As per (ISACA 2007) COBIT supports IT Governance by providing a framework to ensure that:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

Currently, the ISACA is finalizing a special version of COBIT called "QuickStart" for small and medium-sized businesses. It will contain a subset of the COBIT standard and focus on elements that are viewed as most critical for organizations that lack the resources to pursue the full standard.

3.2.3.2. ITIL

The Information Technology Infrastructure Library (ITIL) is the world-wide defacto standard in Service Management (Behr 2004). It is maintained by the United Kingdom's Office of Government Commerce (OGC) and was developed with the input of many organizations beginning in the late 1980s. It offers a common framework for all the activities of the IT department, as part of the provision of services, based on the IT infrastructure. ITIL is not a method, instead it offers a framework for planning the essential processes, roles and activities, indicating the links between them and what lines of communication are necessary (itSMF 2006).

These activities are divided in processes, which when used together provide an effective framework to make the IT service Management more mature. ITIL focuses on critical

business processes and disciplines needed for delivering high-quality services (Larsen 2006).

A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks (itSMF 2007).

Two principal concepts characterize the basic thinking of ITIL: holistic service management and customer orientation.

The Service Management processes are at the center of the ITIL framework, and are divided into the two core areas of Delivery and Support.

- The service delivery describes the services the customer needs to support their business and what is required to provide these services. The service delivery processes are addressed in the ITIL book on Service delivery.
- The service support describes how the customer and users can get access to the appropriate services to support their activities and the business, and how those services are supported. The service delivery processes are addressed in the ITIL book on Service delivery.

3.2.3.3. ISO 17799

The ISO 17799 or the counterpart of British Standard BS 7799 is a standard for information security including a comprehensive set of controls and best practices in information security. It was first release by ISO in December 2000.

Compliance with ISO 17799 and BS 7799 ensures that an organization has established a certain compliance level for each of the ten categories covered (Ma 2005), i.e. security policy, security organization, asset classification and control, personnel security, physical and environment security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance (ISO 2002), (BS 2002).

It can be seen as a basis for developing security standards and management practices within an organization to improve reliability on information security in inter-organizational relationships (ITGI 2005). Standards are very beneficial for organizations. They are recognized internationally, tested by various people and can be shared.

COBIT, ISO 17799 and ITIL all serve as excellent frameworks by which to improve IT governance.

3.3 Risk Management

Risk management must be considered as an essential management function of the business. Risk management should be a line management function not a staff function. It is a management activity and is integral with decision-making. As Peter Drucker, celebrated “father of modern management” puts it, “a decision that does not involve risk, probably is not a decision.” (Herold)

3.3.1. Overview of Risk Management

The management of risks is a cornerstone of IT governance, ensuring that the strategic objectives of the business are not jeopardized by IT failures (ITGI 2005). Executives should ensure that all risks at the business level are identified and that the business impact of an IT risk is agreed and signed off.

For IT governance to be effective, senior management should review and approve the risk action plan, agree to priorities and commit the necessary resources to execute the plan effectively. The IT Governance Institute (ITGI) recommends that an IT executive committee with representation of all stakeholders review and approve the plan collectively on behalf of the board (ITGI 2005). The business should be responsible in creating a risk management plan, provide the resources and funding to maintain the risk management plan and ensuring the risks are managed to protect the business interests.

IT management has the responsibility to support, and monitor the risks associated to IT and ensuring the risks are being controlled or mitigated.

Auditors' services can be used by senior management to highlight inadequate risk management practices or risks that were not considered or improperly addressed.

Auditors should align audits with key business risks and known areas of weakness.

The ITGI also recommends that boards review the risk management approach for the most important IT-related risks on a regular basis, at least annually (ITGI 2005).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a project to develop a framework that would be readily usable by management to evaluate and improve the organizations' enterprise risk management (ERM). The framework provides key principles and concepts, a common language and clear direction and guidance. (ITGI 2005)

It is the next step towards the expansion of the process "Added value" of the Sarbanes-Oxley act.

As per (ITGI 2005) according to COSO ERM Framework, enterprise risk management includes:

- Aligning risk appetite
- Enhancing risk responses
- Reducing operational surprises
- Identifying and managing multiple and cross-enterprise risks
- Seizing opportunities
- Improving deployment of capital

ERM assist organizations in managing risks in a coherent approach throughout the organizations. It ensures that all risks are considered as to not jeopardize the business strategy. ERM also ensures effective reporting and compliance with rules and regulations.

Risk management consists of two main elements:

- Risk Analysis - assessing and combining the risk probability of occurrence and impact (PMI 2004). To inform the organization of the risk exposure so appropriate decisions on managing the risk can be made.
- Risk Management - includes the processes concerned with conducting risk management planning, identification, analysis, responses and monitoring and control (PMI 2004).

Once the organization has identified the risk exposure it can set strategies for managing risks and assign an officer of primary interest (OPI) to take action.

Dependent on the type of risk and the impact to the business, the board or management may choose to:

- Mitigate, by implementing control.
- Accept, acknowledging that the risk exists.
- Transfer, the risk by sharing with other partners or insurance.
- Avoid, by taking another direction.

The US National Institute of Standards and Technology (NIST) *Risk Management Guide* (NIST) states that the principal goal of an organization's risk management process should be to protect the organization and its ability to perform its mission, not just its IT assets. It should not be treated primarily as a technical function carried out by the IT experts who

operate and manage the IT systems, but as an essential management function of the organization.

The ITGI's *Board Briefing on IT Governance, 2nd Edition* suggests the roles and responsibilities listed in Table 3-2.

Table 3-2: Risk Management Roles and Responsibilities

Role	Responsibility
Board of Directors	<ul style="list-style-type: none"> • Be aware about IT risk exposures and their containment • Evaluate the effectiveness of management's monitoring of IT risks
IT Strategy Committee	<ul style="list-style-type: none"> • Provide high-level direction for sourcing and use of IT resources, e.g. strategic allowances • Oversee the aggregate funding of IT at the enterprise level
CEO	<ul style="list-style-type: none"> • Adopt a risk, control and governance framework • Embed responsibilities for risk management in the organization • Monitor IT risk and accept residual IT risks
Business Executives	<ul style="list-style-type: none"> • Provide business impact assessments to the enterprise risk management process
CIO	<ul style="list-style-type: none"> • Assess risks, mitigate efficiently and make risks transparent to the stakeholders • Implement an IT control framework • Ensure that roles critical for managing IT risks are appropriately defined and staffed.

Table 3-2: Risk Management Roles and Responsibilities (cont.)

Role	Responsibility
Project Manager	<ul style="list-style-type: none">• Creates a risk management plan including an action plan• Performs risk management at the project level• Ensure risks are recorded, controlled and maintained in a risk register• Reports the risks status to stakeholders

Source: (ITGI 2003)

3.3.2. Project Risk Management

The Risk Management Plan describes how project risks management will be structured and conducted on the project. Three topics that may serve well as the elements of a Project Risk Management Plan are; sensitivity analysis, evaluating alternatives and inventory risks and actions (Schuyler 2001). A risk management planning process identifies, analyzes, plans, responses, tracks, and monitors risks which may have a negative or positive impact on the organization.

In order to increase project performance a project's risk management profile needs to vary according to the project's risk exposure (Barki 2001). The higher the project risk the higher the level of planning is required by management.

The project manager should organize a weekly team meeting to go over the risks and particularly focus on the ones having a high to medium probability and high to medium

impact. The PM should ask the OPI the progress made in reference to the risk and see if he or she can do something to decrease the criticality of the risk. In some instances the risk may be reported to the project steering committee or forwarded to higher authority for direction.

3.3.3. Minimize Risks

Every organization handles risks differently. Despite the approach, the end result is to ensure risks are minimized. However, there are approaches that should be considered. ITGI provides the following list of best practices to ensure IT risks are managed effectively:

- Embed into the enterprise an IT governance structure.
- Establish an audit committee.
- Appoint and oversee an internal audit function.
- Coordinate and review project documentation using risk-based approach.
- Define the scope and charter of the audit committee.
- Monitor how management determines what IT resources are needed to achieve strategic objectives.
- Pay attention to IT control failures and weaknesses in internal control.
- Evaluate the scope and quality of management's ongoing monitoring of IT risks and controls.
- Ascertain that risk analysis is part of the overall management's strategic planning process.

If IT risks are managed effectively the end results will be minimized risks.

If organizations are already managing risk, ensuring transparency into operational procedures or providing accurate financial reports, they've already on their way to compliance (Forbes 2006).

3.4 Compliance

3.4.1. Overview of Compliance

According to the Concise Oxford dictionary "compliance" is an action in accordance with request, command. The Merriam-Webster's collegiate dictionary definition is that compliance is the act or process of complying to a desire, demand, proposal, or regimen or with coercion. Compliance is the conformity in fulfilling official requirements.

Compliance is "A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes" (I.T.G.I. 2000).

Organizations need to think more about security today. They need to protect their customer's data as well as their employee's data and ensure the utmost safeguards are in place to minimize security risks. To do this, the organization needs to establish rules in accessing the information and a mechanism to monitor compliance against regulations and procedures.

The Sarbanes-Oxley Act of 2002 (SOX) was passed by the congress of the United States in response to financial fraud and deceptions in firms such as Enron, whose public auditing firm failed to discover this abuse.

Senior management, must be actively or become involved with and accountable for the accuracy of the data used in financial reporting: and that public auditors remain independent of their client's firm (Haworth 2006).

One of the most pressing issues facing IT managers today is the creation of and maintenance of rigorous internal controls (Goff 2005). The process of ensuring that processes and systems operate as intended is known as internal control (Board 2004). Control activities "include a range of activities as diverse as approvals, authorizations, verifications of duties (COSO 1992).

Since the Sarbanes-Oxley act was implemented managers of publicly-held companies have been required to confirm internal controls are in place. A part of these internal controls are used to ensure IT security policies and procedures support the business processes.

The Sarbanes-Oxley Act is intended to ensure the accuracy and integrity of financial statements reported by publicly-held companies (Wagner 2006). Section 404 of the Act goes beyond auditing accounting ledgers to require an in-depth assessment of the integrity of the business processes and information systems that generates information ultimately reported in financial statements (Vance 2007).

This requirement has necessitated substantial costs to both corporate management and IT auditors required to implement internal controls. It is estimated that a total of six billion dollars were spent on Sarbanes-Oxley compliance in 2005 (Goff 2005).

The sections of the Sarbanes-Oxley Act that are most relevant to the IT departments are discussed here:

- **Management Control.** Top managers need to institute controls and be accountable for the operation of those controls. They need to report to the Security and Exchange Commission (SEC) any fraudulent transactions, embezzlement and material changes of the company.
- **Systems or Processes.** The Act is concerned with any automated or manual processes that may have an impact on the overall operation of the organization.
- **Evaluation.** Under section 302 and 404 of the Act, management is required to assess and report the effectiveness of its internal control. Each public accounting firm that prepares an independent audit of a financial report must also attest to the management's assessment of its internal controls over financial reporting (Hardesty 2003).
- **Disclosure Controls.** Section 409 of the Act requires real-time disclosure of "material changes in the financial condition or operations of the issuer (Hardesty 2003).

- **Internal Controls over Financial Reporting.** The principal focus of the Sarbanes-Oxley Act is in the controls over financial reporting. In section 404 of the Act, the management is required to include in its annual report an assessment of its “internal controls” structure and procedures for financial reporting (Hardesty 2003). This assessment must provide evidence that management has adequately designed control activities and that control activities have been tested to be operating effectively (Board 2004).

In addition, an audit report needs to be performed by a registered accounting firm attesting the management’s assessment of its internal control.

3.4.2. Compliance with Legal Requirements

Organizations need to operate within legal requirements. Any unlawful activities performed by the organization may cause the organization to be scrutinized. This can potentially lead to the organization’s closure. It is up to senior executives and the board to ensure that all activities are compliant with legal requirements to ensure the viability of the organization.

The following sections summarize the relationship of each ISO area to the ACT. The far right column in Table 3-3, Table 3-4 and Table 3-5 provides specific components about the applicability to SOX for each of the ISO components.

Table 3-3 represents Compliance with legal requirements as per ISO 17799 section A.12.1.

Table 3-3: Compliance with Legal Requirements

A.12 Compliance	
ISO/IEC 17799 Sections	Notes
A.12.1 Compliance with legal requirements	
A.12.1.1 Identification of applicable legislation	Because of continuing changes in the law and the regulatory environments (the Sarbanes-Oxley Act of 2002 is an example), this must be an ongoing activity
A.12.1.2 Intellectual property rights (IPR)	These areas are covered by existing legislation or legal precedent.
A.12.1.3 Safeguarding of organizational records	These areas are covered by existing legislation or legal precedent.
A.12.1.4 Data protection and privacy of personal information	These areas are covered by existing legislation or legal precedent; however, recent incidents may motivate additional legislation that may impose stricter requirements.
A.12.1.5 Prevention of misuse information processing facilities	These areas are covered by existing legislation or legal precedent.
A.12.1.6 Regulation of cryptographic controls	These areas are covered by existing legislation.

Table 3-3: Compliance with Legal Requirements (cont.)

A.12 Compliance	
ISO/IEC 17799 Sections	Notes
A.12.1 Compliance with legal requirements	
A.12.1.7 Collection of evidence	There seems to be no intent in the Act to mandate prosecution of those who commit fraud, only that the fraud be detected and reported (Hardesty 2003). Therefore, it appears that procedures for the collection of evidence are beyond the scope of the Act.

Source: (Haworth 2006)

3.4.3. Reviews of Security Policy and Technical Compliance

Every organization requires some security policy to ensure their information assets are protected. The content of the policy depends on the organizational goal to protect its information. The policy needs to be up-to-date to meet the industry standard and distributed to everyone in the organization.

The security policy is a formal statement of rules that how the organization manages, protects and uses their information assets.

An information security policy document prepared in accordance with ISO 17799 (2000, pp.1-2) should contain references to applicable legislation and regulation. Existing documentation must be updated to reflect the Sarbanes-Oxley Act of 2002 as being an item for compliance. (Haworth 2006)

ISO 17799 / BS 7799 standards are used to help management build a structure that ensures an appropriate level of information security for the organization. It does not prevent data intrusion or data loss.

Table 3-4 indicates the reviews of security policy and technical compliance as per ISO 17799 section A.12.2

Table 3-4: Reviews of Security Policy and Technical Compliance

A.12 Compliance	
ISO/IEC 17799 Sections	Notes
A.12.2 Reviews of security policy and technical compliance	
A.12.2.1 Compliance with security policy	A component that the ISO Standard has in common with the Act and as No.2 legal compliance (above), the ISO Standard suggests no timing other than “regular reviews” (ISO, 2002, p.64).

Table 3-4: Reviews of Security Policy and Technical Compliance (cont.)

A.12 Compliance	
ISO/IEC 17799 Sections	Notes
A.12.2 Reviews of security policy and technical compliance	
A.12.2.2 Technical compliance checking	A component that the ISO Standard has in common with the Act and as No.2 legal compliance (above), the ISO Standard suggests no timing other than “regular reviews” (ISO, 2002, p.64).

Source: (Haworth 2006)

3.5 System Audit Consideration

The SOX Act lacked specifics and in part because implementation details are left to a board created by the Act. The board’s implementation guidelines were published in 2003 (Hardesty 2003). Many organizations turned to external auditors for guidance on how to interpretate and implement parts of the SOX Act that is relevant to them.

One of the sections in the act (A.12.2) refers to security. It is very important that once a process for security assets is in place that auditors schedule a security audit regularly to determine if the process is working properly. This is done to ensure that whatever is in the security policy it is being followed by the appropriate people in the organization.

This is also an opportunity for the auditor to perform balances and checks and find any weaknesses that exist in the process. Recommendations are also given as to the type of controls required to maintain or improve the security of its critical system.

Table 3-5 shows the system audit considerations as per ISO 17799 section A.12.3.

Table 3-5: System Audit Considerations

A.12 Compliance	
ISO/IEC 17799 Sections	Notes
A.12.3 System audit considerations	
A.12.3.1 System audit controls	These form part of the IT general controls and provide one means for management to evaluate the effectiveness of other IT controls (PCAOB 2004)
A.12.3.2 Protection of system audit tools	The suite of tools used to audit information systems must be reviewed regularly to ensure coverage of the IT general controls and the specific controls over financial reporting. These appear to fall under the monitoring area of Paragraph 49 (PCAOB 2004)

Source: (Haworth 2006)

In summary, ISO/IEC 17799 compliance, including increased managerial evaluation of controls and improved documentation can bring the organization into reasonable compliance with the mandate of the Sarbanes-Oxley Act of 2002. (Haworth 2006)

3.6 Relating GRCM to Other SE Practices

While not part of our GRCM framework, we can identify some other key relationship with SE practices and methods.

According to ANSI/IEEE Standard 1471-2000, architecture is defined as the “fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution” (Winter 2008).

Enterprise architecture (Lankhorst 2005) (Lankhorst 1998) (Zachman 1987) provides a way to enable cross-functional, cross-discipline collaboration essential to articulating and implementing strategic business requirements.

In order to provide and maintain alignment between Business-IT enterprise architecture management has to be anchored in IT as well as in business. In contrast to traditional architecture management approaches like IT architecture, software architecture of IS architecture, EA explicitly incorporate “pure” business-related artifacts and therefore provides a chance to align business and IT constructs more effectively (Winter 2008).

Many EA frameworks are widely used such as the Zachman Framework, The Open Group Architecture Framework (TOGAF), the Federal Enterprise Architecture Framework (FEAF), and the ARIS Framework. The selection of the appropriate framework must meet the defined requirements of the organization. The framework should enable to describe, develop and maintain enterprise architecture.

EA is not only an instrument for (strategic) IS/IT planning, but for corporate planning and business related functions such as compliance management, business continuity management, or risk management as well.

Only when 'purely' business related artifacts are covered by EA, important activities like business continuity planning, change impact analysis, risk analysis, and compliance management can be supported effectively (Winter 2008).

3.7 GRCM Measurement Framework

This section covers the first objective identified in section 1.2 of this paper. To build the GRCM capability measurement framework, GRCM constructs are used. Table 3-6 outlines the GRCM elements, the operationalization statements or constructs which indicates how each element should be practiced, the metrics used to measure the construct's level of integration (Fully Integrated "FI", Semi Integrated "SI", and Not Integrated "NI") and references from re-known authors to support the constructs.

Table 3-6 outlines the GRCM elements, constructs, measures and authors.

Table 3-6: GRCM Operationalization and Theoretical Justification

Independent Variable (GRCM)	Operationalization (Constructs)	Measure (FI, SI, NI)	Authors
Governance			
<ul style="list-style-type: none"> IT Strategic Planning 	<ul style="list-style-type: none"> Adequate infrastructure 		(Ewushi-Mensah 1997)
	<ul style="list-style-type: none"> First point of escalation for variance to project cost and timescale 		(Ewushi-Mensah 1997)
	<ul style="list-style-type: none"> Assign ownership and accountability for technical risks 		(Ewushi-Mensah 1997)
<ul style="list-style-type: none"> IT Project Management 	<ul style="list-style-type: none"> Employ sound project management techniques and controls 		(Ewushi-Mensah 1997), (Phelan 2002), (Weigers 1998)
	<ul style="list-style-type: none"> Small scope and scale 		(Parr 2000)
	<ul style="list-style-type: none"> Request realistic and adequate budget 		(Jurison 1999)
	<ul style="list-style-type: none"> Adhere to standardized specifications 		(Sumner 1999)
<ul style="list-style-type: none"> IT Control Framework 	<ul style="list-style-type: none"> Development of management control structure 		(Sumner 1999)
	<ul style="list-style-type: none"> Create an accountability framework 		(Neela 2003)
	<ul style="list-style-type: none"> Establish an access control to information 		(Kim 2007)
<ul style="list-style-type: none"> IT Asset Management 	<ul style="list-style-type: none"> To prevent damage to assets and interruptions to business activities 		(Kim 2007)
	<ul style="list-style-type: none"> To maintain appropriate protection of corporate assets 		(Kim 2007)
	<ul style="list-style-type: none"> To ensure that information assets receive an appropriate level of protection 		(Kim 2007)

Table 3-6: GRCM Operationalization and Theoretical Justification (cont.)

Independent Variable (GRCM)	Operationalization (Constructs)	Measure (FI, SI, NI)	Authors
Governance			
<ul style="list-style-type: none"> IT Processes 	<ul style="list-style-type: none"> Establish IT processes 		(Mingay 2002)
	<ul style="list-style-type: none"> Establish conformance process 		(Connell 2004)
	<ul style="list-style-type: none"> Establish performance processes 		(Connell 2004)
Risk Management			
<ul style="list-style-type: none"> Embed into the project/enterprise an IT governance structure 	<ul style="list-style-type: none"> The structure needs to be accountable, effective and transparent 		(ITGI 2003), (Knut S 2006)
<ul style="list-style-type: none"> Support auditing and monitoring operations 	<ul style="list-style-type: none"> Support a variety of different auditing and monitoring operations 		(Zoellick 2005)
	<ul style="list-style-type: none"> Establish an auditing committee 		(ITGI 2003)
Risk Management			
<ul style="list-style-type: none"> Monitor and Track risk regularly 	<ul style="list-style-type: none"> Active monitoring and regular viewing of risks 		(ITGI 2003), (PMI 2004)
	<ul style="list-style-type: none"> Risk monitoring and control 		(PMI 2004)
	<ul style="list-style-type: none"> Breaking the project into smaller pieces to better addressed and manage risks. 		(May 1996)
<ul style="list-style-type: none"> Risk analysis is part of the project ongoing monitoring of IT risks and controls 	<ul style="list-style-type: none"> Perform analysis and assessment of risks including asset value, vulnerability and threat. 		(Kim 2005), (Rex 1991), (Ron 1988)
	<ul style="list-style-type: none"> Require risk decision process supported by risk analysis, identification and evaluation. 		(ITGI 2003)
Compliance			
<ul style="list-style-type: none"> Brief project mandate to committees involved 	<ul style="list-style-type: none"> Ensure adequate visibility of the project. 		(Weigers 1998), (Jurison 1999)

Table 3-6: GRCM Operationalization and Theoretical Justification (cont.)

Independent Variable (GRCM)	Operationalization (Constructs)	Measure (FI, SI, NI)	Authors
Compliance			
<ul style="list-style-type: none"> • Ensure IT alignment with business 	<ul style="list-style-type: none"> • Align IT with enterprise objectives. 		(Luftman 1993), (Allen 2005)
	<ul style="list-style-type: none"> • Ensure that IT investments decisions and performance measures demonstrate the value of IT. 		(Hardy 2006), (Allen 2005)
<ul style="list-style-type: none"> • Comply with regulations, policies and standards 	<ul style="list-style-type: none"> • Systems to be compliant with organizational security, policies and standards. 		(Kim 2007)
	<ul style="list-style-type: none"> • Ensure compliance with legislation, regulations, security policies and rules. 		(Moulton 2003)
<ul style="list-style-type: none"> • Consider security in the project 	<ul style="list-style-type: none"> • Need to consider security “from the ground up”. 		(Lipner 2004), (Schumacher 2001)

As a result of Table 3-7 a “GRCM Capability Measurement Framework” is created.

Table 3-7 displays the “GRCM Capability Measurement Framework” in a dashboard format. The framework is used to identify the GRCM elements as well as its level of capability. The level of capability for each element is represented by a number and color for visual effect.


In this instance  represents a high level of capability for each GRCM elements. This is the optimum level of capability an organization can achieve. This represents the baseline.

Table 3-7: Dashboard Indicating the GRCM Level of Capability

GRCM Elements	Level of Capability
Governance	
• IT Strategic planning	3
• IT Project Management	3
• IT Control Framework	3
• IT Asset Management	3
• IT Processes	3
Risk Management	
• IT Governance Structure	3
• Audit and Monitor	3
• Monitor and Track Risks regularly	3
• Perform Risk Analysis	3
Compliance	
• Brief Project Mandate to Committees	3
• Ensure IT Alignment with Business	3
• Consider Security	3

Table 3-8 “Rating Guidelines for GRCM capability” gives the significance of the numbering and the color coding.

