

Indicator-based Policy Compliance of Business Processes

Azalia Shamsaei

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the degree of

Ph.D. in Computer Science

Under the auspices of the Ottawa-Carleton Institute for Computer Science



uOttawa

University of Ottawa
Ottawa, Ontario, Canada

October 2012

Abstract

Background: Business process compliance management has recently attracted a lot of attention in both business and academia as it enables organizations to not only control and monitor their business processes from a legal point of view but also to avoid financial penalties and undesirable consequences to their reputation.

Objective: This thesis aims to provide a framework that would enable organizations to:

- Discover business processes that violate regulations, laws and policies;
- Discover the importance level of business processes based on the organization's goals;
- Determine the impact of compliance-related process modifications on business goals, including conflicting goals between stakeholders, and on policies; and
- Enable organizations to measure the level of business process compliance for one or multiple policies.

Methodology: A systematic literature review in the area of goal-oriented business process compliance management and measurement has been conducted, which showed that balancing legal compliance obligations with business objectives remains a difficult challenge. A new Indicator-based Policy Compliance Framework (IPCF), which combines policy and rule models together with models capturing business goals (with their relative importance to the organization) and business processes, has been proposed. This framework builds on the User Requirements Notation (URN), which is the first international standard to combine goal modeling with scenario modeling. The intents and objectives of policies have been modeled, as well as the goals and business processes of organizations, and indicators are used to measure the compliance level of policies. This enables the detection of non-compliant business processes and the evaluation of the impact of compliance-related process modifications on business goals. Human resource policies and busi-

ness processes are used as an example to illustrate the method. Aerodrome security regulations and business processes are then used to validate the method in a real-life environment. Comparisons to related work, evaluation against different sets of criteria, and tool support complement the framework validation.

Results: The Indicator-based Policy Compliance Framework enables organizations to discover business processes that violate policies as well as other types of rules, regulations, and laws. Guidelines for modeling legal text with URN's Goal-oriented Requirement Language (GRL) are proposed. Furthermore, IPCF helps determine the impact of compliance-related process modifications on business goals, including conflicting goals between stakeholders, and on policies. In addition, as policies sometimes apply differently to different types of organizations, a new profile for GRL, with suitable stereotypes, well-formedness constraints, and a modified analysis algorithm defined for GRL model families is used to evaluate the satisfaction level of individual goal models that are members of a larger family model. Finally, the proposed IPCF enables organizations to measure the level of business process compliance for one or multiple policies, and such measures can be visualized directly in URN models but also through interactive Business Intelligence portals, for a wider diffusion.

Acknowledgment

I would like to gratefully thank Dr. Daniel Amyot, whose valuable guidance and supervision helped me very much and kept the project on track. I was very lucky to have him as my supervisor. Furthermore, I would like to thank my co-supervisor Dr. Eric Yu for his comments and input.

Many thanks to NSERC's Business Intelligence Network (BIN) and Collaborative Health Research Program for supporting and funding this research.

I would also like to thank my family for their constant support, especially my parents and my husband, Alireza Pourshahid, for their understanding throughout my studies, and all the people who were involved in our research team.

Table of Contents

Abstract	i
Acknowledgment	iii
Table of Contents	iv
List of Figures.....	viii
List of Tables	xi
List of Acronyms	xiii
Chapter 1. Introduction	1
1.1. <i>Concepts</i>	1
1.2. <i>Problem Statement</i>	4
1.3. <i>Motivations and Objectives</i>	5
1.4. <i>Research Method</i>	6
1.5. <i>Thesis Contributions</i>	7
1.5.1 Major Contributions	8
1.5.2 Minor Contributions	8
1.5.3 Validation and Impact	9
1.6. <i>Publications and Presentations Based on Thesis</i>	9
1.7. <i>Thesis Outline</i>	11
Chapter 2. Background.....	12
2.1. <i>Reports on Compliance</i>	12
2.2. <i>Authoritative Rules</i>	14
2.2.1 Regulations and Laws.....	14
2.2.2 Policies	15
2.2.3 Service Level Agreement (SLA).....	16
2.2.4 Standards	16
2.3. <i>Methodologies to Extract Metrics/Indicators</i>	17
2.3.1 Goal Question Metric (GQM).....	17
2.3.2 Practical Software and Systems Measurement (PSM)	18
2.3.3 Software Metrics - A Rigorous and Practical Approach	19
2.4. <i>Semantics of Business Vocabulary and Business Rules</i>	20