Table 3-8: Rating Guidelines for GRCM capability

RATING GUIDELINES			
Capability Categories	Green (3) Meets requirements	Yellow (2) Warning Zone	Red (1) Intervention Required
2. GRCM Considers Governance, risks and compliance as a discipline.	The development of RE is in line with GRCM elements. Baseline	The implementation of GRCM is not in line with the baseline and may impact the project such as scope, schedule or costs.	One or more of the GRCM elements does not meet the baseline thus needs to be intervened by senior management.
Governance – these elements are fully integrated (FI)	<ul style="list-style-type: none"> • IT Strategic planning • IT Project Management • IT Control Framework • IT Asset Management • IT Processes 		
Risk Management – these elements are fully integrated (FI)	<ul style="list-style-type: none"> • IT Governance Structure • Audit and Monitor • Monitor and Track Risks regularly • Perform risk analysis 		
Compliance – these elements are fully integrated (FI)	<ul style="list-style-type: none"> • Brief project mandate to committees • Ensure IT Alignment with business • Consider security 		
	Constructs are achieved.		

3.8 Measuring the Level of Capability in the Organizational Context

The method for measuring the level of capability for the Organizational Context (OC) dimension is the same method used for the RE and GRCM dimensions. Table 3-9 indicates the OC as a control variable, the operationalization statement or construct, the metric to measure the level of capability (FI, SI, NI) and the author that supports the construct.

Table 3-9 – OC Operationalization and Theoretical Justification

OC – Control Variable	Operationalization or Construct	Measure (FI, SI, NI)	Author
Senior Management Leadership/Commitment	<ul style="list-style-type: none"> Senior management need to be committed to the project and demonstrate leadership 		(Frame 1994)

As a result of Table 3-9 a “GRCM Capability Measurement Framework” is created.

Table 3-10 displays the “OC Capability Measurement Framework” in a dashboard format. The framework is used to identify the OC construct as well as its level of capability. The level of capability for the construct is represented by a number and color for visual effect.


In this instance  represents a high level of capability for the OC dimension. This is the optimum level of capability an organization can achieve. This represents the baseline.

Table 3-10: Dashboard Indicating the OC Level of Capability

Organizational Context Element	Level of Capability
<ul style="list-style-type: none"> Senior Management Leadership/Commitment 	3

Table 3-11 “Rating Guidelines for OC capability” gives the significance of the numbering and the color coding.

Table 3-11: Rating Guidelines for OC Capability

RATING GUIDELINES			
Capability Categories	Green (3) Meets requirements	Yellow (2) Warning Zone	Red (1) Intervention Required
<p>3. Organization Context (OC)</p> <p>Deals with management leadership and commitment.</p>	<ul style="list-style-type: none"> • The project has Senior Management leadership and commitment <p>Construct is achieved.</p>	<p>The project is uncertain of the senior management leadership and /or commitment.</p>	<p>The project has no senior management leadership and /or commitment.</p>

In this chapter various elements of the GRCM dimensions were identified. These elements were considered to build the GRCM capability measurement framework.

Metrics were used to indicate the level of capability for each GRCM element.

This framework will indicate which GRCM element is acceptable and which ones will require more attention. The OC context was also considered since it will play a major role in determining the relationship between the GRCM elements and RE activities.

The next chapter discusses the research methodology, the research process, and case profiles.

4.0 RESEARCH METHODOLOGY

The research methodology used in this paper is based on the academic journal entitled “Investigating Information Systems with Positivist Case Study Research” authored by Guy Paré. The case study method will be used to conduct the study, gather data, analyse the data and obtain findings according to the results. In this chapter, the positivist case study research is discussed as well as the research process. Topics such as the design and conduct of the case study, analysis of the case study, the analysis of the case study evidence, writing up the case study report and case profiles will be described.

4.1 Positivist Case Study Research

For at least two decades acceptance of case study research has been increasing in the information systems (IS) discipline (Benbasat 1987);(Lee 1989);(Orlikowski 1992);(Alavi 1992);(Yin 1993);(Markus 1997);(Klein 1999). According to (Paré 2004) the case study methodology is particularly well-suited to IS research. It emphasizes both the emergence of theoretical categories solely from evidence and an incremental approach to case selection and data gathering (Eisenhardt 1989).

Yin, defines the scope of a case study as “an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident” (Yin 2003).

A few IS researchers formulated a set of methodological principles for case studies that are consistent with the convention of positivism (Paré 2004). They recommended that case researchers should provide clearer descriptions of where their topics fit into the

knowledge building process, detail the case selection criteria, and provide detailed information about the data collection process (Benbasat 1987).

Applying a well-defined methodology along the lines described in this paper will help to position case studies even more in the mainstream of IS research (Paré 2004).

Just as case research can be positivist, interpretive or critical, (Myers 1987), positivist case study can research can be descriptive, exploratory or explanatory. Each of these three approaches can be either single or multiple-case studies (Yin 2003).

This research is confined to an exploratory positivist multiple-case study.

An exploratory case study, whether based on single or multiple cases, is aimed at defining questions, constructs, propositions, or hypothesis to be the object of a subsequent empirical study (Yin 1993).

This research examines if a GRCM and RE capability measurement framework can be developed and validated as well if a correlation exists between GRCM capabilities and RE capabilities. Four IT projects are used as part of the multiple-case studies.

There is no current GRCM and RE capability measurement framework available to the community. The intent of this study is to come up with such a framework. This will also help in identifying if a correlation exists or not between the two domains GRCM and RE.

The following section looks at the research process and its various steps.

- 1) “What is the relationship between GRCM and RE?”
- 2) “How can GRCM capabilities and RE capabilities be measured?”

These two research questions will provide guidance to assist in capturing specific data items such as (i.e. project selection, constructs for GRCM and RE, level of measurement, possible relationships between GRCM and RE).

Prior Theorizing

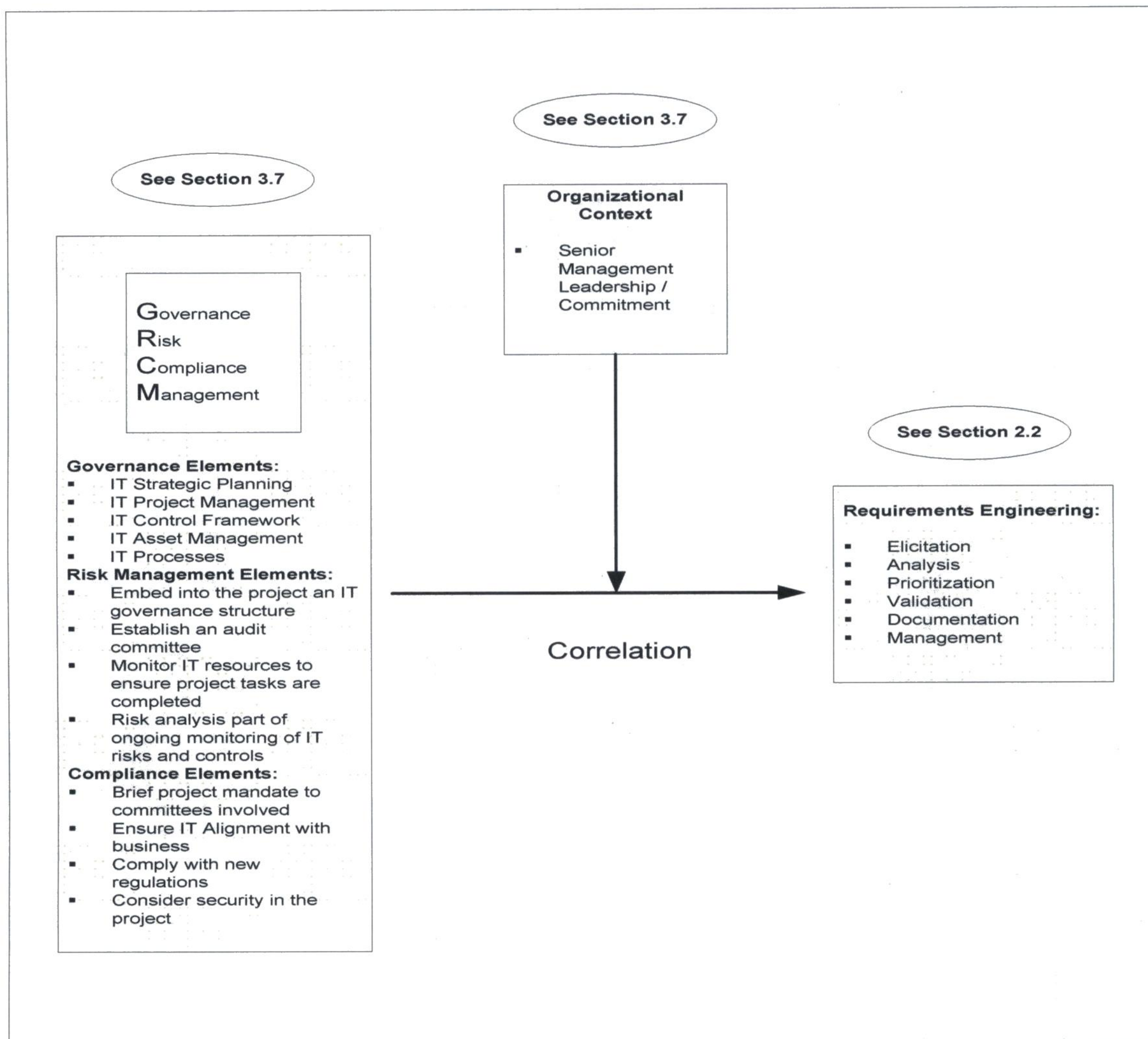
A conceptual framework becomes a “researchers first cut at making some explicit theoretical statements” (Miles 1994).

As per the research conceptual framework Figure 4-1, there are thirteen elements considered in the GRCM dimension, six activities in the RE dimension and one in the Organizational Context dimension.

A link between the GRCM dimension and the RE dimension is drawn to show possible relationships. This link needs to exist if one implements GRCM hoping to enhance RE.

As per the author’s experience the organizational context needs to be considered if the relationship between GRCM and RE is to be looked at.

Figure 4-1: Research Conceptual Framework



Unit of Analysis

The third component of a case study is related to the fundamental problem of defining what the “case” is (Yin 2003).

A case can be defined as an “integrated system” bounded by time and place (Stake 1995). In this paper an embedded case design was used to investigate the relationship of multiple unit of analysis.

- IT Governance
- Requirements Engineering
- Organizational Context

This was chosen to be in accordance with (Guha 1997). The definition of the unit of analysis must be related to the way the initial research questions are defined and the generalization desired at the project’s completion (Yin 2003).

Number and Selection of Cases

An issue in research design is the decision of selecting one or more cases in the research. The number of replications for case studies is basically a matter of discretionary and judgment choice; it depends upon the certainty a researcher wants to have about the multiple-case results (Yin 2003). Ideally, researchers should stop adding cases when theoretical saturation is reached (Eisenhardt 1989). Theoretical saturation is the point at which incremental learning is minimal because the researchers are observing phenomena seen before (Glaser 1967).

Selection of cases represents another important but difficult aspect of case study research (Yin 2003), (Lee 1989), (Benbasat 1987), (Eisenhardt 1989). In a multiple-case design, the selection of cases should follow a literal replication logic (conditions of the case lead

to predicting the same results) or a theoretical logic (conditions of the case lead to contrasting results) (Yin 2003).

This paper follows literal replication logic since an assumption is made that the multiple-case should provide similar results. The results are unknown until the case studies analysis are performed and the data is validated.

The four case studies selected are based on the fact that the projects were managed by the author. The sampling was done by convenience. All the projects are software engineering projects and were implemented in organizations where security is of concern. The difference in the projects is scope, time, budget and resource skill sets.

According to literature, sampling by convenience is fast and convenient. (Patton 2002) states that this strategy is probably the most common sampling strategy, and the least desirable. This strategy saves time, money and effort, but at the expense of information and credibility.

Use of a Case Study Protocol

Reliability should be considered an important issue in positivist case research (Yin 2003).

The data needs to be reliable as well as able to be validated. It is important to have the final version of the case study reviewed, not just by peers, but also by the participants and informants in the case (Yin 2003). To ensure reliability and validity of the information presented in the case studies, case informants were contacted by the author.

Figure 4-2 shows a typical case protocol that should contain four components.

Figure 4-2: Main Components of a Case Study Protocol

1. An overview of the case study project (objectives, issues, topics being investigated)
2. Field procedures (credentials and access to sites, sources of information)
3. Interview guides and/or survey instruments
4. A guide for case study report (outline, format for the narrative)

Source: (Paré 2004)

4.2.2. Conduct of the Case Study

There are six sources of qualitative evidence identified in case research: documentation, archival records, interviews, direct observation, participant observation, physical artifacts.

In fact, the more all of these techniques are used in the same study, the stronger the case study evidence will be (Yin 1999). Table 4-4 identifies the main types of evidence, their strengths and weaknesses.

Table 4-1: Sources of Evidence in Case Research: Strengths and Weaknesses

Source of Evidence	Strengths	Weaknesses
Documentation	<ul style="list-style-type: none"> - Stable—can be reviewed repeatedly - Unobtrusive—not created as a result of the case study - Exact—contains exact names, references, and details of an event - Broad coverage—long span of time, many events, and many settings 	<ul style="list-style-type: none"> - Retrievability —can be low - Biased selectivity, if collection is incomplete - Reporting bias—reflects (unknown) bias of author - Access—may be deliberately blocked
Archival records	<p>same as above for documentation] precise and quantitative</p>	<p>[same as above for documentation] - accessibility due to privacy concerns</p>

Table 4-1: Sources of Evidence in Case Research: Strengths and Weaknesses (cont.)

Source of Evidence	Strengths	Weaknesses
Interviews	Targeted-focuses directly on case study topic Insightful-provides perceived causal inferences	- Bias due to poorly constructed questions - Response bias - Inaccuracies due to poor recall - Reflexivity-interviewee gives what interviewer wants to hear
Direct observations	- Reality-covers events in real time - Contextual-covers context of event	- Time consuming - Selectivity-unless broad coverage - Reflexivity-event may proceed differently because it is being observed
Participant observation	[same as above for direct observations] - insightful into interpersonal behaviour and motives	[same as above for direct observations] - bias due to investigator's manipulation of events
Physical artifacts	- insightful into cultural features - insightful into technical operations	- selectivity - availability

Adapted from (Yin 2003)

The source of evidence for this research is compared to participant observation. The data collected is a re-collection of events experienced by the author while managing IT projects. The researcher is an active participant in the events being studied. According to Paré this phenomenon often occurs in studies of system development.

Another source of evidence which will be considered in this research are the physical artifacts. Physical artifacts can be tools, instruments, computer outputs, emails, or some other physical evidence that may be collected during the study as part of a field visit (Paré 2004).

Theoretical Saturation

In exploratory as well as in explanatory case study research, data collection must go on until theoretical saturation (Glaser 1967) is reached; namely, when additional qualitative data no longer contributes to anything new about a concept, a construct, or a relationship between constructs.

4.2.3. Analysis of the Case Study Evidence

Inspired by the work of (Miles 1994), Paré divided the data analysis stage into three distinct stages, namely, "Early Steps in Data Analysis," "Within-Case Analysis," and "Cross-Case Analysis." The data analysis stage for this research is explained in the following three distinct stages.

In the Early Steps in Data Analysis as stressed by (Eisenhardt 1989), qualitative data analysis is both the most difficult and the least codified part of the process. According to Paré coding can support case researchers during preliminary analysis steps. Codes are especially useful tools for data reduction.

As part of this research no coding was used.

As stressed by (Eisenhardt 1989), a key step in building theory from case research is within-case analysis. The analytical techniques used in this analysis comprise of an adoption of a dominant mode of data analysis, the use of visual displays, and the review of case reports by key informants.

The dominant mode of data analysis for this research is the explanation building.

Explanation-building, is also considered a form of pattern-matching in which the analysis of the case study is carried out by building an explanation of the case (Paré 2004). This analysis is used to understand the how and why GRCM can enhance RE in IT Projects.

Visual displays such as checklist matrices and dashboards are used throughout this paper indicating the level of GRCM, RE and OC capabilities.

It is very important that the information in the case studies represents the exact situation of the organization at the time of the study. The data needs to be reliable as well as able to be validated. It is important to have the final version of the case study reviewed, not just by peers, but also by the participants and informants in the case (Yin 2003).

To ensure reliability and validity of the information presented in the case studies, case informants have been contacted by the author.

The Cross-Case Analysis is to enhance generalizability. It is to ensure that findings in reference to GRCM make sense beyond a specific case. To deepen the understanding of how GRCM can be used to enhance RE by looking at a broader perspective. Multiple Cases, when adequately sampled and analyzed carefully, can help researchers make sense beyond the reasonable question “Do these findings make sense beyond this specific case?” (Miles 1994).

4.2.4. Writing up the Case Study Report

The case studies written in this thesis, considered the desired qualities of a case study report identified by Lincoln 2002. As per (Lincoln 2002) Figure 4-3 presents the desired qualities of a case study report.

Figure 4-3: Qualities of a Case Study Report

- Resonance criterion (degree of fit between the case study report as written and the set of beliefs under girding the philosophical paradigm which the investigator has chosen to follow);
- Rhetorical criteria (unity, coherence, corroboration, simplicity and clarity);
- Empowerment criteria (fairness, educativeness, and actionability, i.e. the ability of the case study to evoke action on the part of the reader);
- Applicability criterion (extent to which the case study facilitates the drawing of inferences by the reader).

Adapted from (Lincoln 2002)

The following is a summary in which the concept, techniques and tools (Paré 1997) were considered when the case study methodology was applied during this research.

Table 4-5 summarizes how the various concepts, techniques and tools (Paré 2004) drawn from the proposed methodology are applied in the four exploratory case studies in this research.

Table 4-2: Application of the Positivist Case Study Research

Stage	Concept, Techniques and Tools	Research Thesis
1. Design of the case study	Research questions	To what extent. How
	Prior theorizing	Conceptual Framework
	Unit of analysis	Investigate the relationship of multiple unit of analysis. - IT Governance - Requirements Engineering - Organizational Context
	Number of cases	4
	Selection of cases	Literal replication logic
	Case study protocol	Overview of project
2. Conduct of the case study	Qualitative data collection methods	Participant observation Documents
	Quantitative evidence	N/A
	Sampling strategies for interviews	N/A
	Data triangulation	N/A
	Theoretical saturation	Yes
3. Analysis of the case study evidence	Field Notes	Yes
	Reflective Remarks	Yes
	Coding of Raw Data	Yes
	Case Study Data Base	No
	Dominant Mode of Analysis	Explanation Building
	Visual Display Techniques	Checklist Matrices Dashboard
	Project Review	No
	Cross-Case Analysis	Yes
4. Writing up the case study report	Resonance Criteria	Fit with Positivism paradigm
	Rhetoric criteria	Central idea articulated, coherence, corroboration, Clarity
	Empowerment	Evokes action on the part of readers
	Applicability	Practical insights

4.3. Case Profiles

As per the literature review the case study research is accepted as a valid research strategy within the IT/IS community. This paper will utilize the case study strategy to support or not support the research objectives identified in section 1.2 of this paper. Four case studies are used as part of the research. Each case study is an actual case that the author experienced as a project manager.

Table 4-3 outlines the case profile summary. More details on the cases studies are available in the Appendix section.

Table 4-3: Case Profile Summary

Case Profile	Case Study #1	Case Study #2	Case Study # 3	Case Study #4
Case Name	Registration of Services on the Web	Corporate Intranet	Travel Automation Information System	Financial Management Information System
Case Industry	The case study relates to an organization in which a part of their mandate is to ensure security is emphasized.	The case study relates to an organization in which a part of their mandate is to ensure security is emphasized.	The case study relates to an organization in which a part of their mandate is to ensure security is emphasized.	The case study relates to an organization in which a part of their mandate is to ensure security is emphasized.
Case Summary	This organization needs to build a WEB application (in-house) and make it available to the public domain for organizations to register their business across Canada. A set date is legislated to have the web application built and readily available for the businesses to register.	This organization needs to revitalize their internal corporate website to better reflect the services they offer to their clients: interdepartmental. The information should be accurate, reliable, clear and accessible. It should be organized so that the employee, manager or director can go in a specific area of the intranet and retrieve specific information.	This organization needed to automate some of their travel manual processes. More employees were traveling on business and it became difficult for the travel office to keep up. The organization went through an exercise of identifying functional requirements and then met with technical to identify non-functional requirements. An option analysis document was created and a recommendation was given as to whether they should opt for an in-house solution or go with COTS. The first project phase completed in February 2007.	This organization upgraded their existing financial application and needed to ensure all requirements were identified, prioritized and approved, before installing and configuring the application.
Case Context	A look at the organization is taken to see if GRCM is considered throughout the project phases. To identify any gaps when comparing their performance to established GRCM methods. To see if RE is impacted by GRCM. To see how the identified gaps (if any) could be closed in respect to future projects considering using the GRCM discipline.	A look at the organization to see if GRCM is considered throughout the project phases. To identify gaps when comparing their performance to established GRCM methods. To see if RE is impacted by GRCM. To see how the identified gaps (if any) could be closed in respect to future projects considering using the GRCM discipline.	A look at the organization to see if GRCM is considered throughout the project phases. To identify gaps when comparing their performance to established GRCM methods. To see if RE is impacted by GRCM. To see how the identified gaps (if any) could be closed in respect to future projects considering using the GRCM discipline.	A look at the organization to see if GRCM is considered throughout the project phases. To identify gaps when comparing their performance to established GRCM methods. To see if RE is impacted by GRCM. To see how the identified gaps (if any) could be closed in respect to future projects considering using the GRCM discipline.

Table 4-3: Case Profile Summary (cont.)

Case Profile	Case Study #1	Case Study #2	Case Study # 3	Case Study #4
Case Informants	The information gathered on the case study is a re-collection of the author's experience. An outside source involved in the project will be asked to review the case information for its reliability and validity.	The information gathered on the case study is a re-collection of the author's experience. An outside source involved in the project will be asked to review the case information for its reliability and validity.	The information gathered on the case study is a re-collection of the author's experience. An outside source involved in the project will be asked to review the case information for its reliability and validity.	The information gathered on the case study is a re-collection of the author's experience. An outside source involved in the project will be asked to review the case information for its reliability and validity.
Case Outcomes	The project was delivered before the legislative date and deemed successful by the client.	The project was still in the requirements phase when the project manager's contract expired.	The project was not considered by senior management as a priority thus shelving the project until it is required.	The project was delivered on time and deemed successful by the client.

As one can determine from Chapter 4 the research is executed in a methodological way in order to ensure no steps are omitted.

The next chapter covers the data analysis phase. Different activities such as gathering data, analyzing the data, and trying to make sense of it are executed. The Capability Measurement Framework for both GRCM and RE are tested for its usefulness and simplicity. The relationships between GRCM and RE are questioned.

5.0 DATA ANALYSIS

The data analysis was performed in steps. The following are the steps that were considered.

1. Prepare the capability framework for GRCM and for RE
2. Analyze each case studies and record the data results in pre-set tables
3. Roll up the data results from each case studies and insert the data in the GRCM framework and the RE framework
4. Perform an analysis on the results indicated in the frameworks and identify if any relationships exists between GRCM and RE

5.1. Capability Measurement Framework for GRCM and RE

As identified as a research objective, a capability measurement framework is required for both the GRCM and for the RE. This framework is to measure the level of capability for the GRCM elements and the RE activities. Two capabilities frameworks were prepared; one for GRCM and one for RE. Both frameworks are based on constructs, and have metrics (NI, SI, FI) to measure the level of capability.

Table 5-1 displays the “GRCM Capability Measurement Framework” which summarizes the GRCM integration and the level of capability for all four case studies.

Table 5-1: GRCM Capability Measurement Framework

GRCM Elements	Case Study			
	A	B	C	D
	Level of Capability			
Governance				
• IT Strategic planning	3	2	2	3
• IT Project Management	3	2	2	3
• IT Control Framework	2	2	2	3
• IT Asset Management	3	3	3	3
• IT Processes	3	2	2	3
Risk Management				
• IT Governance Structure	2	3	2	3
• Audit and Monitor	1	1	1	1
• Monitor and Track Risks regularly	3	3	3	3
• Perform risk analysis	3	2	2	3
Compliance				
• Brief project mandate to committees	3	3	2	3
• Ensure IT Alignment with business	2	2	2	3
• Comply with regulations, policies and procedures.	3	3	3	3
• Consider security in the project	3	3	3	3

Green (3) = Fully Integrated / full capability

Yellow (2) = Semi Integrated / poor capability

Red (1) = Not Integrated /no capability

Table 5-2 displays the “RE Capability Measurement Framework” which summarizes the RE activities and the level of capability for all four case studies.