2.5.	<i>User Requirements Notation</i>	21
2.5.1	Goal-oriented Requirement Language.....	22
2.5.2	Use Case Maps.....	25
2.5.3	Tools Support - jUCMNav	29
2.6.	<i>URN for Compliance</i>	29
2.7.	<i>URN and Key Performance Indicators</i>	30
2.8.	<i>Goal Model Families</i>	31
2.9.	<i>Business Intelligence</i>	33
2.10.	<i>Summary</i>	33
Chapter 3. Systematic Literature Review		35
3.1.	<i>Introduction</i>	35
3.2.	<i>Phase 1: Selection of Related Work</i>	36
3.2.1	Identification of Search Engines and Other Sources	36
3.2.2	Selection Criteria.....	37
3.2.3	Inclusion/Exclusion Criteria and Procedures	38
3.3.	<i>Phase 2: Analysis of Related Work</i>	39
3.3.1	Quantitative Analysis of the Related Work	39
3.3.2	Analysis of the Papers Based on their Content	41
3.4.	<i>Phase 3: Summary of Selected Papers</i>	42
3.4.1	Compliance Frameworks and Standards	42
3.4.2	Measurement of Compliance Levels	45
3.4.3	Discovery and Control of Non-Compliant Business Processes	46
3.4.4	Goal-oriented Techniques and KPI	48
3.4.5	Others	49
3.5.	<i>Summary</i>	50
Chapter 4. Indicator-based Policy Compliance Framework.....		52
4.1.	<i>Framework Overview</i>	52
4.2.	<i>Step A: Modeling</i>	54
4.2.1	Regulations Structure	56
4.2.2	Procedures to Model Policies/Regulations from Legal Documents	59
4.2.3	Optimization Steps	70
4.3.	<i>Step B: Evaluation</i>	73
4.4.	<i>Step C: Improvement</i>	76
4.5.	<i>Step D: Monitoring</i>	76
4.6.	<i>Summary</i>	77
Chapter 5. Human Resource Case Study		79
5.1.	<i>Step A: Modeling</i>	79
5.1.1	Organization Business Process Model	79

5.1.2	Organization Business Goal Model.....	81
5.1.3	Policy Model.....	85
5.2.	<i>Step B: Evaluation</i>	89
5.2.1	Evaluation of Satisfaction Levels.....	90
5.2.2	Evaluation of Importance Values	93
5.2.3	Importance/Compliance Quadrant Diagram Representation	95
5.3.	<i>Step C: Improvement</i>	100
5.3.1	Rule Prioritization	101
5.3.2	Business Process Improvement.....	102
5.3.3	Handling of Goal and Rule Conflicts	103
5.4.	<i>Step D: Monitoring</i>	104
5.5.	<i>Summary</i>	109
Chapter 6. Evaluation Example – Aerodrome Perimeter Security		111
6.1.	<i>Step A: Modeling</i>	111
6.1.1	Organization Business Process Model	112
6.1.2	Organization Business Goal Model.....	116
6.1.3	Regulation Model.....	121
6.2.	<i>Step B: Evaluation</i>	123
6.2.1	Evaluation of Satisfaction Levels.....	124
6.2.2	Evaluation of Importance Values	125
6.2.3	Importance/Compliance Quadrant Diagram Representation	126
6.3.	<i>Step C: Improvement</i>	131
6.3.1	Rule Prioritization	131
6.3.2	Business Process Improvement.....	132
6.4.	<i>Step D: Monitoring</i>	139
6.4.1	Analysis of Three Strategies	139
6.4.2	Improved Visualization of Strategy Differences with jUCMNav	148
6.5.	<i>Summary</i>	153
Chapter 7. Specifying and Analyzing Goal Model Families with GRL		154
7.1.	<i>Example Illustrating the Issues</i>	155
7.1.1	Example of Regulation - Perimeter Security	155
7.1.2	Requirement for Families of Goal Models	156
7.2.	<i>First Attempt: Modeling Families with Standard GRL</i>	157
7.2.1	Modeling Goal Model Families with Dependency Links.....	157
7.2.2	Problem Definition	159
7.3.	<i>Solution: Measured Compliance Profile for GRL</i>	160
7.3.1	Specifying Goal Model Families with New GRL-Based Concepts	161
7.3.2	New Analysis Algorithm: Overview	162
7.3.3	Measured Compliance Profile: Summary of Stereotypes.....	165
7.3.4	New Analysis Algorithm: Formal Definition	167
7.3.5	Measured Compliance Profile: OCL Well-Formedness Rules	173