Table 5-2: RE Capability Measurement Framework

RE activities	Case Study			
	A	B	C	D
	Level of Capability			
Elicitation	3	2	2	3
Analysis	3	3	2	3
Prioritization	3	2	2	3
Validation	3	3	2	3
Documentation	2	2	2	3
Management	2	2	2	3

Table 5-3 displays the “OC Capability Measurement Framework” which summarizes the OC context and the level of capability for all four case studies.

Table 5-3: OC Capability Measurement Framework

Organizational Context	Case Study			
	A	B	C	D
	Level of Capability			
Senior Management Leadership/Commitment	3	3	2	3

5.2. Within-Case Analysis to Identify Key Relationships between GRCM and RE

As part of the within-case analysis each case study data is recorded and organized in pre-set tables to ensure data integrity as per Appendix (Table A1 to Table D6). The next step is to analyze the data within each case. The dominant mode of data analysis used is the adoption of “explanation building” as per section 4.2.3. Checklists are used in individual cases to record the level of capability for each GRCM elements (A-1, B-1, C-1, D-1) and RE activities (A-3, B-3, C-3, D-3). The results are then rolled up to a summary table (Table 5-1 and Table 5-2) where key relationship between GRCM and RE are sought. The data from the four case studies is used as the primary input to the analysis. Once the within-case analysis is completed the next step is to perform the cross-case analysis.

5.3. Cross-Case Analysis to Identify Key Relationships between GRCM and RE

The purpose of the cross-case analysis is to identify/highlight key relationships between GRCM capabilities and RE capabilities. The data used for this analysis is the results of the four case studies within-case analysis. As seen the data results from the with-in case analysis is easily accommodated by the GRCM framework and the RE framework (Table 5-1 and Table 5-2). Data entry is simple and the information reveals that some key relationships exists between the GRCM capabilities and RE capabilities.

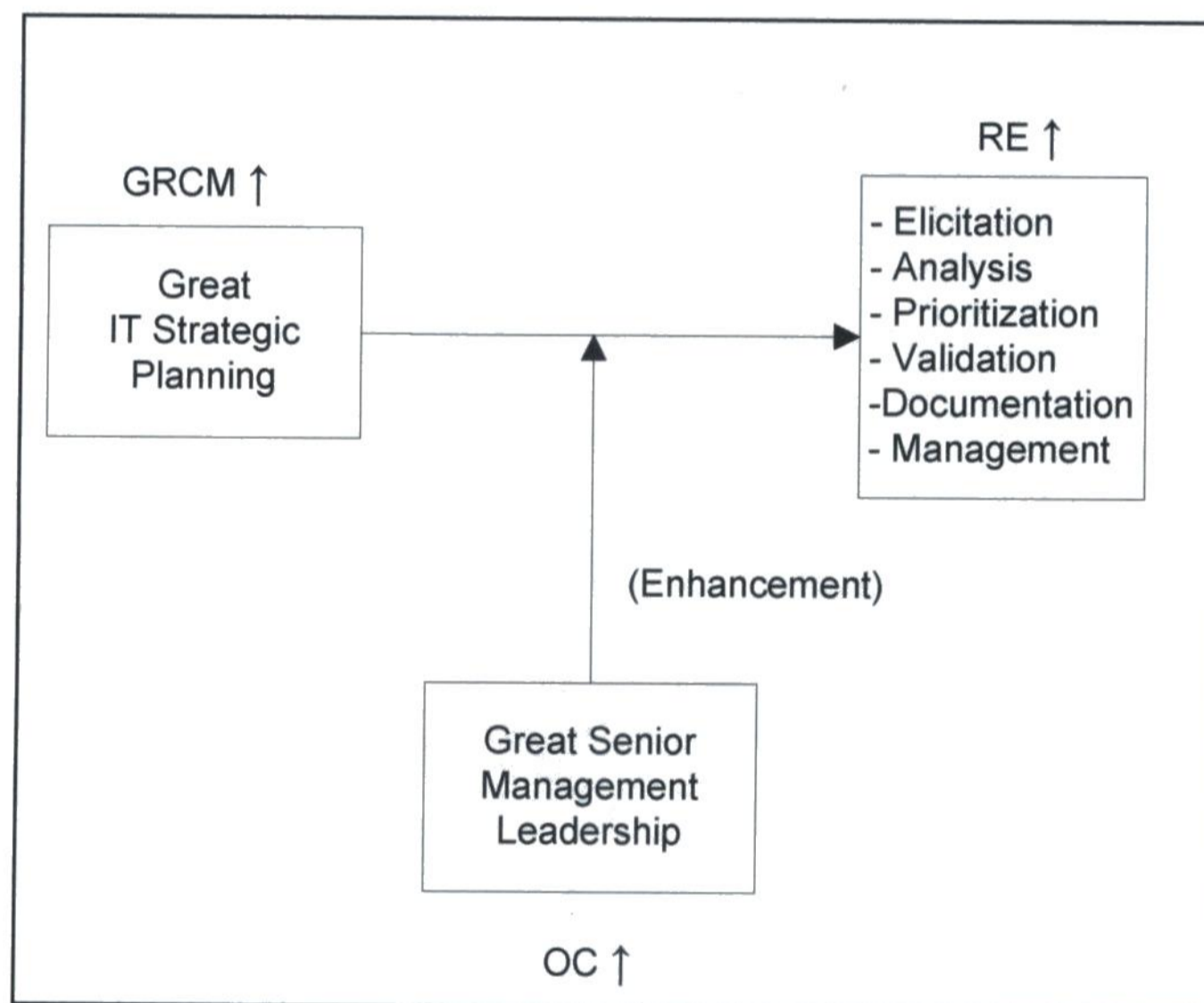
The following cases studies D and A, were selected since they represented both spectrum of the scale. The observations identifies/highlights key relationship between the GRCM capabilities and RE capabilities when using the “Capability Measurement Frameworks”.

Case Study D

According to the GRCM and RE “Capability Measurement Frameworks” results indicate when GRCM elements are at a high level of capability (3), the RE activities tend to reflect the same. The following are five observations to support the results.

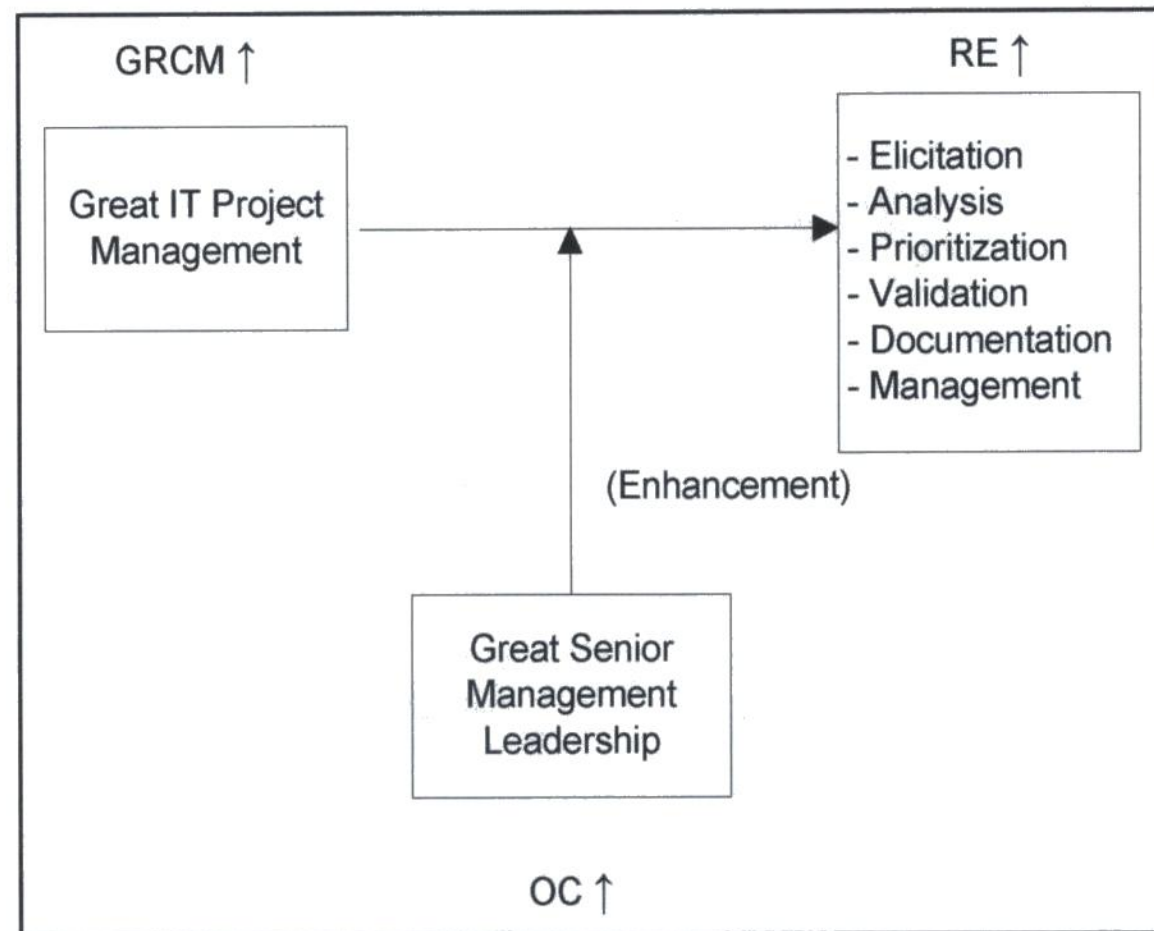
Observation #1

- a. The GRCM element, IT Strategic Planning is at a high level of capability (3).
- b. The RE activities, elicitation, analysis, prioritization, validation, documentation and management are at a high level of capability (3).
- c. The Organizational Context (OC) is at a high level of capability (3).



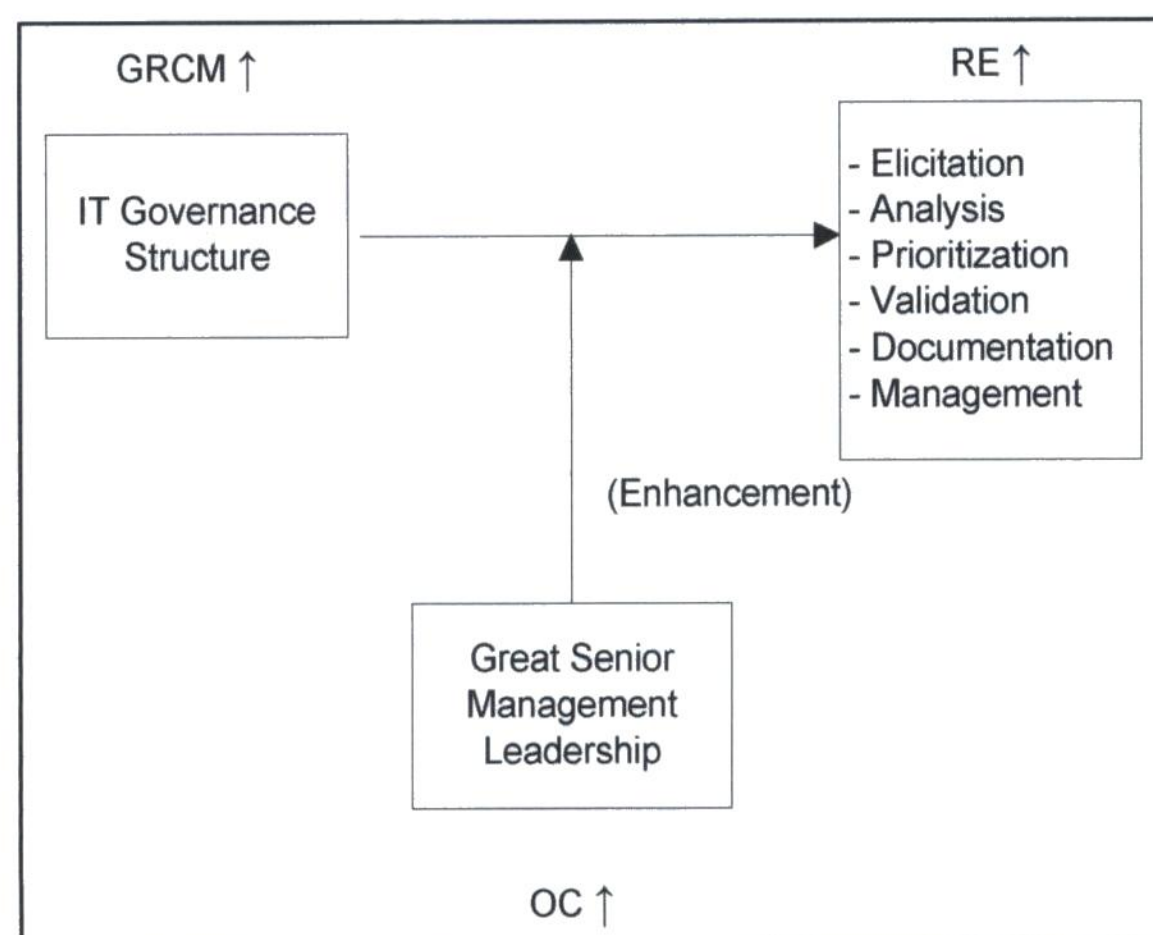
Observation #2

- a. The GRCM element, IT Project Management is at a high level of capability (3).
- b. The RE activities, elicitation, analysis, prioritization, validation, documentation and management are at a high level of capability (3).
- c. The Organizational Context (OC) is at a high level of capability (3).



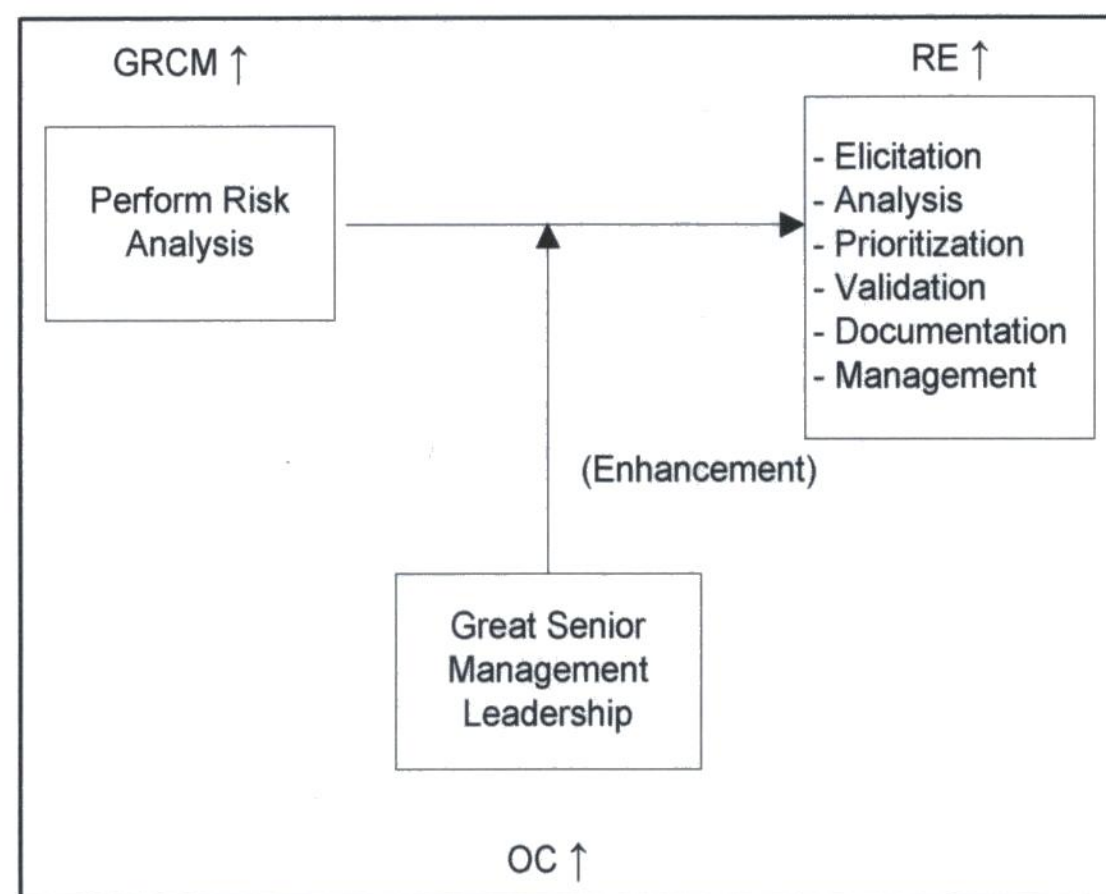
Observation #3

- a. The GRCM element, IT Governance Structure is at a high capability (3).
- b. The RE activities, elicitation, analysis, prioritization, validation, documentation and management are at a high level of capability (3).
- c. The Organizational Context (OC) is at a high level of capability (3).



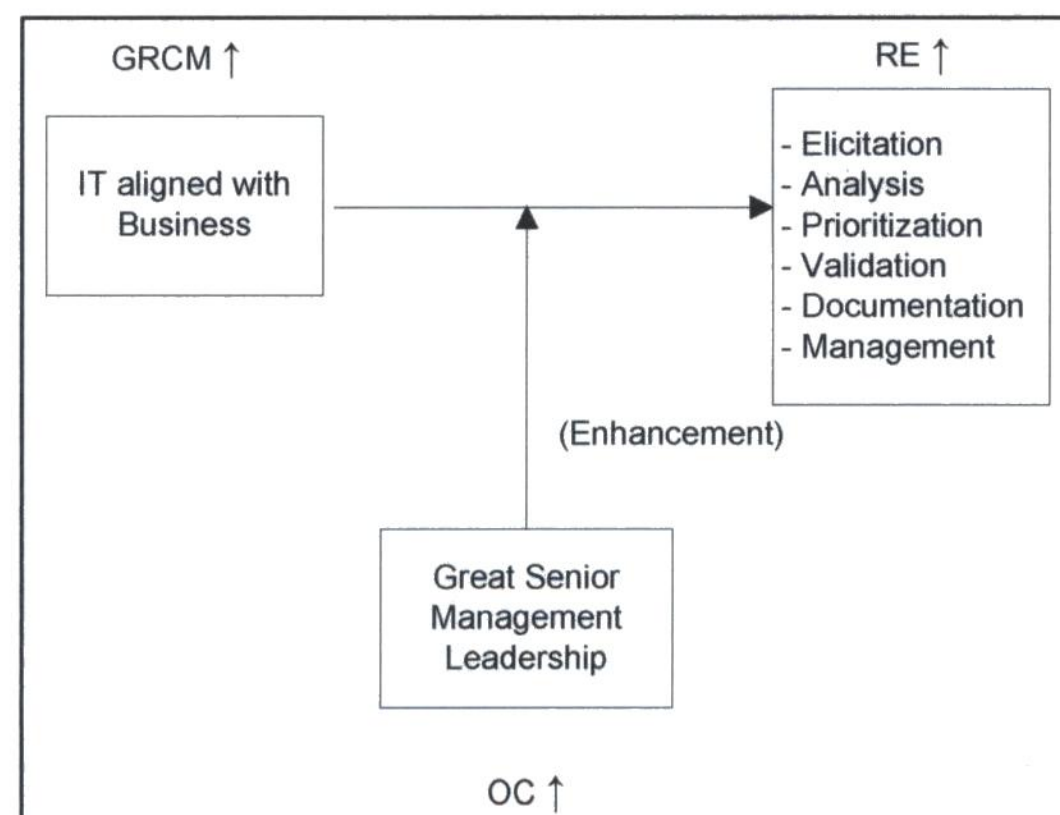
Observation #4

- a. The GRCM element, Perform Risk Analysis is at a high level of capability (3).
- b. The RE activities, elicitation, analysis, prioritization, validation, documentation and management are at a high level of capability (3).
- c. The Organizational Context (OC) is at a high level of capability (3).



Observation #5

- a. The GRCM element, IT is aligned with Business is at a high level of capability (3).
- b. The RE activities, elicitation, analysis, prioritization, validation, documentation and management are at a high level of capability (3).
- c. This is considering the Organizational Context (OC) at the maximum level of capability.

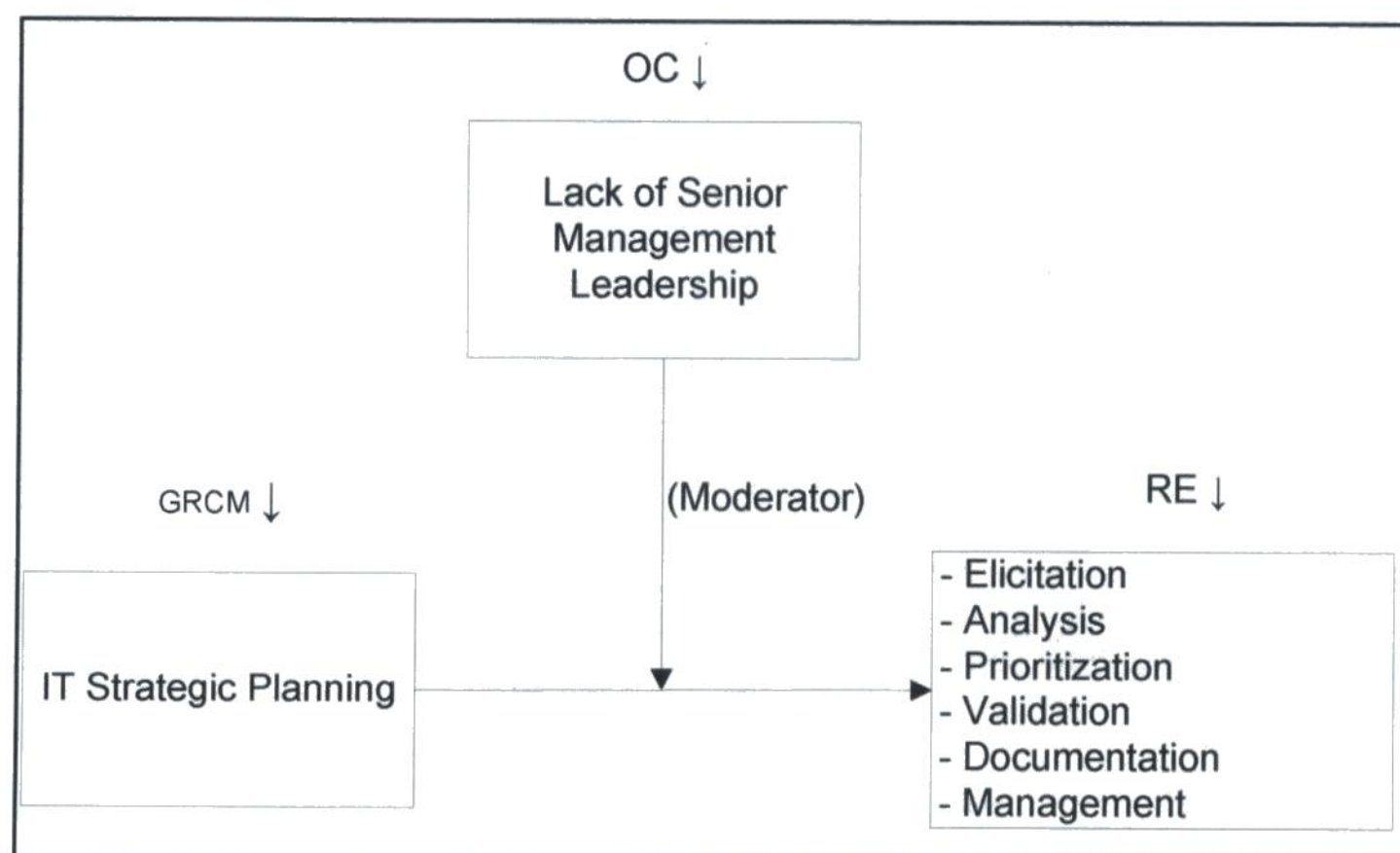


Case Study C

According to the GRCM and RE “Capability Measurement Frameworks” results indicate when GRCM elements are at a lower level of capability (1), the RE activities tend to reflect the same. The following are five observations to support the results.

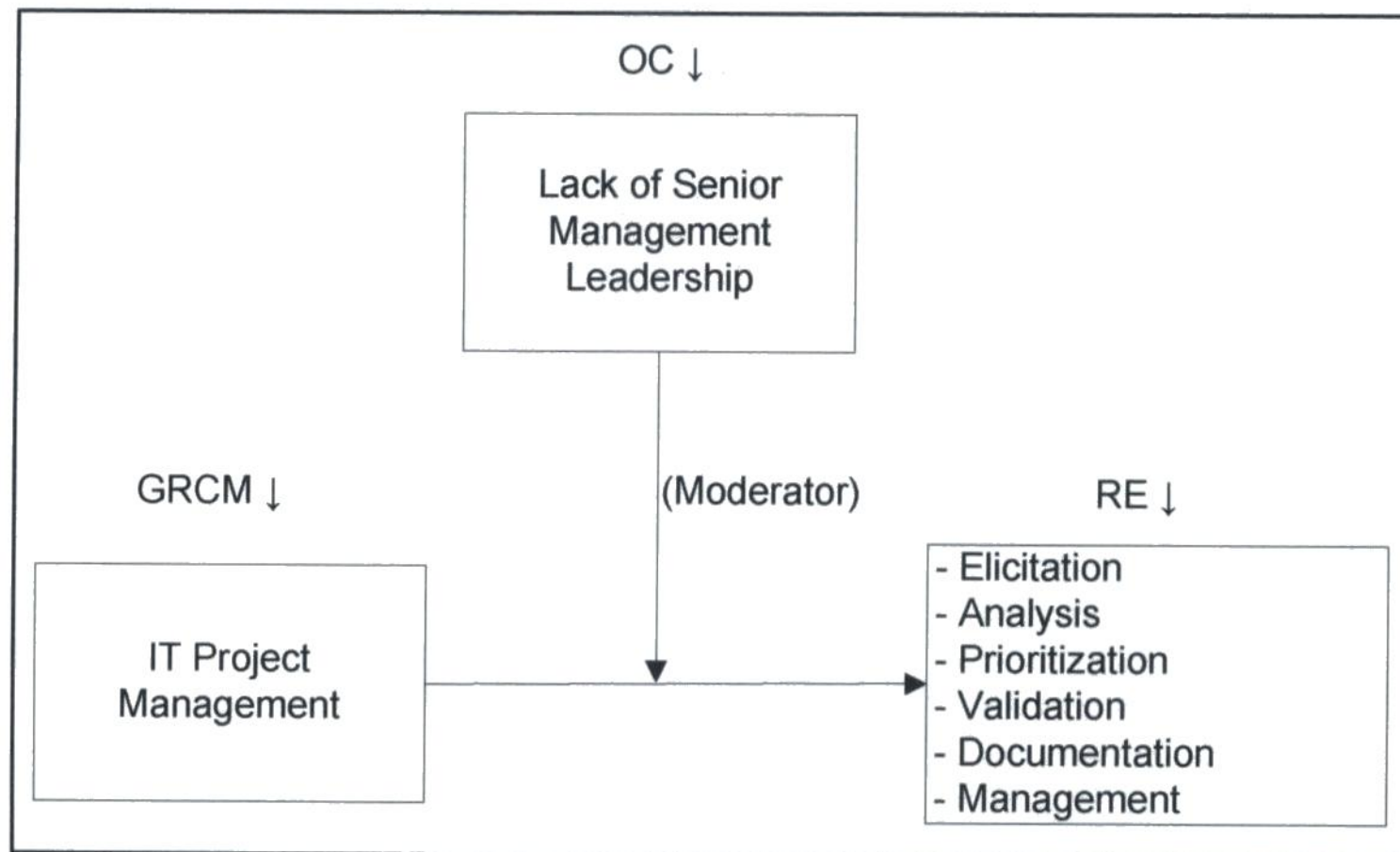
Observation #6

- a. The GRCM element, IT strategic planning is at a lower level of capability (2)
- b. The RE activities, elicitation, analysis, prioritization, validation, documentation and management are at a lower level of capability (2).
- c. The Organizational Context (OC) is at a lower level of capability (2).



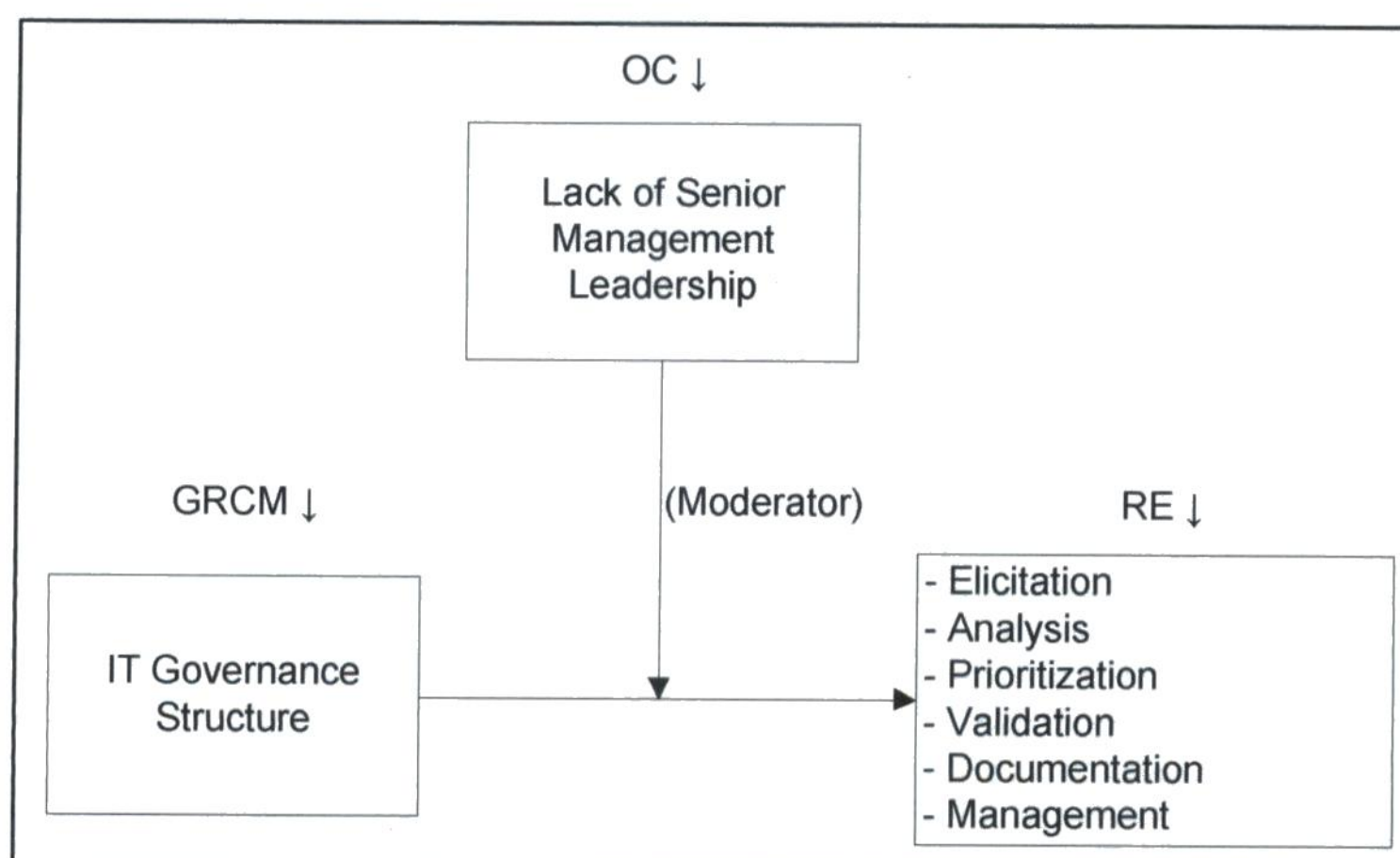
Observation #7

- a. The GRCM element, IT Project Management is at a lower level of capability (2).
- b. The RE activities elicitation, analysis, prioritization, validation, documentation and management are at a lower level of capability (2).
- c. The Organizational Context (OC) is at a lower level of capability (2).



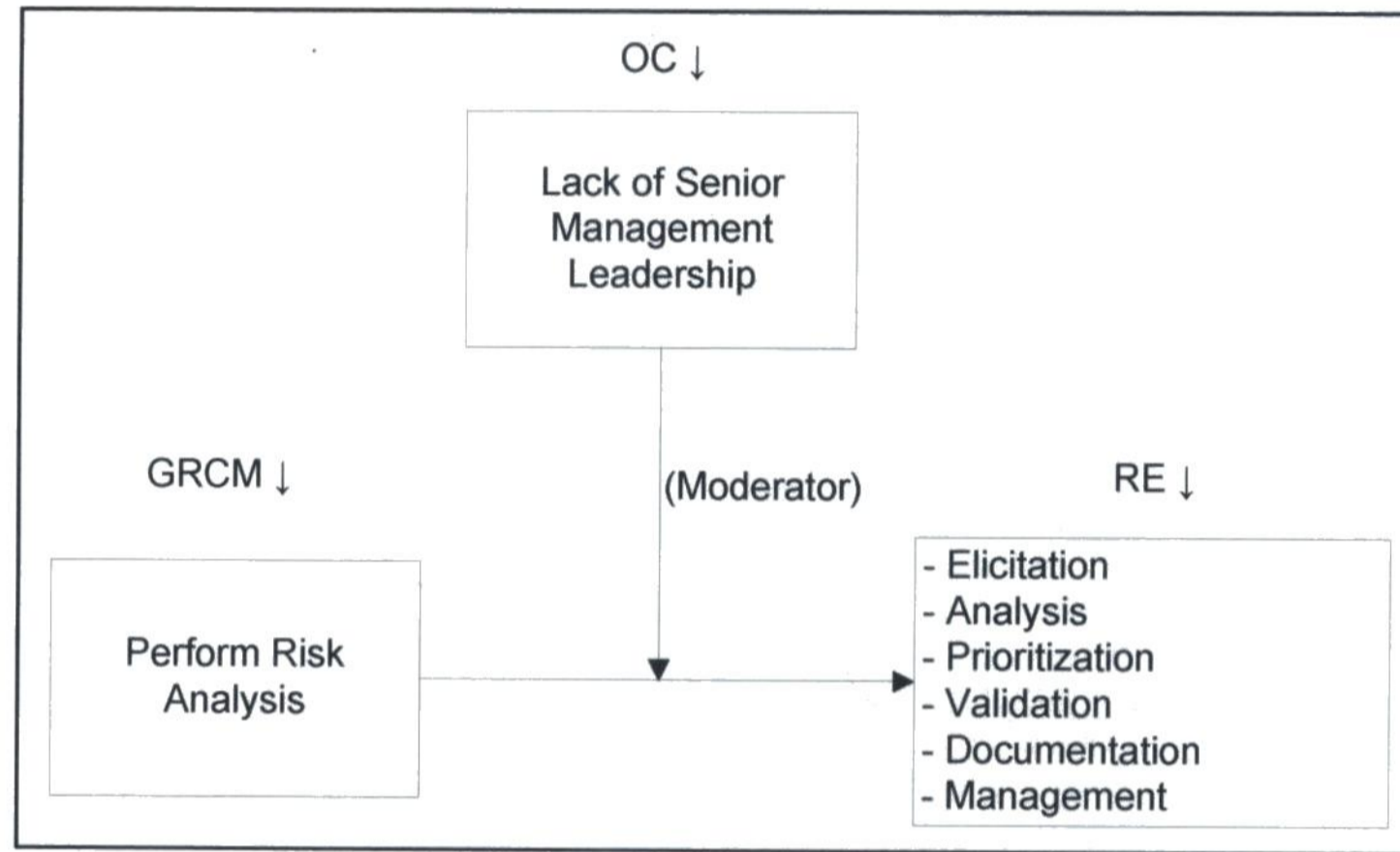
Observation #8

- a. The GRCM element, IT Governance Structure is at a lower level of capability (2).
- b. The RE activities elicitation, analysis, prioritization, validation, documentation and management are at a lower level of capability (2).
- c. The Organizational Context (OC) at a lower level of capability (2).



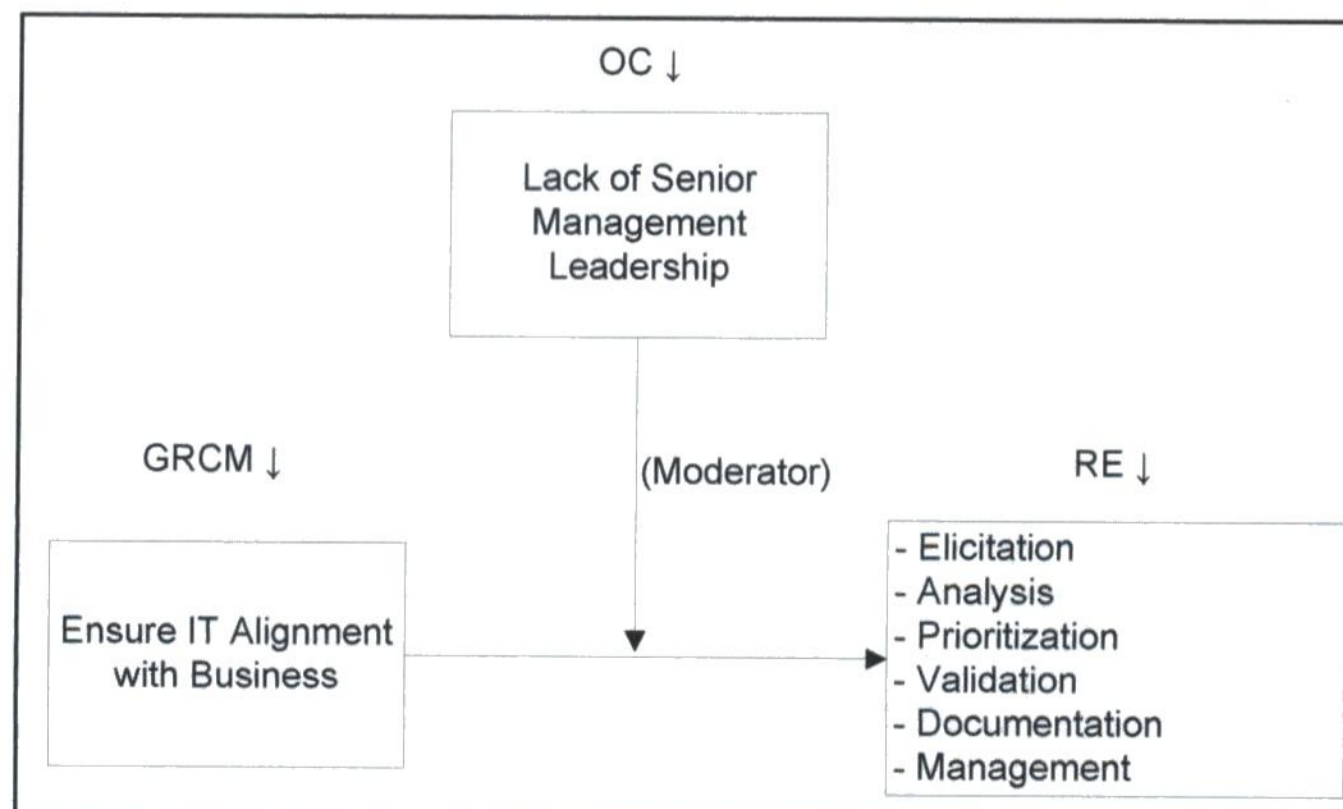
Observation #9 –

- a. The GRCM element, Perform Risk Analysis is at a lower level of capability (2)
- b. The RE activities elicitation, analysis, prioritization, validation, documentation and management are at a lower level of capability (2).
- c. The Organizational Context (OC) is at a lower level of capability (2).



Observation #10

- a. The GRCM element, IT Alignment with Business is at a lower level of capability (2)
- b. The RE activities elicitation, analysis, prioritization, validation, documentation and management are at a lower level of capability (2).
- c. The Organizational Context (OC) is at a lower level of capability (2).



As per the data analysis results the two objectives identified in section 1.2 are fulfilled. In other words the proposed Capability Measurement Framework for both GRCM and RE can be used as an instrument to measure the level of capability. There are relationships between GRCM capabilities and RE capabilities.

The next chapter concludes with the results, to what extent they have been fulfilled, the limitations of this study and future studies to be considered.

6.0 CONCLUSION

The results from the research support the two objectives.

- a) Develop and validate a new GRCM and RE Capability Measurement Framework
- b) Explore to what extent GRCM capabilities are correlated with RE capabilities.

The extent the research supports the first objective is as follows:

A new GRCM and a new RE Capability Measurement Framework were created by using thirteen elements from the GRCM domain and six activities from the RE domain. Each element/activity was based on a specific construct and theoretically justified by known academics. For each element/activity the level of capability was measured by using a numeric value as well as color coded. This method was simple to use and demonstrate quickly which elements/activity needed further attention.

The extent the research supports the second objective is as follows:

The data analysis reveals GRCM capabilities are somewhat correlated with RE capabilities. It seems that if GRCM elements are well integrated the RE activities will benefit and if the GRCM elements are not well integrated the RE activities will not benefit.

Despite the results there are limitations to this study. The research was limited to four case studies due to time and resource constraints. The case studies used in this research are all from the same industry (security). The data collected from the case studies is a recollection of the authors experience working as a project manager in the past. The author performed the exercise of rating the level of capability for both the GRCM elements and

RE activities for each case study. The project sponsor was not involved in this rating exercise.

At best, the results produced are both valid and reliable. The case studies scenarios have been validated by the project sponsors. Some may say the results may be biased due to having one person due the rating exercise.

One needs to be cautious when rating the level of capability for the GRCM elements and RE activities. It is more of a subjective exercise than a true or false statement.

In function of the results and limitations the following are research strategies that could be considered after the thesis (e.g. as part of a PhD project).

- Perform an engineering empirical study regarding the relationship between GRCM and RE vis à vis organizations across industries by using the proposed “Capability Measurement Framework”.
- Perform an engineering empirical study regarding the relationship between GRCM and RE across various government agencies or departments by using the proposed “Capability Measurement Framework”.

Further Research Considerations:

- Define what Canadian companies are using as best GRCM practices.
- Define a functional model that would integrate GRCM best practices into on discipline.
- Identify GRCM Standards and Procedures as one discipline.
- Consider having a GRCM role within the IT Project environment.

- Establish a framework to implement GRCM to enhance RE in a Software Engineering Project.
- Define a functional model that would integrate GRCM to enhance RE across all projects in an organization in a coherent way.
- Define a functional model that would integrate GRCM to enhance RE across the organization (enterprise wide) in a coherent way.

To conclude, one can see that more research is needed to better understand how GRCM is relevant for RE. By performing more research it will lead us to more questions and answers thus increasing our understanding on these relationships. This will undoubtedly help the GRCM and RE communities.

APPENDIX A - Case Study A: Registration of Businesses on the Web

Abstract

In the spring of 2008, an organization was directed by the authorities to create a new section on their existing website permitting business owners to register on-line. In order to do so the organization needed to develop an on-line application where the user would enter his or her business information. As well the application would need to store data, have a search function capability as well as reporting capabilities.

A closer look on how governance, compliance and risk management (GRCM) was integrated during the project was considered. As well various elements such as requirements, resources, lifecycle, processes, disciplines, roles, tasks, artifacts, guidelines and risks were also discussed.

The study concludes with various tables. The data in the tables indicate the level of GRCM integration and level of capability, the RE integration and level of capability, and the Organizational Context support and level of capability. The data recorded in the tables is a recollection of the author's experience working on the project as a project manager.

Key words: governance, project management committee, project steering committee, change advisory board, compliance, requirements engineering.

Introduction

An organization was legislated by the government to become a registration centre for businesses to register on-line in order to provide services to the public. The organization main focus was to ensure the businesses could register on-line before the set legislative date. The businesses needed to be registered prior to the legislative date to be recognized as a legitimate operating centre. After that date the business was known to operate illegally.

The organization had various departments but the focus of this case study is on the IT department. The IT department is responsible to maintain day to day operations as well as implementing various IT projects.

Governance Structure

The organization had a Chief Information Officer (CIO) that believed in streamlining processes, providing continuous support to its clients, proceed with innovative ideas and utilizing up to date technologies. The CIO reported project statuses as well as operation issues to the Executive Committee. Reporting directly to the CIO were the functional IT managers. The functional managers were responsible for activities within their areas.

Some of the functional managers were also members of project committees. For example, the Project Management Committee (PMC) was chaired by a functional managers where the CIO attended, as well as people from different departments including the IT project managers. The purpose of this committee was for the project managers to inform the PMC of the project progress, risk, issues and dependency if any. The PMC mandate was to give guidance to the project managers, ensure the projects were on track, identify if any interdependencies existed between projects, resolve any resource allocation issues and identify any potential risks that would potentially jeopardize the projects.

Another committee that was available to the projects was the project steering committee (PSC). This committee consisted of a few IT functional managers as well as subject matter experts (SMEs). The mandate for this committee was to give direction or make a business decision that required management authority prior to the project manager moving forward. This committee also approved or rejected change requests (CRs) based on the Change Advisory Board (CAB) recommendation.

The CAB was another committee consisting of functional managers and SMEs in which their mandate was to assess the CR impact on the organization enterprise wide. Upon the completion of the assessment the CAB would send a recommendation to the PSC. If the recommendation was favorable the PSC would then approve the CR.

Compliance

Many of the IT projects were initiated by the business client who had specific business requirements. IT projects were also stood up to comply with new legislations. When this happened, tremendous pressure was set on the IT department. The IT department needed to ensure that the new legislation was clearly understood by the ones involved in identifying requirements and possibly changing the business processes. Having a clear interpretation of the legislation was the utmost importance if the application was to meet legislation. There was no time for re-work once the application was built.

Requirements

The project was stood up in 2008 to satisfy imposed legislation. The business client met with the business analyst, project manager and application developer, to discuss the following: business process changes, proposed software application, the impact on existing infrastructure, network and systems, as well as the benefits to the organization at the enterprise level.

A business model was drawn by the business analyst representing the changes imposed by the new legislation. The model was also used as a tool to ensure stakeholders had the same understanding of the proposed business changes and were in agreement. From the business model, various case studies and scenarios were created to flush out the requirements.

Process

The organization used the Requirement Engineering (RE) process to identify, communicate and document the requirements that the system needed to satisfy. Many working sessions were held between the client, project team members and stakeholders to capture their needs, wants and desire. Once this exercise was completed, all the identified requirements including supplementary requirements were classified in categories, urgency and priorities and documented with the use cases in a functional requirements document.

The working sessions were also helpful in identifying dependencies amongst other projects being implemented and possible impact the new project may inflict to existing systems.

The functional requirements document needed to be approved by the IT department CIO, the business client, the functional manager responsible for the application built and development and the project manager. None of the design and development of the application work could commence, until the functional requirement document was signed by all stakeholders. At this point the project was baselined.

Lifecycle

The organization used a combination of the waterfall lifecycle model and Unified Process to build, develop and implement the new software application. The first phase was the inception phase where all requirements were needed to be flushed out before going to the second phase or elaboration phase. In the first phase a business model was created, use cases were drawn up as well as scenarios which were more aligned with the Unified Process.

Disciplines

The functional requirement document was the work product for both the business modeling and requirements discipline as per the Unified process. The next step was for the developers to analyze and design the application according to approved requirements. Once the design was approved by the appropriate stakeholders the developers started coding in the development environment. Upon completion of the code development, the coding was then implemented and tested in the test environment prior to going into production. The application was deployed prior to the legislation date and the next day the business owners were able to register their business on-line.

Any changes to the project requirements or design are required to go through the configuration management process. The change request or CR are presented and accepted at the CAB to get acceptance and then approved by the steering committee.

Project management is practiced during all project phases. The PM ensures that the project is moving forward and that upper management and stakeholders are aware of the progress of the project.

Roles

The project team consisted of various roles and was fulfilled with people having different skill set and knowledge. The team had one common objective and that was ensuring the project success.

The roles for the project were the following:

Project Sponsor/Business Owner

A person with authority that represented the business client. The person was responsible in identifying the business requirements as well as the business processes.