7.4.	<i>Limitations and Threats to Validity</i>	174
7.5.	<i>Summary</i>	175
Chapter 8. Evaluation		177
8.1.	<i>Gap Analysis Based on the Systematic Review</i>	177
8.2.	<i>Assessment Against CMS Criteria</i>	180
8.3.	<i>Assessment Against BPCMS Features</i>	187
8.4.	<i>Tool Support</i>	190
8.5.	<i>Summary</i>	194
Chapter 9. Conclusions		195
9.1.	<i>Contributions</i>	195
9.2.	<i>Validation Outcomes and Threat Mitigation</i>	197
9.2.1	Modeling Step	198
9.2.2	Evaluation Step	199
9.2.3	Improvement Step	199
9.2.4	Monitoring Step	199
9.3.	<i>Future Work</i>	200
References		202
Appendix A: Systematic Literature Review		214
Appendix B: Human Resource Policy		221
Appendix C: URN Measured Compliance OCL Rules		226
Appendix D: Standard URN Metamodel		229

List of Figures

Figure 1, Research Method.....	7
Figure 2, Sample example for Business Rule Definition with SBVR	20
Figure 3, Summary of the GRL Notation Elements [4]	23
Figure 4, Sample GRL Model.....	24
Figure 5, Summary of the UCM Notation Elements [4]	26
Figure 6, Sample UCM with a Plug-in.....	27
Figure 7, jUCMNav Views.....	28
Figure 8, Literature Review Research Method	36
Figure 9, Distribution of Articles by Subject.....	39
Figure 10, Distribution of Articles by Year.....	40
Figure 11, Distribution of Articles by Region	40
Figure 12, Analysis of Papers Based on Groupings.....	42
Figure 13, Compliance Management System (CMS) Properties.....	44
Figure 14, Framework Inputs and Outputs	53
Figure 15, Method Steps.....	54
Figure 16, Elements of the Framework	55
Figure 17, Regulations Structure Metamodel	59
Figure 18, Object Diagram for a Subset of the Guideline Example (Aeronautics Acts) ..	61
Figure 19, Regulation Modeling, Step 3	63
Figure 20, Regulation Modeling, Step 8	66
Figure 21, Regulation Modeling, Step 9	67
Figure 22, Regulation Modeling, Step 10.....	68
Figure 23, Regulation Modeling, Step 13.....	69
Figure 24, Mapping regulation metamodel to GRL model elements.....	70
Figure 25, Extracting GRL models from legal documents, sample example	72
Figure 26, Optimized Sample Example.....	73
Figure 27, Importance Value Propagation.....	75
Figure 28, Rules Quadrant Diagram	76
Figure 29, Hiring Process	80
Figure 30, Confirm Job Sub-Process.....	80
Figure 31, Interview Internal Candidates Sub-Process (As-Is)	81
Figure 32, Business High-level Goal Model	82
Figure 33, Employees' Business Goal Model, with Impact on Business Goals.....	83
Figure 34, Hiring Manager's Business Goal Model, with Impact on Business Goals.....	84
Figure 35, HR Manager's Business Goal Model, with Impact on Business Goals	85
Figure 36, Sub-policies for Human Resources (top) and Hiring (bottom).....	86
Figure 37, Rules and Key Performance Indicators for Job Posting	87
Figure 38, Rules and Key Performance Indicators for Interview	88
Figure 39, Retention Guidelines, Government of Canada.....	89

Figure 40, Initializing KPIs in jUCMNav	91
Figure 41, Policy and Rule Satisfaction Level.....	92
Figure 42, Interview Policy Satisfaction Level.....	93
Figure 43, Job Posting Policy Satisfaction Level	93
Figure 44, Importance Value Propagation from Business Goals to Rules	95
Figure 45, Importance and Compliance of Rules on a Quadrant Diagram	96
Figure 46, Employees' Satisfaction Level before Process Modification	97
Figure 47, HR Manager's Satisfaction Level before Process Modification.....	98
Figure 48, Hiring Manager's Satisfaction Level before Process Modification	99
Figure 49, Business' Satisfaction Level before Process Modification.....	100
Figure 50, Interview Internal Candidates Sub-process after Process Modification.....	102
Figure 51, Job Posting Satisfaction Level after Process Modification	105
Figure 52, Employees' Satisfaction Level after Process Modification.....	106
Figure 53, HR Manager's Satisfaction Level after Process Modification.....	107
Figure 54, Hiring Manager's Satisfaction Level after Process Modification.....	108
Figure 55, Business' Satisfaction Level after Process Modification	109
Figure 56, Restricted Area in Aerodromes	112
Figure 57, Sign Inspection Business Process (As-Is).....	114
Figure 58, Report on Non-Compliance Areas Sub-Process (As-Is)	114
Figure 59, Improve Non-Compliance Areas Sub-Process (As-Is).....	114
Figure 60, Sign Installation Business Process (As-Is)	115
Figure 61, Write Sign Proposal Sub-Process (As-Is).....	116
Figure 62, Sign Checklist Sub-Process	116
Figure 63, Business High-level Goal Model for Aerodrome Security.....	117
Figure 64, Compliance Department's Business Goal Model, with Impact on Business Goals.....	119
Figure 65, Aerodrome Operator's Business Goal Model, with Impact on Business Goals.....	120
Figure 66, Finance Department's Business Goal Model, with Impact on Business Goals.....	121
Figure 67, Sign Policy	122
Figure 68, Sample Metadata Used to Navigate to Regulation Source Documents.....	123
Figure 69, Initializing Signs KPIs in jUCMNav for Sign Example.....	124
Figure 70, Sign Regulation Satisfaction Level (Before Modification)	125
Figure 71, Importance and Compliance of Sign Rules on a Quadrant Diagram	127
Figure 72, Compliance Department's Satisfaction Level before Process Modification .	128
Figure 73, Aerodrome Operator's Satisfaction Level before Process Modification.....	129
Figure 74, Finance Department's Satisfaction Level before Process Modification	130
Figure 75, Business's Satisfaction Level before Process Modification	130
Figure 76, Sign Inspection Table Design in Database Server (Microsoft SQL)	133
Figure 77, Report on Non-Compliance Areas Sub-Process (To-Be).....	134
Figure 78, Sign Inspection Business Process (To-Be)	134
Figure 79, R1 KPI Value (As-Is Process).....	135
Figure 80, R2 KPI Value (As-Is Process).....	135
Figure 81, R3 KPI Value (As-Is Process).....	136
Figure 82, R4 KPI Value (As-Is Process).....	136

Figure 83, Sign Dashboard	137
Figure 84, Sign Installation Business Process (To-Be).....	138
Figure 85, Write Sign Proposal Sub-Process (To-Be)	139
Figure 86, Sign Regulation Satisfaction Level (After Modification).....	141
Figure 87, Compliance Department's Satisfaction Level after Process Modification- Strategy 1	142
Figure 88, Aerodrome Operator's Satisfaction Level after Process Modification- Strategy 1	143
Figure 89, Finance Department's Satisfaction Level after Process Modification- Strategy 1	144
Figure 90, Business's Satisfaction Level after Process Modification- Strategy 1	144
Figure 91, Base Strategy.....	149
Figure 92, Difference: Base Strategy- After Process Modification Strategy 1	150
Figure 93, Difference: Base Strategy- After Process Modification Strategy 2	151
Figure 94, Difference: Base Strategy- After Process Modification Strategy 3	152
Figure 95, Goal Model of a Perimeter Security Regulation	155
Figure 96, Sample of Condition on a Rule	156
Figure 97, Generic Model from Scenario TYPE1 (Artificial Example)	158
Figure 98, Conceptual Model for the GRL Profile for Goal Model Families	161
Figure 99, Example of Conventional GRL Quantitative Analysis	163
Figure 100, Example of Modified GRL Analysis Algorithm.....	164
Figure 101, Example of TYPE1 Aerodrome with the Modified GRL Analysis Algorithm.....	165
Figure 102, GetStrategyStereotypes Algorithm.....	167
Figure 103, CheckIgnoredElement Algorithm	168
Figure 104, CalculateEvaluation Algorithm.....	169
Figure 105, CheckConditions Algorithm	170
Figure 106, CalculateContribution Algorithm.....	172
Figure 107, Example of Violations of the Profile's OCL Rules in jUCMNav	174
Figure 108, OCL Compliance Rule.....	182
Figure 109, Policy Model	184
Figure 110, Tasks Required Enforcing Compliance for Sign Installation	184
Figure 111, Tasks Required Enforcing Compliance Write Sign Proposal.....	185
Figure 112, Evaluation of TYPE1 with the New Propagation Algorithm	192
Figure 113, Evaluation of TYPE1/TYPE2 with the New Propagation Algorithm.....	193
Figure 114, Evaluation of TYPE1/TYPE2 Strategies when Condition1 is 0	193
Figure 115, URN Specification, Links, Metadata and Model Elements [57].....	229
Figure 116, GRL Specification [57].....	230
Figure 117, GRL Model, Linkable, and Containable elements [57].....	231
Figure 118, GRL Actors, Intentional elements, and Links [57]	231