The project sponsor was referenced as the business owner since the same organization was receiving the business value of IT from the project deliverables.

Project Manager

A person selected by the organization to manage the project deliverables from the beginning to end.

Business Analyst

A person that provided analysis and development while the software application was under development.

Software developers

A group responsible for the design and development of the on-line application.

Web developers

A group responsible for creating web pages as an interface between the registrant and the application.

Stakeholders

Interest groups whose needs must be satisfied by the project. They are the ones that are most likely impacted by the project.

Tasks

Each role had specific tasks to perform in order to complete the project. Every task were identified in a work breakdown structure as well as scheduled.

The tasks for each project roles were the following:

Project Sponsor/Business Owner (Employee)

- Provided project funding to cover monthly expenses
- Monitored the project progress to ensure the project benefits were realized
- Reported the project progress to the senior executives
- Gave guidance and direction to the project manager if required

Project Manager (Consultant)

- Established the project's define RE process
- Met with various stakeholders to go through the RE process
- Managed stakeholders expectation
- Ensured proper management documents were created
- Created a work breakdown structure and implementation plan (schedule)
- Created and maintained a Risk Register
- Reported the project progress to the PMC
- Presented change request to the PSC and to the CAB
- Met on a weekly basis with the project team members to discuss project progress, risks and issues

Business Analyst (Employee)

- Conducted joint application design (JAD) sessions with various stakeholders
- Confirmed and finalized business requirements
- Confirmed and finalized functional requirements
- Ensured newly implemented system features or enhancements met user needs as documented in the specifications

Software developers (Employees)

- Participated in the joint application design (JAD) sessions with various stakeholders
- Met with the client and business analyst to ensure the requirements were clear and the interpretations were correct.
- Used appropriate software development tools to design and build the application
- Built a prototype of the web registration application and demonstrated it to the client and management for feedback
- Informed the project manager of any changes required to the application design or build
-

Web developers (Employees)

- Participated in the joint application design (JAD) sessions with various stakeholders
- Used appropriate web tools to design and build the web interface.

Stakeholders (Employees)

- Participated in the JAD sessions to identify requirements
- Reviewed the functional requirement document
- Accepted the web prototype
- Reviewed the Certification and Accreditation document

Resources

The project team members were full time employees (matrix) or contractors. Each member had certain skills set that together covered the spectrum of the disciplines identified in the Unified Process. Most of the full time staff was not allocated to the project at 100% except for the business analyst. The other team members were shared between operations and the project.

The organization was constantly re-allocating resources between projects. It had difficulty with resource allocation due to its shortage and increasing number of projects. The organization was in dire straits once new legislations were imposed. The organization needed to re-prioritize its projects ensuring that the new legislation requirements were dealt in time and that limited resources were available.

Artifacts

The project used the Project Management Body of Knowledge (PMBOK) as a good practice and many of the artifacts were derived from it. The project produced a project charter, a functional requirement document, a work breakdown structure, a schedule, a risk and issue log, a lessons learned document, a Certification and Assessment (C&A) document, various slide deck, agendas, minutes of various project meeting, and monthly status reports.

Guidelines

The project team members followed guidelines, standards and policies written by the organization. A number of the guidelines focused on the security aspect of the organization. By having the team members adhere to the guidelines it ensured compliancy between the people and the organization, between the organization and organizations, between the organization and other agencies.

No guidelines were available for the RE process as well as for the software development methodology.

Risks

Continuous risk management was applied throughout the project. The project manager tracked and monitored risks as the project moved forward. At every weekly team meeting the project managers would go through the risk and issue log ensuring that all was well. Risks that were identified as outside of the project scope were brought forward to the PMC meeting. At the PMC meeting the risks were tagged for resolution and assigned to the appropriate section.

Challenges

Due to the organization of not defining a proper software development methodology the project was tied in using the waterfall life cycle model and the Unified Process. During the first project phase the project was following an RE process and needed to have the functional requirement document signed by authorities before going to the design and built stage. This meant the developers could not start on the design or built of the application.

There were constant delays in having the client signed the functional requirements document. This was due to the client changing requirements or adding new ones. This meant that for every day the document was not signed the developers could not start on the application design.

Resource allocation continued to be problematic within the project due to operation issues. When an operation issue arose in respect to software applications the project developers needed to stop their work and address operations. Sometimes the developers worked two to three days to solve operation issues and involved overtime. The organization had no one to maintain software applications on a daily basis.

There were no guidelines available for the RE process and software development methodology. The project needed to come up with some partial guidelines as to ensure everyone knew of the various processes being used.

The organization was continuously dealing with the re-prioritization of projects and resource allocation. A big part of this challenge was due to imposed legislation by government.

Conclusion

The paper addresses how GRCM was applied in the organization. It gives an idea on the approach the organization took to ensure its requirements were defined (RE process) prior to designing and building the application. It also describes the challenges it had in regards to its software development methodology, its resource allocation, and the impact of imposed legislation.

As part of the data analysis, tables were created in respect to the GRCM implementation, the applied RE process and the organizational context.

The following is a list of the tables where data was recorded as part of the data analysis.

1) Table A-1: GRCM an Independent Variable with its Constructs and Measures

This table describes the operationalization statements (constructs) and indicates if they are integrated.

2) Table A-2: GRCM Detailed Observations and Estimated Level of Capability

3) Table A-3: RE a Dependent Variable with its Constructs and Measures

4) Table A-4: RE Detailed Observations and Estimated Level of Capability

5) Table A-5: OC an Independent Variable with its Construct and measure

6) Table A-6: OC Detailed Observations and Level of Capability

This case study in addition to three more is part of the analysis where the following question will be answered.

Can this data lead us to believe that the GRCM integrated in the projects do enhance Requirements Engineering?

Table A-1: GRCM an Independent Variable with its Constructs and Measures

Independent Variable (GRCM)	Operationalization (Constructs)	Measure (NI, SI, FI)
Governance		
• IT Strategic Planning	• Adequate infrastructure	FI
	• First point of escalation for variance to project cost and timescale	FI
	• Assign ownership and accountability for technical risks	FI
• IT Project Management	• Employ sound project management techniques and controls	FI
	• Small scope and scale	FI
	• Request realistic and adequate budget	FI
	• Adhere to standardized specifications	FI
• IT Control Framework	• Development of management control structure	FI
	• Create an accountability framework	SI
	• Establish an access control to information	FI
• IT Asset Management	• To prevent damage to assets and interruptions to business activities	FI
	• To maintain appropriate protection of corporate assets	FI
	• To ensure that information assets receive an appropriate level of protection	FI
• IT Processes	• Establish IT processes	FI
	• Establish conformance process	FI
	• Establish performance processes	FI
Risk Management		
• Embed into the project/enterprise an IT governance structure	• The structure needs to be accountable, effective and transparent	SI
• Support auditing and monitoring operations	• Support a variety of different auditing and monitoring operations	NI
	• Establish an auditing committee	NI
• Monitor and Track risk regularly	• Active monitoring and regular viewing of risks	FI
	• Risk monitoring and control	FI
	• Breaking the project into smaller pieces to better addressed and manage risks.	FI

Table A-1: GRCM an Independent Variable with its Constructs and Measures (cont.)

Independent Variable (GRCM)	Operationalization (Constructs)	Measure (NI, SI, FI)
Risk Management		
<ul style="list-style-type: none"> Risk analysis is part of the project ongoing monitoring of IT risks and controls 	<ul style="list-style-type: none"> Perform analysis and assessment of risks including asset value, vulnerability and threat. 	FI
	<ul style="list-style-type: none"> Require risk decision process supported by risk analysis, identification and evaluation. 	FI
Compliance		
<ul style="list-style-type: none"> Brief project mandate to committees involved 	<ul style="list-style-type: none"> Ensure adequate visibility of the project. 	FI
<ul style="list-style-type: none"> Ensure IT alignment with business 	<ul style="list-style-type: none"> Align IT with enterprise objectives. 	FI
	<ul style="list-style-type: none"> Ensure that IT investments decisions and performance measures demonstrate the value of IT. 	SI
<ul style="list-style-type: none"> Comply with regulations, policies and standards 	<ul style="list-style-type: none"> Systems to be compliant with organizational security, policies and standards. 	FI
	<ul style="list-style-type: none"> Ensure compliance with legislation, regulations, security policies and rules. 	FI
<ul style="list-style-type: none"> Consider security in the project 	<ul style="list-style-type: none"> Need to consider security “from the ground up”. 	FI

Table A-2: GRCM Detailed Observations and Estimated Level of Capability

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
IT Strategic Planning	Jan 08 to May 08	17 weeks	P - CIO, Project Sponsor (PS) - Project Manager (PM) S - PMC - NI Team	An adequate infrastructure was available for the web application. The project manager (PM) reported any variance to project cost or timescale to the Project Management Committee (PMC) held monthly. The network infrastructure (NI) team was assigned ownership and accountability to ensure the systems were available for the developers to work on.	3
IT Project Management	Jan 08 to May 08	17 weeks	P - PM S - Stakeholders - Team members	The PM was assigned to the project in the early phase of the project. Sound project management techniques were based on the Project Management Body of Knowledge (PMBOK). The PM met with various stakeholders to define work to be completed. A work breakdown structure (WBS) was divided in work packages so they can be manageable. The WBS was balanced accordingly. A budget to perform the work was adequately allocated. The WBS met standardized specification set by the organization such as ensuring proper project phases were considered when implementing the project and that resources with specific skills set were allocated to the proper work packages.	3
IT Control Framework	Jan 08 to May 08	17 weeks	P - PM S - Stakeholders - Team members - IT department	The project was using a Record Data Information Management Information Systems (RDIMS a.k.a. CERRRID) to centralized the information. Project members had different privileges to access the information. The access privileges were based on the role. The IT department ensured there was a development environment available for developers to do their coding and testing. It wasn't clear who was deciding what technology to use during the project implementation.	2

Green (3) = Fully Integrated / full capability, Yellow (2) = Semi Integrated / poor capability, Red (1) = Not Integrated /no capability

Table A-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
IT Asset Management	Jan 08 to May 08	17 weeks	P - IT department S - Managers - Employees - Contractors	All of the organizations' computerized systems were located in a server room where proper ventilation was given. Uninterruptible power supplies were connected to the systems as well as back up servers. Access to the room was limited to card holders to prevent system tampering. The whole floor was protected by having a card swipe system at the entrance. These protective measures protected corporate assets as well as organization information and prevented damage to assets and interruptions to business activities.	3
IT Processes	Jan 08 to May 08	17 weeks	P - IT department S - PM - Team members	The IT department had various IT processes in place to ensure the continuity of business and the security of systems and information. It also had established conformance processes and performance processes in place. The project followed these practices.	3

Table A-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

RISK MANAGEMENT	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
IT Governance Structure	Jan 08 to May 08	17 weeks	P - CIO S - PMC - PM, BA - Developers, testers, integrators - Other PM's - Subject Matter experts (SME) - Other members from the department	The organization as a whole had an IT governance structure in place. The IT structure consisted of the CIO, various sectors such as the networking group, service management, applications development and desktop services. Various committees were also stood up such as the Project Management Committee (PMC), project steering Committee (PSC) and a change advisory board (CAB) The project governance structure consisted of the PMC, PSC, PM, BA, developers, testers, and implementers. Despite of having a governance structure in place the project was experiencing difficulties in nailing down the requirements with the business client. The client kept changing the requirements even though they were agreed amongst the stakeholders.	2
Audit and Monitor	Jan 08 to May 08	17 weeks	None Identified	No specific auditing exercises were performed during the application built and test. No auditing committee was established in the project.	1
Monitor and Track Risks Regularly	Feb 08 to May 08	15 weeks	P - PM S - Stakeholders - Team members	The PM created a risk register and identified all potential risks. All risks were tracked and monitored weekly. Every week a project team meeting was held to discuss the project progress as well as project risks and mitigations. Critical risks were reported to the PMC for information or for resolution. All known risks were built in the WBS to ensure timelines were met.	3
Perform Risk Analysis	Feb 08 to May 08	15 weeks	P - PM S - Team Members	After the risks were identified a risk analysis was performed. The level of impact, probability of it occurring, the mitigation strategy and the cost to mitigate the risk were all considered.	3

Table A-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

COMPLIANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Brief Project Mandate to Committees	Feb 08	.5 day	P - PM S - PMC, PSC	The PM presented the project to the Project Management Committee (PMC) and the Project Steering Committee (PSC).	3
Ensure IT Alignment with Business	Feb 08 to May 08	15 weeks	P - CIO S - PMC - PM's	The CIO ensured that IT was aligned with the business. Monthly meetings were held with the PMC to discuss if the way of doing business today was adequate or if it needed to change. Was the existing IT in place sufficient or it needed to be upgraded due to business changes. It was not apparent that IT investments decisions and performance measures demonstrated the value of IT.	2
Comply with Regulations, Policies and Standards	Jan 08 to May 08	17 weeks	P - CIO S - IT department	All systems were compliant with legislation, regulations, security policies and rules.	3
Consider Security	Jan 08 to May 08	17 weeks	P - CIO S - IT Security	The organization enforced security since it was in the security business. All of its assets, resources and information were monitored by IT security. The security measures were also enforced at the project level.	3

Table-A-3: RE a Dependent Variable with its Constructs and Measures

RE - Dependent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Elicitation	<ul style="list-style-type: none"> The client needs to be involved and all requirements need to be identified by some means. 	FI
Analysis	<ul style="list-style-type: none"> Negotiation and conflict management is important. 	FI
Prioritization	<ul style="list-style-type: none"> The requirements need to be prioritized and classified. 	FI
Validation	<ul style="list-style-type: none"> The requirements need to be validated by the client. 	FI
Documentation	<ul style="list-style-type: none"> The requirements need to be clear so there are no misinterpretations of requirements by the developer. 	SI
Management	<ul style="list-style-type: none"> Requirement changes need to be managed 	SI

Table-A-4: RE Detailed Observations and Estimated Level of Capability

RE - Dependent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Elicitation	Jan 08 to Mar 08	8 weeks	P - BA S - Stakeholders	The BA held various working sessions with stakeholders to discuss how the business was conducted today and how the web application would change some ways of doing business. A business model was created to give a big picture followed by use cases. High level requirements were then flushed out. The PM started the contract when most of the requirements elicitation tasks were completed. The previous PM had moved on to another project.	3
Analysis	Mar 08	2 weeks	P - BA S - Stakeholders - Developers	The BA conducted a requirement analysis with some of the stakeholders and developers to identify which requirements were feasible, and technically do-able. Negotiations on requirements were successful. A requirement list was then developed and circulated to stakeholders for their acceptance.	3
Prioritization	Apr 08	1 week	P - BA S - Stakeholders	The BA with the stakeholders prioritized the requirements as a need, want or wish.	3
Validation	Apr 08	1 week	P - BA, PM S - Stakeholders	The BA and PM met with the various stakeholders to ensure the requirements were validated and accepted.	3

Table-A-4: RE Detailed Observations and Estimated Level of Capability (cont.)

RE - Dependent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Documentation	Apr 08	1 day	P - BA, PM S - Stakeholders - Developers	<p>The BA developed a functional requirements document (FRD) and most of the information pertaining to the project requirements was in this document. This document became official and required signing from the authorities before development work could begin.</p> <p>The client held back in signing the FRD till the very last minute. They were in fact late. This creating friction between the client, the BA and the Developers.</p> <p>This document ensured that the requirements were clear, concise and that everyone had the same interpretation of the requirements. It took a while before the document was signed since the client kept on changing their requirements.</p>	2
Management	Jan 08 to May 08	17 weeks	P - PM S - BA - Developers	<p>Some of the change requests were not properly handled. The BA would go straight to the developer asking to implement the changes without notifying the PM. The FRD was stored in a locked cabinet where authorized personnel would have access to the original copy. Another working copy was stored on the project shared drive where project team members with permissions had access.</p>	2

Table A-5: OC an Independent Variable with its Construct and Measure

OC – Independent Variable	Organizational Context	Measure (NI, SI, FI)
Management Support	Senior Management Leadership/Commitment	FI

Table A-6: OC Detailed Observations and Level of Capability

OC – Independent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Management Support	Jan 08 to May 08	17 weeks	Senior Management Team	Full Senior Management Support was provided by the organization.	3

APPENDIX B - Case Study B: Corporate Intranet Revamp Project

Abstract

In the fall of 2007, an organization needed to revamp its corporate intranet due to responses from an employee survey. A survey was distributed to its employee's enterprise wide asking them what they thought of the existing corporate intranet. The results were not very positive. Some employees were saying it was difficult to find information pertaining to services, others were suggesting that the primary page be more intuitive, others were suggesting that the site needed more cosmetics, others wanted to have an up to date section and the list of suggestions was extensive. The management also suggested that a section be available for them to do administrative work.

A business case was written and presented to the executive committee for project funding. The business case was accepted and funds were deliberated

A closer look on how governance, compliance and risk management (GRCM) was integrated during the project was considered. As well various elements such as requirements, resources, lifecycle, processes, disciplines, roles, tasks, artifacts, guidelines and risks were also discussed.

The study concludes with various tables. The data in the tables indicate the level of GRCM integration and level of capability, the RE integration and level of capability, and the Organizational Context support and level of capability. The data recorded in the tables is a recollection of the author's experience working on the project as a project manager.

Key words : governance, compliance, project management office, steering committee, change advisory board, requirements engineering, risks

Introduction

The organization had many departments and offered numerous services to its employees as well as procuring goods from external vendors. The organization had revamped its external website to ensure the information was easily accessible to the general public. After distributing a survey to its employee's major concerns arose in regards to its existing corporate intranet. Many had indicated that the corporate intranet needed to be revamped. After submitting a business case to the senior management explaining the employee's concerns and benefits of revamping the existing corporate website the demand was approved and funds were released. The Corporate Intranet revamp project was then established.

Governance Structure

The project governance structure consisted of a director as the project sponsor, a project manager that was appointed to manage the project, various stakeholders, and project team members. To support the project a web working group was stood up and consisted of functional managers representing different departments of the organization.

Compliance

The project needed to ensure the Corporate Intranet was compliant with the common look and feel (CLF) regulation set by the Treasury Board. Every government department and organization needed to be compliant with the CLF. To enforce this regulation Treasury Board auditor were to randomly inspect government internet and intranet sites ensuring the agencies were compliant with the CLF. At the time auditors were focusing more on external sites where the general population would browse to get various types of information. The reason for the CLF is to have all government sites look the same where one can easily navigate through the myriad of information, where information can be easily accessible and retrieved.

Requirements

A list of high level requirements was provided by the project sponsor once the project started but it wasn't specific enough to go forward with the design and development of the corporate intranet. The requirements were short listed, lacked clarity and room for misinterpretation on the developer's part. According to the project sponsor not to many stakeholders were not part of identifying the high level requirements; neither as the users.

Processes:

The department had no RE process in place. The project manager had to set up an RE process and present it to the director and stakeholders to inform them of the steps required acquire better requirements. As the project moved forward it was identified that prototypes of the intranet website should be built and presented to the stakeholders to get there buy-in. In other words the stakeholders required an iteration approach to the design.

Requiring an iteration approach to the design met that the software development approach would best be met by following the Unified Process.

Various work sessions were held between the stakeholders and project team members to go through the RE process. Many of the requirements were high level but some that were considered high priority were more detailed. One of the top requirement identified were to do some quick fixes on the existing corporate intranet. This would translate to quick fixes, thus projecting a positive image on the existence of the project.

Lifecycle:

This project was following the Unified Process. It started with the inception, elaboration, construction and transition phase.

The Corporate Intranet Website update was being implemented in a three step approach.

- First step - Identification of client requirements and quick fixes to be done on the existing corporate website
- Second step - Launch of the re-designed website including various organization sections
- Third step - Final website design which included tools and other capabilities

Disciplines:

The project followed the various disciplines as per the Unified Process. This project had some difficulty with the business modeling and requirements discipline. There was no business analyst as part of the project team which made it difficult for the project manager to perform his duties as well as the business analyst duties. The requirements could have been better identified if case studies and scenarios were used to explain the business process. The RE process was not exactly being followed.

Roles:

The project team consisted of a few roles and was fulfilled with people having different skill set and knowledge. It was difficult as a team to go through the RE process due to the lack of a business analyst.

The project roles were the following:

Project Sponsor

A person with authority that represented the organization undertaking the project as well as funding it.

Project Manager

A person appointed to lead and manage the Corporate Intranet Revamp project.

Web Publisher

A group responsible in designing and developing the intranet website according to the stakeholder's requirements and CLF set by Treasury Board.

Stakeholders

Interest groups whose needs must be satisfied by the project. They are the ones that are most likely impacted by the project.

Tasks:

Each role had specific tasks to perform in order to complete the entire project.

The tasks performed by the roles were the following:

Project Sponsor/Business Owner - (Employee)

- Provided project funding to cover monthly expenses
- Monitored the project progress to ensure the project benefits would be realized
- Reported the project progress to the senior executives

Project Manager – (Consultant)

- Established the project's defined RE process
- Met with stakeholders to go through the RE process
- Met with stakeholders to identify quick fixes
- Managed stakeholders expectation
- Ensured proper management documents were created and available
- Created a work breakdown structure and implementation plan (schedule)
- Monitored and controlled the project schedule including team members tasks
- Created and maintained a Risk Register
- Chaired the organization Website Working Group
- Reported the project progress to the Project Sponsor

Team member - Web Publishers (Employees)

- Designed and developed the organization website according to the stakeholders requirements using Web application software and CLF
- Participated as a member of the Website Working Group
- Designed folder architecture
- Responsible for the Graphic manipulation within the central cavity
- Created tables and links
- Applied XML coding where deemed necessary - tables
- Built numerous page layouts
- Built corporate web site prototypes and presented it to stakeholders and users for buy-in.

Stakeholders (Employees)

- Participated as members of the working group to define requirements
- Approved the functional requirements
- Gave in input on the web corporate website – content, cosmetics, etc..
- Reviewed various project documents

Artifacts:

The project used the Project Management Body of Knowledge (PMBOK) as a good practice and many of the artifacts were derived from it. The artifacts included a project charter, project work breakdown structure including a schedule, a governance document and a communication strategy document.

The project charter was created to ensure the stakeholders knew what was in scope and out of scope. It also stated the high level requirements, milestone dates, approved budget, and resource allocations.

The project work breakdown structure and schedule was created and used as a guide and tool to ensure the work packages were delivered on time and with the appropriate resources.

A governance document was created to describe the specific players, their roles and responsibilities and their interaction between them. It covered the project governance as well as the Web Content Management.

A communication document was created to ensure the stakeholders knew what was coming up as far as deliverables, milestone dates and their involvement.

A risk and issue log was created and presented weekly to the web working group.

A monthly status report was created and submitted to the director indicating the project progress, risks and issues.

Guidelines:

The treasury board Common Look and Feel guidelines were used during the design and development of the Corporate Intranet.

Risks

A risk and issue log was created to assist in performing continuous risk management. A weekly meeting was held with the website working group to discuss the project progress as well as risks. The risks with high to medium impact and probability were assigned to an Officer of Primary Interest (OPI) to have it resolved.

Challenges

One challenge was to have people agree on the requirements and priorities. Some requirements were seen by stakeholders as not required but nice to have while others thought otherwise. It took a while before the requirements were finally flushed out, prioritized and accepted by the various stakeholders.

Another challenge was to get the people agree on the intranet prototype. Some stakeholders were emphasizing too much on the cosmetics thus losing sight of the intended functionality of the intranet. As of the summer of 2008, the prototype still needs to be approved by the stakeholders prior to the web developers commencing on the design and development of the corporate intranet.

Conclusion

The paper addresses how GRCM was applied in the organization. It gives an idea on the approach the organization took to ensure its requirements were defined (RE process) prior to designing and building the web application. It also described the challenges it had in regards to stakeholders agreeing on requirements and the intranet prototype.

As part of the data analysis, tables were created in respect to the GRCM implementation, the applied RE process and the organizational context.

The following is a list of the tables where data was recorded as part of the data analysis.

1) Table B-1: GRCM an Independent Variable with its Constructs and Measures

This table describes the operationalization statements (constructs) and indicates if they are integrated.