List of Tables

Table 1, Survey Result of Governance, Risk and Compliance	14
Table 2, Some Federal Laws for HRM Practices [53]	16
Table 3, Automatic and Manual Search Results	37
Table 4, Selected Papers and Criteria.....	38
Table 5, Contributions and Locations	41
Table 6, Regulation Modeling, Step 1.....	61
Table 7, Regulation Modeling, Step 2.....	62
Table 8, Regulation Modeling, Step 4.....	64
Table 9, Regulation Modeling, Step 5.....	64
Table 10, Regulation Modeling, Step 6.....	65
Table 11, Regulation Modeling, Step 7.....	65
Table 12, Job Posting Rules and KPIs	87
Table 13, Mapping between Business Processes and Job Posting Rules	87
Table 14, Interview Rules and KPIs.....	88
Table 15, Mapping between Business Processes and Interview Rules	88
Table 16, Mapping between Business Processes and Retention Guidelines Rules	89
Table 17, List of KPIs and Value Sets for Rules	91
Table 18, Satisfaction Level of Actors before Process Modification	99
Table 19, KPIs Values for Employees, HR Manager and Hiring Manager before Process Modification	100
Table 20, Priority between Rules	101
Table 21, Prioritization List	102
Table 22, Conflicts between R7 and R9	103
Table 23, KPIs Values for Employees, HR Manager and Hiring Manager after Process Modification	106
Table 24, Comparison between Stakeholders' Satisfaction Levels	109
Table 25, Sign Regulations and KPIs.....	123
Table 26, Mapping between Business Processes and Sign Regulation.....	123
Table 27, List of Sign's KPIs and Value Sets for Rules before Process Modification...	125
Table 28, Satisfaction Level of Aerodrome Security Actors before Process Modification.....	131
Table 29, KPIs Values for Aerodrome Security Actors before Process Modification ...	131
Table 30, Priority between Sign Rules	132
Table 31, Sign Rules Prioritization List	132
Table 32, Sign Inspection Questionnaire.....	133
Table 33, KPIs Values for Aerodrome Security Actors after Process Modification- Strategy 1	141
Table 34, Comparison between Satisfaction Level of Aerodrome Security Actors before and after Process Modification- Strategy 1	145

Table 35, KPIs Values for Aerodrome Security Actors after Process Modification- Strategy 2	146
Table 36, Satisfaction Level of Intentional Elements for Strategies 1, 2, and 3.....	146
Table 37, Comparison between Satisfaction Level of Aerodrome Security Actors before and after Process Modification- Strategy 2.....	146
Table 38, KPIs Values for Aerodrome Security Actors after Process Modification- Strategy 3	147
Table 39, Comparison between Satisfaction Level of Aerodrome Security Actors before and after Process Modification- Strategy 3.....	147
Table 40, Comparison between Satisfaction Level of Aerodrome Security Actors before and after Process Modification- All Strategies	152
Table 41, Mapping between Aerodrome Categories and Regulations.....	157
Table 42, Measured Compliance Profile Metadata/Stereotypes	166
Table 43, Comparison between IPCF and other Related Frameworks	178
Table 44, Compliance Management Framework Properties, with Assessment of IPCF	187
Table 45, Assessment of IPCF against Common BPCMS Features	190
Table 46, Papers Selected from IEEE Explorer.....	215
Table 47, Papers Selected from Springer	216
Table 48, Papers Selected from Google Scholar.....	217
Table 49, Papers Selected from ACM.....	218
Table 50, Papers Selected from iSTAR.....	219
Table 51, Papers Selected from GRCIS	219
Table 52, Selected Papers' Locations, Regions and Years.....	220

List of Acronyms

Acronym	Definition
BI	Business Intelligence
BIN	Business Intelligence Network
BPC	Business Process Compliance
BPCMS	Business Process Compliance Management System
BPM	Business Process Management
BPMN	Business Process Modeling Notation
CGD	Compliance Governance Dashboard
CMM	Capability Maturity Model
CMS	Compliance Management System
COBIT	Control Objectives for Information and Related Technology
EMF	Eclipse Modeling Framework
EPMD	Engineering & Project Management Division
FCL	Formal Contract Language
GEF	Graphical Editing Framework
GQM	Goal Question Metric
GRL	Goal-oriented Requirement Language
GRCIS	Governance Risk Compliance Information System
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resource
HRM	Human Resource Management
IBA	Illinois Banker Association
IPCF	Indicator-based Policy Compliance Framework
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU-T	International Telecommunication Union - Telecommunication
KPI	Key Performance Indicator
NFR	Non-Functional Requirement
OCEG	Open Compliance and Ethics Group
OCL	Object Constraint Language
OECD	Organisation for Economic Co-operation and Development
PHIPA	Personal Health Information Privacy Act
PSM	Practical Software Measurement
SAS	Statistical Analysis System
SBVR	Semantics of Business Vocabulary and Business Rules
SOX	Sarbanes-Oxley Act
UCM	Use Case Map
URN	User Requirements Notation

Chapter 1. Introduction

This thesis intends to develop an Indicator-based Policy Compliance Framework that exploits goal, process, and indicator modeling and analysis to support organizations in managing the compliance of business processes with policies, rules, regulations, and laws.

This introduction chapter summarizes basic concepts required to understand the thesis, the problem statement, the motivation, as well as the objectives for this research. Furthermore, the research methodology and lists of existing contributions and publications based on this research are discussed. Finally, the content of this document is outlined.

1.1. Concepts

This section briefly explains some of the concepts required to understand this research.

Business Process Management (BPM): BPM is a comprehensive system whose goal is to transfer and manage an organization's operations derived from set of ideas about dealing with organization performance [49]. In another definition by van der Aalst *et al.* [133] "Business Process Management (BPM) includes methods, techniques, and tools to support the design, enactment, management, and analysis of operational business processes".

Business Intelligence (BI): Business intelligence is used to analyze business data and help organizations to better understand their business and make better decisions. BI technologies help decision makers determine how a business is doing. Common functions of business intelligence technologies are query and reporting, data mining, business process performance, and online analytical processing [138]. In another definition by Negash *et al.* [91] "We define business intelligence (BI) as systems that combine data gathering, data storage, and knowledge management with analysis to evaluate complex corporate

and competitive information for presentation to planners and decision makers, with the objective of improving the timeliness and the quality of the input to the decision process”.

Compliance: Compliance is about acting according to certain accepted standards. In addition, as indicated by Dang *et al.* [32], compliance is the act or process of complying with a demand or recommendation. In another definition by Foorthuis *et al.* [37], compliance is “a state of accordance between an actor’s behavior or products on the one hand, and predefined explicit rules, guidelines, legislation or other norms on the other hand”. In yet another definition by Zdun *et al.* [142], “the term compliance addresses the external regulations, internal policies, standards, and governance to which an organization must adhere”.

Businesses Process Compliance: Refers to a set of technologies and methodologies helping processes and systems comply with policies and legal requirements.

Measure: Defined by the Glossary of Software Engineering Terminology as providing “a quantitative indication of the extent, amount, dimensions, capacity or size of some attribute of a product or process” [56]. Another definition by smartKPIs.com [125] suggests: “A number or a quantity that records a directly observable value or performance. All measures are composed of a number and a unit of measure. The number provides magnitude (how much) for the measure, while the unit gives number a meaning (what). Examples of unit measures are: dollars, hours, meters, inches, etc.”. For example, 10 applicants per year is a specific measure.

Metrics: Defined by the Glossary of Software Engineering Terminology as “A quantitative measure of the degree to which a system, component, or process possesses a given attribute” [56]. In another definition by smartKPIs.com [125]: “A generic term encompassing the quantitative basis by which objectives are established and performance is assessed. It helps quantify the achievement of a result, the quantifiable component of an organization’s performance. In the context of measuring and managing performance these terms are used interchangeably”. For example, the Number of applicants per year is a specific metric.

Indicator: “A variable with characteristics of quality, quantity, and time used to measure, directly or indirectly, changes in a situation and to appreciate the progress made in addressing it. It also provides a basis for developing adequate plans for improvement” [139]. Indicators are defined in many ways but the common sense for all of them is that they refer to specific information. For example, the Organisation for Economic Co-operation and Development (OECD) defines an indicator as “a qualitative or quantitative factor or variable that provides a simple and reliable means to measure achievement, to reflect changes connected to an intervention, or to help assess the performance of a development actor”. For example, the Number of applicants per year, where the target is at least 50 is an indicator.

Key Performance Indicators (KPI): Key performance indicators are quantifiable measures that organizations usually use to calculate *important* aspects of the business [71]. A KPI is an indicator commonly used to calculate if a company meets its strategic and operational goals. In another definition by smartKPIS.com [125]: “A selected indicator considered key for monitoring the performance of a strategic objective, outcome, or key result area important to the success of an activity and growth of the organization overall. KPIs make objectives quantifiable, providing visibility into the performance of individuals, teams, departments and organizations and enabling decision makers to take action in achieving the desired outcomes. Typically, KPIs are monitored and distributed in dashboards, scorecards and other forms of performance reports”.

Law: A law is a rule or collection of rules prescribed under the authority of the state or nation. In Canada, laws must be approved by the provinces, or at the federal level through the House of Commons, the Senate, and the Royal Assent given by the Governor General. “A law is considered to be an act when it has already been duly passed by a legislative body. This legislative body may be statewide or nationwide” [33].

Regulation: A regulation is also a rule or collection of rules, only this time the authority can be that of a government department, not necessarily the state or nation. Regulations are often more focused, detailed, and procedural than laws. “A regulation is [one that is] approved by a group of individuals based on an act (law) that has already been passed. These regulations are based on the act that has been approved and served as

a means to make the act a lot easier to follow and adhere to. For this reason, one act can have numerous regulations” [33].

Policy: There is no single definition for what a policy is. Torjman *et al.* [131] discuss the concept of policy from a general perspective. Anderson in [9] describes that “A policy is a guiding principle used to set direction in an organization, It can be a course of action to guide and influence decisions”. Policies also “reflect the aims and objectives of the organization” [34]. However, in this thesis, policies are seen as parts of laws and regulations, or they can be defined internally in an organization that wants to give directions to its business processes.