2) Table B-2: GRCM Detailed Observations and Estimated Level of Capability

3) Table B-3: RE a Dependent Variable with its Constructs and Measures

4) Table B-4: RE Detailed Observations and Estimated Level of Capability

5) Table B-5: OC an Independent Variable with its Construct and measure

6) Table B-6: OC Detailed Observations and Level of Capability

This case study in addition to three more is part of the analysis where the following question will be answered.

Can this data lead us to believe that the GRCM integrated in the projects do enhance Requirements Engineering?

Table B-1: GRCM an Independent Variable with its Constructs, and Measures

Independent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Governance		
• IT Strategic Planning	• Adequate infrastructure	FI
	• First point of escalation for variance to project cost and timescale	FI
	• Assign ownership and accountability for technical risks	SI
• IT Project Management	• Employ sound project management techniques and controls	SI
	• Small scope and scale	FI
	• Request realistic and adequate budget	SI
	• Adhere to standardized specifications	SI
• IT Control Framework	• Development of management control structure	FI
	• Create an accountability framework	SI
	• Establish an access control to information	FI
• IT Asset Management	• To prevent damage to assets and interruptions to business activities	FI
	• To maintain appropriate protection of corporate assets	FI
	• To ensure that information assets receive an appropriate level of protection	FI
• IT Processes	• Establish IT processes	SI
	• Establish conformance process	FI
	• Establish performance processes	SI
Risk Management		
• Embed into the project/enterprise an IT governance structure	• The structure needs to be accountable, effective and transparent	FI
• Support auditing and monitoring operations	• Support a variety of different auditing and monitoring operations	NI
	• Establish an auditing committee	NI
• Monitor and Track risk regularly	• Active monitoring and regular viewing of risks	FI
	• Risk monitoring and control	FI
	• Breaking the project into smaller pieces to better addressed and manage risks.	FI

Table B-1: GRCM an Independent Variable with its Constructs, and Measures (cont.)

Independent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Risk Management		
<ul style="list-style-type: none"> Risk analysis is part of the project ongoing monitoring of IT risks and controls 	<ul style="list-style-type: none"> Perform analysis and assessment of risks including asset value, vulnerability and threat. 	FI
	<ul style="list-style-type: none"> Require risk decision process supported by risk analysis, identification and evaluation. 	FI
Compliance		
<ul style="list-style-type: none"> Brief project mandate to committees involved 	<ul style="list-style-type: none"> Ensure adequate visibility of the project. 	FI
<ul style="list-style-type: none"> Ensure IT alignment with business 	<ul style="list-style-type: none"> Align IT with enterprise objectives. 	FI
	<ul style="list-style-type: none"> Ensure that IT investments decisions and performance measures demonstrate the value of IT. 	SI
<ul style="list-style-type: none"> Comply with regulations, policies and standards 	<ul style="list-style-type: none"> Systems to be compliant with organizational security, policies and standards. 	FI
	<ul style="list-style-type: none"> Ensure compliance with legislation, regulations, security policies and rules. 	FI
<ul style="list-style-type: none"> Consider security in the project 	<ul style="list-style-type: none"> Need to consider security “from the ground up”. 	FI

Table B-2: GRCM Detailed Observations and Estimated Level of Capability

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Strategic planning	Aug 07 to Oct 07	12 weeks	P - CIO S - PM, PS	An adequate infrastructure was available to accommodate the Corporate Intranet. The PM reported any variance to project cost or timescale to the Project Sponsor when required. There was no one who was assigned ownership and accountability for the technical risk.	2
IT Project Management	Aug 07 to Oct 07	12 weeks	P - PS S - PM - Web Developers	Project management techniques and controls could have been better applied according to the Project Management Body of Knowledge (PMBOK). The knowledge areas that were not followed by the Project sponsor were the cost and resources. The budget was not adequately funded to complete the project and resources were lacking to perform the work. A PM was assigned after the budget was given and the resources were allocated. The PM created a work breakdown structure (WBS) and divided into work packages and scaled accordingly. The WBS was created to ensure the web development work was according to web standardized specification set by the organization.	2
IT Control Framework	Aug 07 to Oct 07	12 weeks	P - PM S - Help Desk - Team Members	The PM asked the help desk to create a project shared folder to store project information. Only members of the project team had access to the project information. Sometimes it was difficult to maintain the document versions since it wasn't the best tool to use. It wasn't clear who was deciding what technology to use during the project implementation.	2

Green (3) = Fully Integrated / full capability, Yellow (2) = Semi Integrated / poor capability, Red (1) = Not Integrated /no capability

Table B-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Asset Management	Aug 07 to Oct 07	12 weeks	P - CIO S - Managers - Employees - Contractors	All of the organizations' computerized systems were located in a server room where proper ventilation was given, uninterruptible power supply were connected to the systems as well as back up servers. Access to the room was limited to card holders to prevent system tampering. The whole floor was protected by having a card swipe system at the entrance. A telephone was also available to call someone within the area. These protective measures protected corporate assets as well as organization information and prevented damage to assets and interruptions to business activities.	3
IT Processes	Aug 07 to Oct 07	12 weeks	P - IT Department S - PM, PS	The IT department had various IT processes in place to ensure the continuity of business and the security of systems and information. It also had established conformance processes but had no performance processes in place. The project inherited these processes.	2

Table B-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

RISK MANAGEMENT	Date	Duration	Primary (P) Secondary(S) Actors	Summary of events	Level of Capability
IT Governance Structure	Aug 07 to Oct 07	12 weeks	P - Director S - PS, - PM, - Web Developers, - Web Working Group	The organization as a whole had an IT governance structure in place. The IT structure consisted of the IT director, various sectors such as the networking group, desktop services and web development. The project governance structure consisted of the PS, PM, and web developers. These people were accountable for the success of the project, were effective and decisions made were transparent to the organization.	3
Audit and Monitor	Aug 07 to Oct 07	12 weeks	None identified	No specific auditing exercises were performed during the application built and test. No auditing committee was established.	1
Monitor and Track Risks Regularly	Aug 07 to Oct 07	10 weeks	P - PM S - Web Working Group	The PM created a risk register and identified all potential risks. Any critical risks were reported to the web working group for information or for resolution. The WBS was broken in work packages and known risks were built in to ensure timelines were met.	3
Perform Risk Analysis	Aug 07 to Oct 07	10 weeks	P - PM S - Web Working Group	After the risks were identified a risk analysis was performed. The level of impact, probability of it occurring, the mitigation strategy was considered. Cost to mitigate the risks was not considered.	2

Table B-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

COMPLIANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
Brief Project Mandate to Committees	Aug 07	.5 day	P - PS S - SMT	The PS presented the project to the Senior Management Team (SMT).	3
Ensure IT Alignment with Business	Aug 07	.5 day	P - PS S - SMT	The project sponsor ensured that the proposed IT project would be in line with current business practices at the SMT meeting. It was not apparent that IT investments decisions and performance measures demonstrated the value of IT.	2
Comply with Regulations, Policies and Standards	Aug 07 to Oct 07	12 weeks	P - PM S - SMT	The PM had to ensure the proposed Corporate Intranet design built by the web developers followed the Common Look and Feel (CFL) policy, standard set by the Treasury Board Secretariat.	3
Consider Security	Aug 07 to Oct 07	12 weeks	P - CIO S - IT Security	The organization enforced security since it was in the security business. All of its assets, resources and information were monitored by IT security. The security measures were also enforced at the project level.	3

Table-B-3: RE a Dependent Variable with its Constructs and Measures

RE - Dependent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Elicitation	<ul style="list-style-type: none"> The client needs to be involved and all requirements need to be identified by some means. 	SI
Analysis	<ul style="list-style-type: none"> Negotiation and conflict management is important. 	FI
Prioritization	<ul style="list-style-type: none"> The requirements need to be prioritized and classified. 	SI
Validation	<ul style="list-style-type: none"> The requirements need to be validated by the client. 	FI
Documentation	<ul style="list-style-type: none"> The requirements need to be clear so there are no misinterpretations of requirements by the developer. 	SI
Management	<ul style="list-style-type: none"> Requirement changes need to be managed 	SI

Table-B-4: RE Detailed Observations and Estimated Level of Capability

RE - Dependent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Elicitation	Aug 07 to Sept 07	6 weeks	P - PS S - Web Working Group - Developers	The PM held various working sessions with the stakeholders including the developers to discuss how the current Corporate Intranet was built and how they would like to see it tomorrow. High level requirements were flushed out. No user cases were built to better describe who will be using the system and what information they are looking for and when.	2
Analysis	Sept 07	2 weeks	P - PM S - Stakeholders	The PM conducted a requirement analysis with some of the stakeholders to identify which requirement were a need, want or a wish. After a negotiating period a requirement list was then developed and circulated to stakeholders for their acceptance.	3
Prioritization	Oct 07	1 week	P - PM S - Stakeholders	The PM with all the stakeholders tried to prioritize the requirements. The requirements were semi-prioritized. Some of the stakeholders could not agree on the priority of certain requirements. (e.g. some wanted more cosmetics versus functionalities)	2
Validation	Oct 07	1 week	P - PM S - Stakeholders	The requirements list was finally prioritized, validated and accepted by the stakeholders.	3

Table-B-4: RE Detailed Observations and Estimated Level of Capability (cont.)

RE - Dependent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Documentation	Oct 07	1 week	P - PM S - Stakeholders	A functional requirements document (FRD) was not developed due to a lack of resources. A list of requirements was available but traceability was not achievable. This document became official and required signing from the authorities before web development work could begin. This document ensured that the requirements were clear, concise and that everyone had the same interpretation of the requirements.	2
Management	Oct 07	1 day	P - PM S - Stakeholders	No change request process was in place. It was more of an ad-hoc process. The requirements list was stored in a locked cabinet where authorized personnel would have access to the original copy. Another working copy was stored on the project shared drive where project team members with permission rights had access.	2

Table B-5: OC an Independent Variable with its Construct and Measure

OC – Independent Variable	Organizational Context	Measure (NI, SI, FI)
Management Support	Senior Management Leadership/Commitment	FI

Table B-6: OC Detailed Observations and Level of Capability

OC – Independent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Management Support	Aug 07 to Oct 07	12 weeks	P - SMT S - PS, PM	The project had full support of the Senior Management Team.	3

APPENDIX C - Case Study C: Travel Automation Information System

Abstract

In the fall of 2007 an organization was interested in automating some of their manual steps to their travel processes. Its financial services were responsible for processing travel claims for its employees. Many local and international claims were submitted to the travel office thus requiring more resources to process the numerous claims. At the time the travel office was barely meeting the service level to process claims. The travel clerk had voiced their concerns that if the claims kept increasing they would not be able to meet their service level agreement (SLA). The financial department responded to the clerks' concerns by standing up a project.

The project mandate was to identify which manual steps in the travel processes needed to be automated and what software would be used.

An option and analysis document was created by the project team and was presented to the appropriate authorities. A recommendation was also given as to what the organization should consider to move forward. Since the project was not part of the overall plan it was not deemed a priority. As of the summer of 2008 the project has not yet commence.

A closer look on how governance, compliance and risk management (GRCM) was integrated during the project was considered. As well various elements such as requirements, resources, lifecycle, processes, disciplines, roles, tasks, artifacts, guidelines and risks were also discussed.

The study concludes with various tables. The data in the tables indicate the level of GRCM integration and level of capability, the RE integration and level of capability, and the Organizational Context support and level of capability. The data recorded in the tables is a recollection of the author's experience working on the project as a project manager.

Key words: governance, compliance, project management, steering committee, change advisory board, requirements engineering, risks

Introduction

The organization needed to automate some manual steps in their travel process. The travel office clerks' were concerned that travel claims were not being processed fast enough. This turned some employees into disgruntled employees. The Financial services in charge of travel claims decided to look for a solution. It moved forward and appointed a project manager and project officer to work on a solution. The organization wanted to know what manual steps in the travel process could be automated, how the travel office could benefit, the impact on the existing infrastructure, network, and which application will be used.

The project needed to come up with an options and analysis and a recommendation of a proposed solution for its Travel Automation Information Systems.

Governance Structure

The finance services consisted of a director general (DG) and functional managers. The DG reported the progress of the project further up to the executive level. The project sponsor for this project was a functional manager within the finance department. The project manager was appointed to lead and manage the project. Every week the project manager presented a status report to the project sponsor showing the project progress as well as potential risks and issues.

Compliance

The travel automation information system needed to be compliant with the travel directives set by Treasury Board of Canada. The implementation of the Travel Automation Information system would result in the timely processing of claims (x per month), would be equitable to all users submitting claims due to built-in established guidelines and would reduce/eliminate calculation errors.

Process:

The organization required a system that would process travel claims and take advantage of automation where possible. The system should allow the user to complete and send travel request, allow the responsible authorities to approve the request, process and track it, as well re-imburse the travel claim. The travel claim should be processed within a reasonable time-frame.

The travel automation project proceeded with the requirement engineering (RE) process. It met with various stakeholders to identify, gather and record business, functional and non-functional requirements. Some of the stakeholders included people working in the Travel office, administrative officers and travel coordinators. A business model was presented during the various working sessions but no user cases or scenarios were created. This was due of not having a business analyst as part of the project team.

The project looked at various options such as using a system that was being used by other government departments, shared travel services offered to various government departments, in house application and commercial of the shelf (COTS).

Lifecycle:

The project was using a waterfall lifecycle model to scope out possible solutions. The stakeholders were interested in knowing all the requirements before they would buy-in to possible solutions.

Disciplines:

The disciplines being covered by this project was the business modeling, requirements, analysis and design and project management.

Roles:

The project team consisted of various roles and it was fulfilled with people having different skill set and knowledge. A role that was missing during the RE process was a business analyst.

The project roles were the following:**Project Sponsor**

A person with authority that represented the organization undertaking the project as well as funding it.

Project Manager

A person appointed to lead and manage the project and its deliverables.

Project Officer

Assisted the project manager on various administrative tasks. Looked at travel directives to ensure the options were compliant to the travel directives set by TB.

Software developers

Responsible in analyzing various options ensuring the technical aspect of the option was viable.

Travel Office Staff

Responsible in ensuring the proper requirements are transmitted to the project team.

Stakeholders

Interest groups whose needs must be satisfied by the project. They are the ones that are most likely impacted by the project.

Tasks:

Each role had specific tasks to perform in order to complete the option and analysis exercise.

The tasks identified for each role were the following:

Project Sponsor/Business Owner – (Employee)

- Provided project funding to cover monthly expenses
- Monitored the project progress to ensure the project benefits will be realized
- Reported the project progress to the senior executives
- Provided guidance in respect to travel processes to the project manager when required

Project Manager – (Consultant)

- Established the project's defined RE process
- Met with stakeholders to go through the RE process
- Managed stakeholders expectation
- Ensured proper management documents were created and available
- Created a work breakdown schedule and implementation plan (schedule)
- Monitored and control the project schedule including team member tasks
- Mentored the project officer
- Created a risk and issue log
- Reported the project progress to the Project Sponsor

Software Developer – (Employee)

- Assist the project team in selecting appropriate software options and ensure they can be implemented in the existing architecture.

Project Officer (Employee)

- Performed various administrative tasks
- Created a spreadsheet identifying the travel directives that pertained to the project automated travel information system
- Acted as a liaison between other organization using a travel information system and the project

Travel Office Staff (Employees)

- Assisted the Project manager and Project Officer with the Travel Business model
- Identified the manual steps that needed to be automated
- Assisted in the selection of possible options

Stakeholders (Employees)

- Participated in the RE process
- Reviewed the option and analysis document
-

Artifacts

The project used the Project Management Body of Knowledge (PMBOK) as a good practice and many of the artifacts were derived from it. An option and Analysis document was prepared and distributed to various stakeholders for their feedback. The document was finalized and presented to the executive team. Other documents such a work break down schedule was created by using MS Project, a risk and issue log was created to identify risks, power point presentations were created and presented to the project sponsor, travel office staff and other stakeholders in regards to possible options.

Guidelines:

The Travel Directive set by Treasury Board of Canada were used as a guide when the various options were identified and considered.

Risks

During the option analysis a risk assessment was performed for each option. This exercise was done to ensure no major risk would have an impact on the proposed option. If a major impact was identified and the probability was high the option would be marked as risky. Once the exercise was completed three options were considered. The risk factor played a major part in selecting the options even more so for the final recommendation.

Challenges

One major challenge was the lack of a business analyst. It would have been helpful to have a business analyst on the project team to properly build a business model including use cases and scenarios. The stakeholders would have been more in tuned with the RE process.

Another challenge seemed to be with the technical services. They had previously began working on a solution without even going through the RE process. It was more of a fast solution rather than an optimal one. It was difficult to get their input at the beginning until they noticed the RE process was working.

Once the recommendation was presented to the appropriate authorities no further action was taken. At the last minute the project was no longer on the organization priority list of projects. This was the end of the project for now until it would be reprioritized as high.

Conclusion

The paper addresses how GRCM was applied in the organization. It gives an idea on the approach the organization took to ensure its requirements were defined (RE process) prior to selecting a Travel Automated Information System. It also described the challenges the project had with the lack of a business analyst, technical services and reprioritization of the project.

As part of the data analysis, tables were created in respect to the GRCM implementation, the applied RE process and the organizational context.

The following is a list of the tables where data was recorded as part of the data analysis.

1) Table C-1: GRCM an Independent Variable with its Constructs and Measures

This table describes the operationalization statements (constructs) and indicates if they are integrated.

2) Table C-2: GRCM Detailed Observations and Estimated Level of Capability

3) Table C-3: RE a Dependent Variable with its Constructs and Measures

4) Table C-4: RE Detailed Observations and Estimated Level of Capability

5) Table C-5: OC an Independent Variable with its Construct and measure

6) Table C-6: OC Detailed Observations and Level of Capability

This case study in addition to three more is part of an analysis where the following question will be answered.

Can this data lead us to believe that the GRCM integrated in the projects do enhance Requirements Engineering?

Table C-1: GRCM an Independent Variable with its Constructs and Measures

Independent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Governance		
<ul style="list-style-type: none"> IT Strategic Planning 	<ul style="list-style-type: none"> Adequate infrastructure 	SI
	<ul style="list-style-type: none"> First point of escalation for variance to project cost and timescale 	FI
	<ul style="list-style-type: none"> Assign ownership and accountability for technical risks 	SI
<ul style="list-style-type: none"> IT Project Management 	<ul style="list-style-type: none"> Employ sound project management techniques and controls 	SI
	<ul style="list-style-type: none"> Small scope and scale 	FI
	<ul style="list-style-type: none"> Request realistic and adequate budget 	FI
	<ul style="list-style-type: none"> Adhere to standardized specifications 	FI
<ul style="list-style-type: none"> IT Control Framework 	<ul style="list-style-type: none"> Development of management control structure 	FI
	<ul style="list-style-type: none"> Create an accountability framework 	SI
	<ul style="list-style-type: none"> Establish an access control to information 	FI
<ul style="list-style-type: none"> IT Asset Management 	<ul style="list-style-type: none"> To prevent damage to assets and interruptions to business activities 	FI
	<ul style="list-style-type: none"> To maintain appropriate protection of corporate assets 	FI
	<ul style="list-style-type: none"> To ensure that information assets receive an appropriate level of protection 	FI
<ul style="list-style-type: none"> IT Processes 	<ul style="list-style-type: none"> Establish IT processes 	SI
	<ul style="list-style-type: none"> Establish conformance process 	SI
	<ul style="list-style-type: none"> Establish performance processes 	SI
Risk Management		
<ul style="list-style-type: none"> Embed into the project/enterprise an IT governance structure 	<ul style="list-style-type: none"> The structure needs to be accountable, effective and transparent 	SI
<ul style="list-style-type: none"> Support auditing and monitoring operations 	<ul style="list-style-type: none"> Support a variety of different auditing and monitoring operations 	NI
	<ul style="list-style-type: none"> Establish an auditing committee 	NI
<ul style="list-style-type: none"> Monitor and Track risk regularly 	<ul style="list-style-type: none"> Active monitoring and regular viewing of risks 	FI
	<ul style="list-style-type: none"> Risk monitoring and control 	FI
	<ul style="list-style-type: none"> Breaking the project into smaller pieces to better addressed and manage risks. 	FI

Table C-1: GRCM an Independent Variable with its Constructs and Measures (cont.)

Independent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Risk Management		
<ul style="list-style-type: none"> Risk analysis is part of the project ongoing monitoring of IT risks and controls 	<ul style="list-style-type: none"> Perform analysis and assessment of risks including asset value, vulnerability and threat. 	SI
	<ul style="list-style-type: none"> Require risk decision process supported by risk analysis, identification and evaluation. 	SI
Compliance		
<ul style="list-style-type: none"> Brief project mandate to committees involved 	<ul style="list-style-type: none"> Ensure adequate visibility of the project. 	SI
<ul style="list-style-type: none"> Ensure IT alignment with business 	<ul style="list-style-type: none"> Align IT with enterprise objectives. 	SI
	<ul style="list-style-type: none"> Ensure that IT investments decisions and performance measures demonstrate the value of IT. 	SI
<ul style="list-style-type: none"> Comply with regulations, policies and standards 	<ul style="list-style-type: none"> Systems to be compliant with organizational security, policies and standards. 	FI
	<ul style="list-style-type: none"> Ensure compliance with legislation, regulations, security policies and rules. 	FI
<ul style="list-style-type: none"> Consider security in the project 	<ul style="list-style-type: none"> Need to consider security “from the ground up”. 	FI

Table C-2: GRCM Detailed Observations and Estimated Level of Capability

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Strategic planning	Apr 07 to Jul 07	16 weeks	P - PS S - PM	The project had an adequate infrastructure to work with. The project manager (PM) reported any variance to project cost or timescale to the Project Sponsor when required. There was no one who was assigned ownership and accountability for the technical risk.	2
IT Project Management	Apr 07 to Jul 07	16 weeks	P - PM S – SME's	The PM practiced techniques and controls according to the Project Management Body of Knowledge (PMBOK). The project sponsor had allocated the funds for an option analysis exercise but no other funds were allocated to implement the project. The PM created a work breakdown structure (WBS) to divide work packages and scaled accordingly. Various subject matter experts (SME's) were consulted to get the information. The WBS was created to meet standardized specification set by the organization towards the traveling process.	2
IT Control Framework	Apr 07 to Jul 07	16 weeks	P - PM S -Team Members	The PM created a project shared folder to store project information. Only members of the project team had access to the project folders within the project shared folder. It was difficult to maintain the versions of the documents. The PM needed to ensure the latest document version was available when reporting was required. It wasn't clear who was deciding what technology to use during the project implementation.	2

Green (3) = Fully Integrated / full capability, Yellow (2) = Semi Integrated / poor capability, Red (1) = Not Integrated /no capability

Table C-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Asset Management	Apr 07 to Jul 07	16 weeks	P - Director S – Managers Employees Contractors	All of the organizations’ computerized systems were located in a server room where proper ventilation was given, uninterruptible power supply were connected to the systems as well as back up servers. Access to the room was limited to card holders to prevent system tampering. The whole floor was protected by having a card swipe system at the entrance. These protective measures protected corporate assets as well as organization information and prevented damage to assets and interruptions to business activities.	3
IT Processes	Apr 07 to Jul 07	16 weeks	P - Director S – Managers	The IT department had various IT processes in place to ensure the continuity of business and the security of systems and information. It also had established conformance processes but had no performance processes in place.	2

Table C-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

RISK MANAGEMENT	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Governance Structure	Apr 07 to Jul 07	16 weeks	P - Director S - Networking - Service Desk - Desktop Applications	<p>The organization as a whole had an IT governance structure in place. The structure consisted of an IT director, with various sectors such as networking, service desk and desktop applications.</p> <p>The project governance structure consisted of the Director, a functional manager who she was manager, a Project Manager and Project Officer (PO).</p> <p>The project had a governance structure in place but getting decisions from upper management took a long time. The structure was not efficient.</p>	2
Audit and Monitor	Apr 07 to Jul 07	16 weeks	None identified	No specific auditing exercises were performed during the application built and test. No auditing committee was established.	1
Monitor and Track Risks regularly	Apr 07 to Jul 07	15 weeks	P - PM S - PS, PO	A risk register was created and all potential risks were identified and monitored weekly. Critical risks were reported to the Project Sponsor for information or for resolution. The WBS was broken in work packages and known risks were built in to ensure timelines were met.	3
Perform risk analysis	Apr 07 to Jul 07	15 weeks	P - PM S - Web Working Group	After the risks were identified a risk analysis was performed. The level of impact, probability of it occurring, and the mitigation strategy was considered. Cost to mitigate the risks was not considered.	2