Rule: “While policies are broad guidelines that reflect the aims and objectives of the organization, rules are meant more for day to day operations to proceed smoothly without any glitches” [34]. In this thesis, rules are so fine-grained that they can be used at the operational process level.

Note that in this thesis, the terms *indicator* and *KPI* are used interchangeably. The focus is not on trying to differentiate between indicators that are “key” and those that are not, nor is it about the distinction between indicators related to “performance” and those related to other topics such as compliance. This also reflects the language of the main industrial partner (a national regulator), as they often consider *KPI* to be equivalent to *indicator*, even in a compliance context. The terms “compliance indicators” and “key compliance indicators” are not part of their common vocabulary.

1.2. Problem Statement

Compliance with various levels of policies is a critical activity in any organization. Every year, organizations invest time and money to ensure their business processes are compliant with different policies. Policies may vary depending on an organization’s sector of activity. In addition, different legislative bodies and regulators, possibly from different jurisdictions, create regulations that contain policies. Therefore, they may conflict or overlap with each other. Compliance management becomes complex partly due to over-

whelming number of laws, regulations, standards, policies, and other types of authoritative rules introduced or modified each year. With so many rules to follow, large organizations have a difficult time keeping track of business process compliance levels and evaluating the impact on the organization goals of making these processes compliant. Different stakeholders in an organization have different and perhaps conflicting goals, which make the situation even more complicated. Furthermore, it is challenging to comply with all imposed policies given limited resources (e.g., human and financial) and conflicting rules. Hence, organizations have to pick and choose the compliance areas they want to address considering different factors. Finally, many organizations use a reactive approach to compliance and only address issues after failures in audits as opposed to taking a proactive approach to prevent such failures.

In this context, it is necessary to develop a framework that would allow organizations to address the above issues. Such a framework should help organizations answer the following questions: How can we establish simple traceability between laws, regulations, policies in general, business processes, and organization goals? How can organizations constantly monitor the level of compliance of business processes to avoid audit failures? How does making a process compliant with a particular policy impact organization goals, including goals of different stakeholders? What is the overall compliance level of the organization with respect to one or multiple policies? What if modifications to a process improved compliance with a policy while degrading compliance with other policies? How can organizations select the most important compliance issues to address given their limited resources?

1.3. Motivations and Objectives

Much work related to compliance audits of business process instances has been presented in the literature. However, modeling the intents and objectives of policies, organization goals, and key performance indicators for measuring compliance level of policies as an integrated framework has not been explored yet. A goal view with associated compliance KPIs integrated with a process view allows for reasoning about what to do next as well as

about the impact of candidate improvements on organization goals, hence providing a holistic view.

This work is motivated by the need to provide a framework that would enable organizations to:

- Discover business processes that violate regulations, laws and policies;
- Discover the importance level of business processes based on the organization's goals;
- Determine the impact of compliance-related process modifications on business goals, including conflicting goals between stakeholders, and on conflicting rules; and
- Enable organizations to measure the level of business process compliance for one or multiple policies.

The *Indicator-based Policy Compliance Framework* (IPCF) proposed in this thesis is based on the User Requirements Notation (URN) [57], the first international standard to combine goal modeling (Goal-oriented Requirement Language — GRL) with scenario modeling (Use Case Map notation — UCM). URN was created for modeling telecommunication services and reactive systems, but it was shown to be a competitive language for business process modeling [137]. In addition to being a standard notation that combines goals with business processes, URN supports strategy definition with quantitative evaluations, and it has been extended with the concept of indicator for measuring various aspects of businesses. URN was also shown to support the modeling of laws. No other language offers such a combination of features, which fit the problem at hand. In addition, jUCMNav [62], a free Eclipse-based tool, is used to analyze and manage URN models.

1.4. Research Method

This section presents the steps of this research as illustrated in Figure 1. These steps are inspired from the “Design science in information systems research” research method proposed by Henver [51].