Table C-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

COMPLIANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
Brief project mandate to committees	Apr 07	.5 day	P - PM S - Financial Managers	The PM presented the project to the financial managers. It was not presented to the senior management team.	2
Ensure IT Alignment with business	Apr 07	1 week	P - Finance Department S - PS, SMT	The Finance department wanted to have the Travel Automation System but was not aligned with the organization overall business priorities. This led the project to be shelved after the option and analysis phase. The finance department was aware of the IT investment required to complete this project, knew the value of IT but failed to sell it to the SMT.	2
Comply with regulations, policies and standards	Apr 07 to Jul 07	16 weeks	P - PM S - Stakeholders	The PM needed to ensure the proposed system was compliant with organizational security, policies and standards as well with Treasury Board travel directives.	3
Consider security	Apr 07 to Jul 07	16 weeks	P - Director S - IT Security	The organization enforced security since it was in the security business. All of its assets, resources and information were monitored by IT security. The security measures were also enforced at the project level.	3

Table C-3: RE a Dependent Variable with its Constructs and Measures

RE - Dependent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Elicitation	<ul style="list-style-type: none"> The client needs to be involved and all requirements need to be identified by some means. 	SI
Analysis	<ul style="list-style-type: none"> Negotiation and conflict management is important. 	SI
Prioritization	<ul style="list-style-type: none"> The requirements need to be prioritized and classified. 	SI
Validation	<ul style="list-style-type: none"> The requirements need to be validated by the client. 	SI
Documentation	<ul style="list-style-type: none"> The requirements need to be clear so there are no misinterpretations of requirements by the developer. 	SI
Management	<ul style="list-style-type: none"> Requirement changes need to be managed 	SI

Table C-4: RE Detailed Observations and Estimated Level of Capability

RE - Dependent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Elicitation	Apr 07 to Jul 07	7 weeks	P - PM, PO S - Stakeholders - Travel Office	The PM held various working sessions with the Project Officer, the stakeholders and travel office to identify the current travel process. Once the exercise was completed another was performed to streamline the current process. High level requirements were flushed out during this exercise. No user cases were built to better describe who will be using the system and what information they are looking for and when.	2
Analysis	May 07	1 week	P - PM, PO S - Stakeholders	The PM conducted a requirement analysis with some of the stakeholders to identify which requirement were a need, want or a wish. A list of requirements was created using Requisite Pro. No negotiation of requirements with stakeholders was performed due to time constraints.	2
Prioritization	May 07	1 week	Not performed	The project requirements were not prioritized due to time constraints and lack of funds.	2
Validation	June 07	1 week	Not performed	The requirements list was not validated by the stakeholders due to time constraints and lack of funds.	2
Documentation	June 07 to July 07	5 weeks	P - PM, PO S - IT Support - Stakeholders	An option and analysis document was written by the PM and IT support outlining the different options to procure or to build a "Travel Automation Information System". Due to lack of time it was not reviewed by various stakeholders.	2
Management	Jul 07	2 days	P - PM S - PO	No change request process was in place. It was more of an ad-hoc process. The requirements list was stored in a locked cabinet where authorized personnel would have access to the original copy. Another working copy was stored on the project shared drive where project team members with permission rights had access.	2

Table C-5: OC an Independent Variable with its Construct and Measure

OC – Independent Variable	Organizational Context	Measure (NI, SI, FI)
Management Support	Senior Management Leadership/Commitment	SI

Table C-6: OC Detailed Observations and Level of Capability

OC – Independent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Management Support	Apr 07 to Jul 07	16 weeks	P - SMT S - PS, PM	The project did not have full support or commitment of the Senior Management Team. This is the reason the project did not continue after the “Option and Analysis Phase”.	2

APPENDIX D - Case Study D: Financial Management Information System (FMIS)

Abstract

In the fall of 2006 an organization needed to update its existing financial management information system. The financial services were spearheading this initiative. The financial services were responsible for many aspects of finance. They included accounting operations, contracting and procurement, financial systems, strategic planning, policy and compliance and finance projects. The finance section of the organization was required to update their FMIS before fiscal year end. They also required historic data to be migrated during the FMIS implementation as well as other equipment upgrades.

A closer look on how governance, compliance and risk management (GRCM) was integrated during the project was considered. As well various elements such as requirements, resources, lifecycle, processes, disciplines, roles, tasks, artifacts, guidelines and risks were also discussed.

The study concludes with various tables. The data in the tables indicate the level of GRCM integration and level of capability, the RE integration and level of capability, and the Organizational Context support and level of capability. The data recorded in the tables is a recollection of the author's experience working on the project as a project manager.

Key words: governance, compliance, project management office, steering committee, change advisory board, requirements engineering, risks

Introduction

The organization required an update of their financial management information system which was a Commercial of the Shelf (COTS) application prior to fiscal year end. The update required the installation of new servers on the existing infrastructure, the latest version of the FMIS application, some application coding, and training various users across the organization. All the financial information since April 2004 needed to be migrated to the newly implemented system.

A business case was written by the project sponsor indicating the criticality of standing up a new project to deliver the new FMIS upgrade. The business case was accepted by upper management and funds were released to proceed with the FMIS implementation.

Governance Structure

The finance department consisted of a director general (DG) and functional managers. The DG reported the finance project progress to the executive committee. One of the

managers in the finance department was the project sponsor and business owner of the FMIS project.

The project had access to two committees during its existence. The committees were the project steering committee (PSC) and the Change Advisory Board (CAB). The PSC mandate was to give direction to the project manager when required or when decision making was required by upper management. The CAB was accessible to all projects and was responsible in assessing the impact due to proposed change requests (CR). If the CAB accepted the CR the PSC would usually approve the request.

Compliance

The FMIS needed to be compliant with the Treasury Board financial policy as well as with General Accepted Accounting Principals, and CCRA. The FMIS needed to be flexible and adaptable to quick changes in policy and regulations to remain compliant.

Requirements

The existing Financial Management Information system was a COTS product and was no longer supported by the vendor by the end of 2006. The organization needed to upgrade their FMIS to ensure continuous financial services to their various clients as well as ensuring support from the vendor. New servers were also required since the old ones were getting older and their reliability was questionable.

The upgraded version of the FMIS had new functionalities which demanded user training enterprise wide. The organization needed to ensure a training lab was available; trainers were available and technical support people available to correct technical glitches.

Some coding to the COTS was also required since the upgraded version was missing functionalities that the organization required. Custom interfaces were also added to the COTS application.

Previous data needed to be migrated onto the new servers since the FMIS was capable of retrieving historical data for reporting purposes.

Processes:

Prior to having the project manager appointed to the project no formal requirement engineering (RE) process was used by the project sponsor to identify the requirements. The project manager needed to go through the RE process to ensure the FMIS update would satisfy the users of the system. It was also an exercise to identify any potential impact the upgraded version of the FMIS would bring to the organization enterprise wide.

Lifecycle:

A waterfall lifecycle was used for the FMIS implementation as well as for the software coding. All requirements needed to be identified prior to the vendor doing some coding.

Disciplines:

The business modeling discipline was lacking in this project. No business model or use cases were used to show the stakeholders the reasons for the requirements.

Other disciplines were considered during each phase. It included some analysis and design, implementation, testing, deployment, configuration management due to new servers and project management throughout the project.

Roles:

The project team consisted of various roles and was fulfilled with people having different skill set and knowledge. Everyone together was focusing in the successful implementation of this project.

The project roles were the following:**Project Sponsor/Business Owner (Employee)**

A person with authority that represented the business client. The project sponsor was referenced as the business owner since the same organization was receiving the business benefit of the project deliverables.

Project Manager (Consultant)

A person selected by the organization to manage a project and deliver the outputs from beginning to end.

Business Analyst (N/A)

No business analyst was part of the project core team.

Systems Analyst (Employees)

Three employees from the technical section were part of the project core team. One was involved with the equipment upgrade, another was helping the vendor with the FMIS upgrade and another was working with the vendor on some coding.

Financial Analysts (Employee)

One employee from the financial section was part of the core team. The employee was responsible for writing the various test and acceptance plans.

FMIS Trainers (Employees and vendor)

The vendor initially trained the trainer. Two trainers in the finance section were available to provide training on the upgraded FMIS. Various users across the organization were trained on the upgraded FMIS.

External Vendor (Vendor)

Two employees from the vendor were part of the project core team. One was responsible for the deployment of the application while the other was supporting the financial analyst.

Stakeholders (Employees)

Interest groups whose needs must be satisfied by the project. They are the ones that are most likely impacted by the project.

Tasks:

Each role had specific tasks to perform in order to complete the entire project.

The tasks identified for each role were the following:

Project Sponsor/Business Owner – (Employee)

- Provided project funding to cover monthly expenses
- Monitored the project progress to ensure the project benefits would be realized
- Reported the project progress to the senior executives
- Intermediary between the project management and vendor

Project Manager – (Consultant)

- Established the project's define RE process
- Met with stakeholders to go through the RE process
- Managed stakeholders expectation
- Ensured newly implemented system features or enhancements met user needs as documented in the requirement specifications
- Ensured proper management documents were created
- Created a work breakdown schedule and an implementation plan (schedule)
- Created and maintained a Risk Register
- Reported the project progress to the Project Sponsor
- Met on a weekly basis with the project team members to discuss project progress, risks and issues
- Present change request to the PSC and CAB

Systems Analyst (Employees)

- Participated in the FMIS requirements working sessions
- Ensured supplementary requirements were well defined
- Identified specifications for servers
- Procured servers and other hardware and software
- Installed servers and operating system – in test environment
- Installed COTS application – server and client in test environment
- Performed migration of data in test environment
- Applied coding to application in test environment
- Installed servers and operating system – in test environment
- Installed COTS application – server and client in production environment
- Performed migration of data in production environment
- Applied coding to application in production environment
- Ensured users had access to the newly implemented FMIS

Financial Analysts (Employees)

- Participated in the FMIS requirements working sessions
- Created test plans on various module of the FMIS as well as acceptance test plan
- Performed testing on the various FMIS modules
- Assisted the vendor with the configuration of various FMIS modules

FMIS Trainers (Employees and vendor)

- Attended train the trainer course
- Ensured training material was reflecting the new upgraded version of the FMIS
- Scheduled training sessions and contacted participants requiring FMIS training
- Ensured training material was available for distribution prior to training sessions
- Trained employees on various FMIS modules

External Vendor (Employees)

- Assisted the project manager with the work breakdown structure and implementation plan (schedule)
- Assisted the systems analyst with the implementation of the upgraded FMIS
- Verified the financial analyst test and acceptance plans
- Ensured newly implemented system features or enhancements met user needs as documented in the requirement specifications
- Setup a train the trainer course for the new version of FMIS
- Performed coding to enhance some of the functionalities

Stakeholder (Employees)

- Participated in the requirement process
- Reviewed test plans

- Attended training sessions

Artifacts:

The project used the Project Management Body of Knowledge (PMBOK) as a good practice and many of the artifacts were derived from it. Some of the artifacts produced by the project included a Project Charter, a Project Initiation Plan, a Project Work Breakdown Structure including a schedule, a requirements document, a risk and issue log, monthly status reports financials, lessons learned document, agendas and project team weekly minutes with action items.

Guidelines

The project followed guidelines from CCRA, Treasury Board, General Accepted Accounting principles, internal policies and procedures when the requirements were being considered.

Risks

Continuous risk management was applied by the project. The project manager tracked and monitored the identified risks. Every week at the project team meeting the project managers covered the risk and issues log. The risks were identified and tagged for resolution and assigned to the appropriate person. Risks outside of the project scope were brought forward to the Senior Management Committee to be addressed.

Challenges

There were a few challenges throughout the project phases.

The servers were late in arriving thus the project needed to use the existing servers hoping the servers would hold until the new one came in.

It took some energy to have the vendor agree on some of the coding required to satisfy the user requirements. Not all changes were done. Some were still outstanding after the implementation. None were critical in nature.

There was some concern that the existing FMIS would encounter technical problems and the vendor or manufacturer was incapable of supporting the existing application. The application was a few versions behind thus being no longer supported by the end of December 2006.

The vendors had limited resources and needed to know in advance what the changes were to the COTS product.

Some people scheduled for the upgraded FMIS training, were not showing up thus prolonging the training schedule.

Conclusion

The paper addresses how GRCM was applied in the organization. It gives an idea on the approach the organization took to ensure its requirements were defined (RE process) prior the testing and deployment of the upgraded FMIS. It also described the various challenges it encountered throughout the project phases.

As part of the data analysis, tables were created in respect to the GRCM implementation, the applied RE process and the organizational context.

The following is a list of the tables where data was recorded as part of the data analysis.

1) Table D-1: GRCM an Independent Variable with its Constructs and Measures

This table describes the operationalization statements (constructs) and indicates if they are integrated.

2) Table D-2: GRCM Detailed Observations and Estimated Level of Capability

3) Table D-3: RE a Dependent Variable with its Constructs and Measures

4) Table D-4: RE Detailed Observations and Estimated Level of Capability

5) Table D-5: OC an Independent Variable with its Construct and measure

6) Table D-6: OC Detailed Observations and Level of Capability

This case study in addition to three more is part of an analysis where the following question will be answered.

Can this data lead us to believe that the GRCM integrated in the projects do enhance Requirements Engineering?

Table D-1: GRCM an Independent Variable with its Constructs and Measures

Independent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Governance		
• IT Strategic Planning	• Adequate infrastructure	FI
	• First point of escalation for variance to project cost and timescale	FI
	• Assign ownership and accountability for technical risks	FI
• IT Project Management	• Employ sound project management techniques and controls	FI
	• Small scope and scale	FI
	• Request realistic and adequate budget	FI
	• Adhere to standardized specifications	FI
• IT Control Framework	• Development of management control structure	FI
	• Create an accountability framework	FI
	• Establish an access control to information	FI
• IT Asset Management	• To prevent damage to assets and interruptions to business activities	FI
	• To maintain appropriate protection of corporate assets	FI
	• To ensure that information assets receive an appropriate level of protection	FI
• IT Processes	• Establish IT processes	FI
	• Establish conformance process	FI
	• Establish performance processes	FI
Risk Management		
• Embed into the project/enterprise an IT governance structure	• The structure needs to be accountable, effective and transparent	FI
• Support auditing and monitoring operations	• Support a variety of different auditing and monitoring operations	NI
	• Establish an auditing committee	NI
• Monitor and Track risk regularly	• Active monitoring and regular viewing of risks	FI
	• Risk monitoring and control	FI
	• Breaking the project into smaller pieces to better addressed and manage risks.	FI

Table D-1: GRCM an Independent Variable with its Constructs and Measures (cont.)

Independent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
<ul style="list-style-type: none"> Risk analysis is part of the project ongoing monitoring of IT risks and controls 	<ul style="list-style-type: none"> Perform analysis and assessment of risks including asset value, vulnerability and threat. 	FI
	<ul style="list-style-type: none"> Require risk decision process supported by risk analysis, identification and evaluation. 	FI
Compliance		
<ul style="list-style-type: none"> Brief project mandate to committees involved 	<ul style="list-style-type: none"> Ensure adequate visibility of the project. 	FI
<ul style="list-style-type: none"> Ensure IT alignment with business 	<ul style="list-style-type: none"> Align IT with enterprise objectives. 	FI
	<ul style="list-style-type: none"> Ensure that IT investments decisions and performance measures demonstrate the value of IT. 	FI
<ul style="list-style-type: none"> Comply with regulations, policies and standards 	<ul style="list-style-type: none"> Systems to be compliant with organizational security, policies and standards. 	FI
	<ul style="list-style-type: none"> Ensure compliance with legislation, regulations, security policies and rules. 	FI
<ul style="list-style-type: none"> Consider security in the project 	<ul style="list-style-type: none"> Need to consider security “from the ground up”. 	FI

Table D-2: GRCM Detailed Observations and Estimated Level of Capability

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Strategic planning	Sept 06 to Mar 07	26 weeks	P - PM S - PS - NI Team	An adequate infrastructure was available for the Financial Management Information System (FMIS). The PM reported any variance to project cost or timescale to the Project Sponsor (PS) as required. The network infrastructure (NI) team was assigned ownership and accountability to ensure the systems were available for the developers to work on.	3
IT Project Management	Sept 06 to Mar 07	26 weeks	P - PM S - Team Members - SME's	The PM followed sound project management techniques and controls based on the Project Management Body of Knowledge (PMBOK). The work breakdown structure (WBS) was divided in work packages and scaled accordingly. The PM met with team members and various subject matter experts (SME's) to discuss their work to be completed. The budget allocated to perform the work was adequate. The WBS was created to meet standardized specification set by the organization.	3
IT Control Framework	Oct 06 to Mar 07	24 weeks	P - PM S - Team Members - IT Support	The PM used a project shared folder to store project information. Only members of the project team had access to the information within the project shared folder. A list of most recent documents was available to the project team members. IT support was part of the project team which helps the project in identifying what technology (servers / operating system) were required to host the application.	3

Green (3) = Fully Integrated / full capability, Yellow (2) = Semi Integrated / poor capability, Red (1) = Not Integrated /no capability

Table D-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

GOVERNANCE	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Asset Management	Sept 06 to Mar 07	26 weeks	P - IT Department S - Managers - Employees - Contractors	All of the organizations' computerized systems were located in a server room where proper ventilation was given, uninterruptible power supply were connected to the systems as well as back up servers. Access to the room was limited to card holders to prevent system tampering. These protective measures protected corporate assets as well as organization information and prevented damage to assets and interruptions to business activities.	3
IT Processes	Sept 06 to Mar 07	26 weeks	P - IT Department S - PM - Team members	The IT department had various IT processes in place to ensure the continuity of business and the security of systems and information. It also had established conformance processes and performance processes in place. The project followed these practices.	3

Table D-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

RISK MANAGEMENT	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
IT Governance Structure	Sept 06 to Mar 07	26 weeks	P - IT Director - DG Finance - PM S - Team members - IT support	The organization as a whole had an IT governance structure in place. The IT structure consisted of the IT director, various sectors such as the networking group, desktop services and software applications. The project governance structure consisted of the PS, PM, and various team members such as the system analysts, financial analysts, FMIS trainers, external vendors and other stakeholders. These people were accountable for the success of the project, were effective and decisions made were transparent to the organization.	3
Audit and Monitor	Sept 06 to Mar 07	26 weeks	None Identified	No specific auditing exercises were performed during the application built and test. No auditing committee was established.	1
Monitor and Track Risks regularly	Sept 06 to Mar 07	24 weeks	P - PM S - Team Members	A risk register was created and all potential risks were identified and monitored weekly. Any critical risks were reported to the web working group for information or for resolution. The WBS was broken in work packages and known risks were built in to ensure timelines were met.	3
Perform risk analysis	Sept 06 to Mar 07	26 weeks	P - PM S - Team Members	After the risks were identified a risk analysis was performed. The level of impact, probability of it occurring, the mitigation strategy and the cost to mitigate the risk were all considered.	3

Table D-2: GRCM Detailed Observations and Estimated Level of Capability (cont.)

Compliance	Date	Duration	Primary (P) Secondary (S) Actors	Summary of events	Level of Capability
Brief project mandate to committees	Sept 06	.5 day	P - PM S - PSC	The PM presented the project to the project Steering Committee (PSC).	3
Ensure IT Alignment with business	Sept 06 to Mar 07	26 weeks	P - IT Director S - Director Generals, - Functional Managers	The IT director ensured that IT was aligned with the business. The IT director met with the project to discuss how the FMIS business aspect would integrate with the current IT infrastructure. It was apparent that the IT investment decision and performance measures demonstrated the value of IT.	3
Comply with regulations, policies and standards	Sept 06 to Mar 07	26 weeks	P - PS S - PM - Financial Analysts	All systems were compliant with legislation, regulations, security policies and rules. This included General Accepted Accounting Principals and the Canadian Custom Revenue Agency (CCRA).	3
Consider security	Sept 06 to Mar 07	26 weeks	P - IT Director S - IT Security	The organization enforced security since it was in the security business. All of its assets, resources and information were monitored by IT security. The security measures were also enforced at the project level.	3

Table D-3: RE a Dependent Variable with its Constructs and Measures

RE - Dependent Variable	Operationalization (Constructs)	Measure (NI, SI, FI)
Elicitation	<ul style="list-style-type: none"> The client needs to be involved and all requirements need to be identified by some means. 	FI
Analysis	<ul style="list-style-type: none"> Negotiation and conflict management is important. 	FI
Prioritization	<ul style="list-style-type: none"> The requirements need to be prioritized and classified. 	FI
Validation	<ul style="list-style-type: none"> The requirements need to be validated by the client. 	FI
Documentation	<ul style="list-style-type: none"> The requirements need to be clear so there are no misinterpretations of requirements by the developer. 	FI
Management	<ul style="list-style-type: none"> Requirement changes need to be managed 	FI

Table D-4: RE Detailed Observations and Estimated Level of Capability

RE - Dependent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Elicitation	Sept 06 to Oct 07	4 weeks	P - PM S - System Analysts - Financial Analysts - Stakeholders - Users	The PM with the system analysts and financial analysts performed this task to ensure requirements were identified to implement the FMIS COTS upgraded version. Various working sessions were held with stakeholders and users to discuss requirements. A business model was created to give a big picture on how the FMIS would integrate with other organizational systems.	3
Analysis	Oct 07	2 weeks	P - PM S - System Analyst - Financial Analyst - Stakeholders	A requirement analysis was conducted to identify which requirement were a need, want or a wish. A requirement list was then developed and circulated to stakeholders for their acceptance.	3
Prioritization	Oct 07	1 week	P - PM S - System Analyst - Financial Analyst - Stakeholders	The requirements on the list were prioritized as (high, medium, low).	3
Validation	Nov 07	1 week	P - PM S - Stakeholders	The requirements list was validated by the stakeholders and accepted.	3
Documentation	Nov 07	3 days	P - PM S - Stakeholders	The PM properly identified the requirements by using the Requisite Pro application. Requisite Pro is a Rational Product and is known as a Requirement Management application. A list of requirements was available and traceability was achievable by using Requisite Pro. This document ensured that the requirements were clear, concise and that everyone had the same interpretation of the requirements.	3

Table D-4: RE Detailed Observations and Estimated Level of Capability (cont.)

RE - Dependent Variable	Date	Duration	Primary (P) Secondary (S) Actors	Summary of Events	Level of Capability
Management	Sept 06 to Oct 07	4 weeks	P - PM S - CAB - Team Members	Change requests were processed and decisions were made by the Change Advisory Board (CAB). The change requests and requirements list were stored in a locked cabinet where authorized personnel would have access to the original copies. Working copies were stored on the project shared drive where project team members with permission rights had access.	3

Table D-5: OC an Independent Variable with its Construct and Measure

OC – Independent Variable	Organizational Context	Measure (NI, SI, FI)
Management Support	Senior Management Leadership/Commitment	FI

Table D-6: OC Detailed Observations and Level of Capability

OC – Independent Variable	Date	Duration	Primary (P) and Secondary (S) Actors	Summary of Events	Level of Capability
Management Support	Sept 06 to Mar 07	26 weeks	P - SMT S - PS - PM	The project had full support from the Senior Management Team (SMT).	3

REFERENCES

- Alavi, M., Carlson, P. (1992). "A review of MIS Research and Disciplinary Development." Journal of Management Information Systems **8**(4): 45-62.
- Alfonso, A., Braberman, V., Kicillof, N., Olivero, A. (2004). "Visual timed event scenarios. In Proc. of the IEEE Int. Conf. on Soft. Eng. (ICSE)." 168-177.
- Allen, J. (2005). An introduction to governing for enterprise security. Pittsburgh, Software Engineering Institute, Carnegie Mellon University.
- Alspaugh, A. T., Anton, I.A, (2001). Scenario networks for software specification and scenario management., North Carolina State University at Raleigh.
- Alves, C., Finkelstein, A. (2002). Challenges in COTS decision-making: a goal-driven requirements engineering perspective. In Proc. of the Int. Con. on Soft. Eng. and Know. Eng.: 789-794.
- Aoyana, M. (2005). Persona-and-scenario based requirements engineering for software embedded in digital consumer products. In. Proc. of the IEEE Int. Req. Eng. Conf. (RE): 85-94.
- Baker, P., Bristow, P., Jervis, C., King, D., Thomson, R., Mitchell, B., Burton, S. (2005). Detecting and resolving semantic pathologies in UML sequence diagrams. In Proc. of ACM SIGSOFT Found. on Soft. Eng. (FSE).
- Barki, H., Rivard, S., Talbot, J. (2001). "An Integrative Contingency Model of Software Project Risk Management." Management Information Systems **17**(4): 37-69.
- Beecham, S., Hatt, T., Rainer, A. (2003). "Defining a Requirement Process Improvement Model."
- Behr, K., Kim, G., Spafford, G. (2004). "The Visible Ops Handbook: Starting ITIL in 4 Practical Steps." Information Technology Process Institute.
- Benbasat, I., Goldstein, D.K., Mead, M. (1987). "The Case Research Strategy in Studies of Information Systems." MIS Quarterly: Management Information Systems **11**(3): 369-385.
- Berry, D., Kamsties, Ed. (2004). Ambiguity in Requirements Specification. Perspectives on Software Requirement, chapter 2., Kluwer Academic Publisher.
- Board, P. C. A. O. (2004). "Auditing Standard No.2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements."
- Boehm, B.W. (1981). Software Engineering Economics.
- Boehm, T. P., Wigle, G.B., Tsai, J.T. "Specification of software quality attributes." (Report RADC-TR-85-37.).
- BS (2002). "BS7799-2:2002 Information Security Management. Specification with guidance for use. British Standard."
- Bush, D., Finkelstein, A. (2003). Requirements stability assessment using scenarios. In Proc. of the IEEE Int. Req. Eng. Conf. (RE).
- Calvo-Manzano Villalón, J.A., Cuevas Agustín, G., San Feliu Gilabert, T., de Amescua Seco, A. (2002). "Experiences in the application of software process improvements in SME's." Software Quality Journal **10**(3): 261-273.

- Campbell, L.A., Cheng, B.H.C., McUumber, W.E., Stirewalt, R.E.K. (2002). "Automatically detecting and visualizing errors in UML diagrams." Req. Eng. J., **37**(10): 74-86.
- Carlshamre, P., Sandahl, K., Lindvall, M., Regnell, B., och Dag, J.N. (2001). An industrial survey of requirements interdependencies in software product release planning. In Proc. of the IEEE Int. Req. Eng. Conf. (RE).
- Chan, W., Anderson, R.J., Beame, P., Burns, S., Modugno, F., Notkin, D., Reese, J.D. (1998). "Model checking large software specifications." IEEE Trans. on Soft. Eng. **24**(7): 498-520.
- Cheng, H.C.B., Atlee, M. J. (2007). "Research Directions in Requirement Engineering." IEEE Computer Society.
- Claus, C., Freund, M., Kaiser, M., Kneuper, R., (1999). Implementing systematic requirements management in a large software development programme. Proceedings of the Fifth International Workshop on Requirements Engineering Foundation of Software Quality (REFSQ'99), Presses Universitaire de Namur, 1999.
- Cleland-Huang, J., Zemont, G., Lukasik, W. (2004). A hetero-geneous solution for improving the return on investment of requirements traceability. In Proc. of the IEEE Int. Req. Eng. Conf. (RE)
- Cohene, T., Easterbrook, S. (2005). Contextual risk analysis for interview design. In Proc. of the IEEE Int. Req. Eng. Conf. (RE).
- Conger, J.A., Lawler, E.E., Finegold, L.D. (2001). "Corporate Boards - New Strategies for Adding Value at the Top."
- Connell, B., Rochet, P., Chow, E., Savino, L., Payne, P. (2004). Enterprise governance getting the balance right.
- COSO (1992). Internal Control - Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission, Report. New York.
- Crawford, A., Ed. (1994). Advancing business concepts in a JAD workshop setting.
- Curtis, B. (1997). Software process improvement: methods and lessons learned. Proceedings of the 19th International Conference on Software Engineering (ICSE 1997).
- Damian, D., Moitra, D. (2006). "Global software development." IEEE Software **23**(5).
- Damian, D., Zowghi, D., Vaidyanathasamy, L., Pal, Y. (2002). An industrial experience in process improvement: an early assessment at the Australian Center for Unisys Software. Proceedings of the 2002 International Symposium on Empirical Software Engineering (ISESE'02).
- Daniela, E., Damian, H. (1999). "Challenges in Requirement Engineering." 4.
- Davis, A. (1992). "Operational Prototyping: A New Development Approach." Software **9**(5): 7-78.
- Dekkers, C.A. (2005). "Creating requirements-based estimates before requirements are complete." CrossTalk(4): 13-15.
- Diaz, M., Sligo, J. (1997). "How software process improvement helped Motorola." IEEE Software **14**(5): 75-81.
- Easterbrook, S. (1994). "Resolving requirements conflicts with computer-supported negotiation, in Jirotko, M. and Goguen, J. (Eds)." Requirements Engineering: Social and Technical Issues, Academic Press: 41-65.

- Easterbrook, S., Chechik, M. (2001). A framework for multi-valued reasoning over inconsistent viewpoints. In Proc. of the IEEE Int. Conf. on Soft. Eng. (ICSE).
- Eisenhardt, K.M. (1989). "Building Theories from Case Study Research." Academy of Management review **14**(4): 532-550.
- Engels, G., Küster, M. J., Heckel, R., Groenewegen (2001). "A methodology for specifying and analyzing consistency of object-oriented behavioral models." In Proc. of ACM SIGSOFT Found. on Soft. Eng (FSE): 186-195.
- Ewushi-Mensah (1997). "Critical issues in abandoned information systems development projects." Communications of ACM **40**(9): 74-80.
- Fagan, M. (1986). "Advances in software inspections." IEEE Trans. on Soft. Eng. **12**(7): 744-751.
- Feathers, S.M. (2004). "Towards a unified approach to the representation of, and reasoning with, probabilistic risk information about software and its system interface." In. Int. Sym. on Soft. Reliab. Eng., : 391-402.
- Firesmith, D. (2004). "Prioritizing Requirements." Journal of Object Technology **3**(8): 35-47.
- Forbes (2006). "IT Now." **48**: 8-9.
- Frame, J.D. (1994). The new project management: Corporate reengineering and other business realities. San Francisco: Jossey Bass.
- Glaser, B., Strauss, A., Ed. (1967). Discovery of Grounded Theory: Strategies of Qualitative Research. London: UK, Wiedenfeld and Nicholson.
- Goff, J. (2005). "Looking for Gaps." CFO: 53-58.
- Gonzales, R. (2005). "Quote from The Atlantic Systems Guild issue 2005." IEEE Software.
- Guha, S. et. al. (1997). "Business Process Change and Organizational Performance: Exploring the Antecedent Model." Journal of MIS **14**(1): 119-154.
- Hamaker, S. (2003). "Spotlight on Governance." Information Systems Audit and Control Association. **1**.
- Hardesty, D. (2003). "Practical Guide to Corporate Governance and Accounting: Implementing the Requirements of the Sarbanes-Oxley Act."
- Hardy, G. (2006). "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges." Information Security Technical Report **11**(1): 55-61.
- Hausmann, J.H., Heckel, R., Taentzer, G. (2002). Detection of conflicting functional requirements in a use case-driven approach. In Proc. of the IEEE Int. Conf. on Soft. Eng. (ICSE).
- Haworth, A.D., Pietron, R.L. (2006). "Sarbanes-Oxley: Achieving Compliance by Starting with ISO 17799." Information Systems Management.
- Hayes, J.H., Dekhtyar, A., Sundaram, S.K. (2006). "Advancing candidate link generation for requirements tracing: The study of methods." IEEE Trans. on Soft. Eng. **32**(1): 4-19.
- Heidenheimer, L.C., Kirby, J., Labaw, G.B., Bharadwaj, R. (1998). A toolset for specifying and analyzing software requirements. In Proc. of the Int. Conf. on Comp. Aid. Verf. (CAV): 526-531.
- Heitmeyer, I.C., Jeffords, D.R, Labaw, G.B. (1996). "Automated consistency checking of requirements specifications." ACM Trans. on Soft. Eng. & Meth. **5**(3): 231-261.

- Herbsleb, J., Mockus, A. (2007). "Global software engineering: The future of socio-technical coordination. ." In Future of Software Engineering.
- Herold, R. "The Practical Guide to Managing Risks." Qnet IQ.
- Hofmann, H., Lehner, Franz (2001). "Requirements Engineering as a Success Factor in Software Projects." IEEE Software(July/August 2001): 58-66.
- Hutchings, A.F., Knox, S.T., (1995). "Creating products: customer demand." ACM **38**(5): 72-80.
- I.T.G.I. (2000). "COBIT 3rd Edition: Executive Summary, COBIT Steering Committee and the IT Governance Institute, Illinois, USA, ISBN 1-893209-15-16."
- IEEE, Ed. (1984). IEEE Guide to Software Requirements Specifications (1984), IEEE Std 830-1984. . New York, NY 10017 USA.
- IIBA, Ed. (2006). A guide to the Business Analysis Body of Knowledge, International Institute of Business Analyst.
- ISACA (2007). "COBIT 4.1."
- ISO (2002). "BS ISO/IEC 17799: 2000 Information Technology. Code of practice for information security management. International Standard Organisation."
- ISO/IEC 9126, I. I. "Series of Standards for Measuring Software Quality, I/O/IEC."
- ITGI (2003). Board Briefing on IT Governance. USA, IT Governance Institute.
- ITGI (2003). "IT Governance Institute."
- ITGI (2005). "Aligning Cobit, ITIL and ISO 17799 for Business Benefit."
- ITGI (2005). "Information Risks: Whose Business are they."
- itSMF (2006). Foundation of IT Service Management, based on ITIL, Van Harsen Publishing.
- itSMF (2007). "An Introductory Overview of ITIL v.3."
- Jacobs, S. (1999). Introducing measurable quality requirements: a case study. Proceedings of the 4th IEEE International Symposium on Requirements Engineering, IEEE Computer Society Press.
- Jurison, J. (1999). "Software Project Management: The Manager's View." Communications of the Association for Information Systems **2**(29).
- Kaiya, H., Saeki, M. (2006). Using domain ontology as domain knowledge for requirements elicitation. In Proc. of the IEEE Int. Req. Conf. (RE).
- Kauppinen, M., Kujala, S. (2001). Starting improvement of requirements engineering processes: an experience report. Proceedings of the Third International Conference on Product Focused Software Process Improvement (Profes 2001), Springer, Berlin, Germany.
- Kauppinen, M., Kujala, S., Aaltio, T., Lehtola, L. (2002). Introducing requirements engineering : How to make a cultural change happen in practice. Proceedings of the IEEE Joint International Conference on Requirements Engineering (RE'02), IEEE Computer Society, Los Alamito, CA.
- Kauppinen, M., Vartiainen, Matti, Knotio, Jyrki, Kujala, Sari, Sulonen, Reijo (2004). "Implementing requirements engineering processes throughout organizations: success factors and challenges." Information & Software Technology.
- Kim, S. (2007). Governance of information security: New paradigm of security management. Studies in Computational Intelligence. N. Nedjah, L. Macedo Mourelle and A. Abraham. **57**: 235-254.

- Kim, S. (2007). "IT compliance of industrial information systems: Technology management and industrial engineering perspective." Journal of Systems and Software **80**(10): 1590-1593.
- Kim, S., Leem, C.S. (2005). "Security of the internet-based instant messenger: risks and safeguards." Internet Research: Electronic Networking Applications and Policy **15**: 88-98.
- Klein, H.K., Myers, M.D. (1999). "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems." MIS Quarterly: Management Information Systems **23**(1): 67-04.
- Knut S, B. P., Klakegg, O (2006). Front end Governance of Major Public Projects 1. Paper presented at the EURAM 2006 Conference in Oslo 18. May 2006.
- Kramer, J., Magee, J. (2007). "Self-managed systems: An architectural challenge." In future of Software Engineering.
- Krishnamurthi, S., Tschantz, C.M., Meyerovich, A.L., Fisler, K. (2005). Verification and change-impact analysis of access-control policies. In. Proc. of the IEEE Int. Conf. on Soft. Eng (ICSE).
- Lankhorst, M. (2005). "Enterprise Architecture modeling - the issue of integration." Advanced Engineering Informatics **18**: 205-216.
- Lankhorst, M., et. al. (1998). "Enterprise Architecture at Work: modeling, communication, and analysis." Springer.
- Larsen, H.M., Pedersen, K.M., Andersen, V.K (2006). "Reviewing 17 IT Governance Tools and Analyzing the Case of Novozymes A/S." IEEE.
- Lee, A.S. (1989). "A Scientific Methodology for MIS Case Studies." MIS Quarterly: Management Information Systems **13**(1): 33-52.
- Lincoln, Y. S., Guba, E.G., Ed. (2002). "Judging the Quality of Case Study Reports" in A.M. Huberman and M.B. Miles (eds.) The Qualitative Researchers' Companion, Thousand Oaks, CA, Sage Publications.
- Lipner, S. (2004). The Trustworthy Computing Security Development Lifecycle. Annual Computer Security Applications Conference (ACSAC).
- Luftman, J., Lewis, P., Oldach, S (1993). "Transforming the enterprise: The alignment of business and information technology strategies." IBM Systems Journal **31**(2).
- Lutz, R., Patterson-Hine, A., Nelson, S., Frost, C.R., Tal, D., Harris, R. (2006). "Using obstacle analysis to identify contingency requirements on an unpiloted aerial vehicle." Req. Eng. J., **12**(1): 41-54.
- Ma, Q., Pearson, J.M. (2005). "ISO 17799: "Best Practices" in Information Security Management." Communications of the AIS **15**.
- Magee, J., Pryce, N., Giannakopoulou, D., Kramer, J. (2000). Graphical animation of behavior models. In Proc. of the IEEE Int. Conf. on Soft. Eng. (ICSE).
- Maibaum, T. (2000). "Mathematical Foundations of Software Engineering: A roadmap." Future of Software Engineering.
- Maiden, N., Robertson, S. (2005). Integrating creativity into requirement processes: Experiences with an air traffic management system. In Proc. of the IEEE Int. Req. Eng. Conf. (RE): 105-116.
- Maiden, N., Rugg, G. (1996). "ACRE: Selecting Methods For Requirements Acquisitions." Software Engineering Journal **11**(3): 183-192.

- Markus, M.L. (1997). "The Qualitative Difference in Information Systems Research and Practice." 11-27.
- May, E., Zimmer, A (1996). "The Evolutionary Development Model for Software." Hewlett-Packard Journal.
- McFeeley, B., Ed. (1996). IDEAL: a user's guide for software improvement, Handbook CMU/SEI-96-HB-001. Pittsburgh, PE, USA, Carnegie Mellon University.
- Miles, M.B., Huberman, A.M., Ed. (1994). Qualitative Data Analysis: An Expanded Sourcebook. Beverly Hills, CA, Sage Publications.
- Mingay, S., Bittinger, S. (2002). Combine Cobit and ITIL for powerful IT governance. S. Gartner Inc.
- Mitchell, S. (2005). "Open Compliance and Ethics Group (OCEG): Foundation Guidelines "Red Book"."
- Moreira, A., Rashid, A., Araujo, J. (2005). Multi-dimensional separation of concerns in requirements engineering. In Proc. of the IEEE Int. Req. Eng. Conf. (RE).
- Moulton, R., Coles, R.S. (2003). "Applying information security governance." Computers and Security **22**: 580-584.
- Myers, M.D. (1987). "Qualitative Research in Information Systems." MISQ Discovery.
- Nakajo, T., Kume, H. (1991). "A Case History Analysis of Software Error, Cause and Effect Relationships." Transactions on Software Engineering **17**(8): 830-838.
- Neela, A.M., Mahoney, J. (2003). Work with, not against, your culture to refine IT governance. S. Gartner Inc.
- Nentwich, C., Emmerich, W., Finkelstein, A., Ellmer, E. (2003). "Flexible consistency checking." ACM Trans. on Soft. Eng. & Meth. **12**(1): 28-63.
- NIST "Risk Management Guide for IT Systems."
- Nuseibeh, B., Easterbrook, S. (2000). "Requirements Engineering: A Roadmap." ACM **2000**: 37-46.
- OECD (2000). "The Organization for Economic Co-operation and Development (OECD) US Mission to the OECD newsletter." **2**(1).
- OGC, I. (2005). "Aligning Cobit, ITIL and ISO 17799 for Business Benefit."
- Orlikowski, W.J., Baroudi, J. (1992). "The Duality of Technology: Rethinking the Concept of Technology in Structuration." Organization Science **3**(3): 398-427.
- Paetsch, F., Eberlein, A. Dr., Maurer, F. DR. (2003). "Requirements Engineering and Agile Software Development." IEEE Computer Society: 6.
- Paré, G. (2004). "Investigating Information Systems with Positivist Case Study Research." Communications of the Association of Information Systems **13**: 2004.
- Paré, G., Elam, J.J., Ed. (1997). "Using Case Study Research to Build Theories of IT Implementation" in A.S. Lee, J. Liebenau, and J.I. DeGross (eds.) Information Systems and Qualitative Research. London, UK, Chapman & Hall, pp. 542-568.
- Parnas, L.D., Weiss, M.D. (1987). "Active design reviews: principles and practices." J. Sys. Soft., **7**(4): 259-265.
- Parr, A., Shanks, G. (2000). "Model of ERP Project Implementation." Journal of Information Technology **14**(4): 289-304.
- Patton, M.Q., Ed. (2002). Qualitative Evaluation and Research Models. Newburk Park, CA, Sage Publications.

- PCAOB (2004). "Public Company Accounting Oversight Board. Auditing Standard No.2 - An audit of internal control over financial reporting performed in conjunction with an audit financial statements. New York."
- Phelan, P., Frey, N. (2002). Avoiding failure in large IT projects: new risk and project management initiatives. Gartner.
- Pisan, Y. (2000). Extending requirement specifications using analogy. In Proc. of the IEEE Int. Conf. on Soft. Eng. (ICSE): 70-76.
- PMI, Ed. (2004). A Guide to the Project Management Body of Knowledge. Third Edition, Project Management Institute.
- Poppendieck, M., Poppendieck, T. "A Rational Design Process - It's Time to Stop Faking It."
- Potts, C. (2001). Methaphors of intent. In Proc. of the IEEE Int. Req. Eng. Conf. (RE): 31-39.
- Ranjan, P., Misra, A. (2006). "A Hybrid Model for Agent Based System Requirement Analysis." ACM SIGSOFT Software Engineering Notes, Page 1 Volume 31(3).
- Regnell, B., Karlson, L., Host, M. (2003). An analytical model for requirements selection quality evaluation in product software development. In Pro. of the IEEE Int. req. Eng. Conf. (RE).
- Rex, R.K., Charles, S.A., Houston, C.H. (1991). "Risk Analysis for Information Technology." Journal of Management Information Systems 8.
- Robertson, S. (2005). "Learning from other disciplines." IEEE Software 22(3): 54-56.
- Robinson, N.W., Pawlowski, D.S, Volkov, V. (2003). "Requirements interaction management." ACM Comp. Sur., 35(2): 132-190.
- Rolland, C., Prakash, N. (2001). Matching ERP system functionality to customer requirements. In. Proc. of the IEEE Int. Req. Eng. Conf. (RE): 66-75.
- Ron, W., Ed. (1988). EDP auditing conceptual foundations and practice. New York, McGraw-Hill.
- Ryan, K. (1993). The role of natural language in requirements engineering. In Proceedings of the IEEE International Symposium on Requirements Engineering., IEEE Computer Society Press, Los Alamitos, CA.: 240-242.
- Salo, A., Käkölä, T. (1998). Requirement for groupware-supported requirements process in new prodcut development. Proceedings of the Fourth International Workshop on Requirements Engineering: Foundation of Software Quality (REFSQ'98), Presses Universitaires de Namur.
- Sawyer, P., Rayson, P., Cosh, K. (2005). "Shallow knowledge as an aid to deep understanding in early phase requirements engineering." IEEE Transactions on Software Engineering 31(11): 969-981.
- Schumacher, M., Roedig, U. (2001). Security Engineering with Patterns. PLOP
- Schuyler, Ed. (2001). Risk and Decision Analysis in Projects. Second Edition, Project Management Institute.
- Sharp, H., Finklestein, G. (1999). "Stakeholder identification in the requirement engineering process." 387-391.
- Shaw, M. (2002). ""Self-Healing": Softening precision to avoid brittleness. In Work, on Self-Healing Sys. (WOSS). Position Paper."
- Sommerville, I., Ed. (2001). Software Engineering, Addison-Wesley, Harlow, England.

- Sommerville, I. (2005). "Integrated Requirements Engineering: A Tutorial." IEEE Software.
- Sommerville, I., Sawyer, P. , Ed. (1997). Requirements Engineering: A Good Practice Guide. Chichester, England, Wiley.
- Spafford, G. (2003). "The Benefits of Standard IT Governance Frameworks." IT Management.
- Stake, R.E., Ed. (1995). The Art of Case Study Research,. Thousand Oaks, CA, Sage Publications.
- Standish, T.G. (2003). "Latest Standish Group CHAOS Report Shows Project Success Rates Have Improved by 50 Percent".
- Sumner, M. (1999). Critical Success Factors in Enterprise-Wide Information Management Projects. Proceedings of the America Conference on Information Systems, Milwaukee, US.
- Sutcliffe, A., Chang, C.W., Neville, R. (2003). Evolutionary requirements analysis. In. Proc. of the IEEE Int. Req. Eng. Conf. (RE).
- Sutcliffe, A., Fickas, S., Sohlberg, M.M. (2006). "PC-RE a method for personal and context requirements engineering with some experience." Requirement Engineering Journal **11**(3): 1-17.
- Thompson, J. M., Heimdahl, M.P.E., Miller, S.P. (1999). Specifications-based prototyping for embedded systems. In Proc. of ACM SIGSOFT Found. on Soft. Eng. (FSE).
- van Lamsweerde, A., Letier, E. (2000). "Handling obstacles in goal-oriented requirements engineering." IEEE Trans. on Soft. Eng. **26**(10): 978-1005.
- Vance, A. (2007). "Effectively Complying with Sarbanes-Oxley in Dynamic Business Environments: a Knowledge Traceability Approach." IEEE
- Wagner, S., Dittmar, L. (2006). "The Unexpected Benefits of Sarbanes-Oxley." Harvard Business Review **84**: 133-140.
- Wasson, K.S. (2006). A case study in systematic improvement of language for requirements. In Proc. of the IEEE Int. Req. Eng. Conf. (RE).
- Wasson, S.K., Schmid, N.K, Lutz, R.R., Knight, C.J (2005). Using occurrence properties of defect report data to improve requirements. In Proc. of the IEEE Int. Req. Eng. Conf. (RE): 253-262.
- Weber, M., Weisbrod, J. (2002). Requirements engineering in automotive development experiences and challenges. In. Proc. of the IEEE Int. Req. Eng. Conf. (RE): 331-340.
- Weigers, K. (1998). "Know your enemy: software risk management." Software Development.
- Wiegiers, K. (1999). "Software Requirements." Microsoft Press, Redmond, WA, USA.
- Winter, R., Schelp, J. (2008). "Enterprise Architecture Governance: The Need for a Business to IT Approach." ACM
- Winter, R., Schelp, J. (2008). Proceedings of the ACM Symposium on Applied Computing.
- Yin, R. K., Ed. (1993). Applications of Case Study Research. Beverly Hills: CA, , Sage Publications.
- Yin, R. K. (1999). "Enhancing the Quality of Case Studies in Health Services Research." Health Services Research **34**(5): Supplement Part 2, 1209-1224.

- Yin, R.K., Ed. (2003). Case Study Research, Design and Methods. Beverly Hills:CA, Sage Publications.
- Zachman, J.A. (1987). "Framework for information systems architecture." IBM Systems Journal **26**(3): 276-292.
- Zahran, S., Ed. (1998). Software Process Improvement: Practical Guidelines for Business Success. Harlow, England, Addison-Wesley.
- Zoellick, B., Frank, T. (2005). "Governance, Risk Management and Compliance: An Operational Approach."