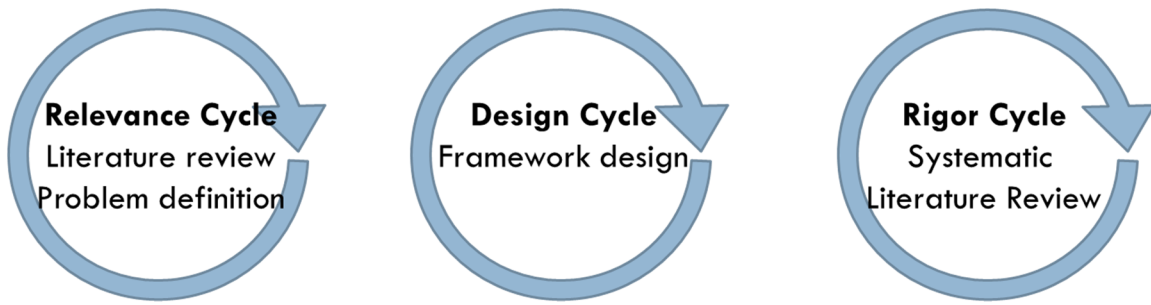


Figure 1, Research Method

The research started with an informal literature review in the relevance cycle. After understanding concepts and the current literature in the context of regulation compliance and goal modeling, the problem area was scoped, and then the research opportunity (i.e., compliance measurement) and steps were defined. In the rigor cycle, while building a knowledge base for the research, a systematic literature review was conducted to find the research papers related to this work and to make sure the research idea was novel. In the design cycle, research started by defining the first version of the framework. Subsequently, in two additional iterations, the framework was improved using two example scenarios. The first scenario involved modeling a human resource policies. Along the way, the opportunities for contributions to solve the defined problems and steps of the methodology were iteratively defined. A second scenario (aerodrome security policies and regulations) was completed to validate the revised steps of the methodology. Tool support was also developed along the way. In addition some improvements were made to the framework after comparing it against existing frameworks and evaluating it against two sets of criteria.

1.5. Thesis Contributions

The major and minor contributions of this research are listed in this section. References to chapters discussing the contributions are also provided.

1.5.1 Major Contributions

- A framework meant to help organizations measure compliance level for business processes, observe non-compliance issues and prioritize them. This framework covers the following sub-contributions (Chapter 4):
 - A unique structure for modeling the objectives of policies, organization goals, and key performance indicators for measuring compliance level of policies as an integrated framework, namely the Indicator Policy-based Compliance Framework (IPCF).
 - Guidelines for moving from document-based compliance to model-based compliance (i.e., a conceptual metamodel describing legal/policy documents and steps to derive GRL policy models).
- A GRL profile for handling compliance and goal models families (Chapter 7)
 - The profile contains suitable stereotypes, well-formedness constraints in OCL, and a novel analysis algorithm defined for GRL model families, with a particular focus on compliance, to support conditional objectives in regulations.

1.5.2 Minor Contributions

- Systematic review of compliance measurement approaches based on goals and indicators (with over thirty publications selected from four search engines and the study of specialized conferences) (Chapter 3).
- A GRL importance algorithm to help organizations select the most important compliance issues given their limited resources (Chapter 4).
- A technique to prioritize non-compliance issues (Chapter 4).
- Extension of the current jUCMNav tool to support the new GRL profile, with appropriate visualizations (Chapter 7).
- Combination of the URN-based profile and a BI tool (Chapter 6) to:
 - Obtain KPI values from the BI environment (IBM Cognos);
 - Generate interactive reports on the status of organization business process compliance for stakeholders.

1.5.3 Validation and Impact

The evaluation of IPCF (Chapter 6, and Chapter 8) was done in three ways:

- Validation of the framework with examples related to human resources and aerodrome security policies/regulations and business processes.
- A comparison between this framework and existing frameworks.
- An evaluation against different sets of criteria from the literature.

The main impact of this work on the research community is the demonstration that a framework that combines goal and scenario modeling with indicators is valuable in a context where compliance to regulations needs to be measured in order to help determine what business processes should be improved. This work has also influenced the development of new analysis and visualization features of the jUCMNav tool, which will be beneficial outside the compliance and business improvement contexts.

In terms of industrial impact, part of IPCF (mainly the modeling and evaluation steps) is already being explored by a national regulator that develops policies and regulations to make Canadian transportation safe and secure [127]. This national regulator is moving away from prescriptive-based compliance to outcome-based compliance, where goals and KPIs play an important role. Regulations need to be written in a different way, and regulated parties should have more freedom in choosing how to achieve compliance to regulations. This framework enables regulators to move towards better assessments of outcome-based regulations, and this has the potential to influence the process of creating policies and regulations, as the focus on goals and measures is now taken into account much earlier, while writing/evolving regulations, and not just as an afterthought. This will lead to regulations that are clearer and to easier compliance assessment. This framework is also attracting the attention of other regulators, in Canada and elsewhere.

1.6. Publications and Presentations Based on Thesis

All publications based on this research are listed in this section.

1. **Shamsaei, A.**, Amyot, D., Pourshahid, A., Mussbacher, G., Tawhid, R., Yu, E., Braun, E., and Cartwright, N.: “An Approach to Specify and Analyze Goal

- Model Families”. In: *7th System Analysis and Modelling (SAM)*, Innsbruck, Austria, LNCS. Springer (October 2012) (*to appear*) [120]
2. Amyot, D., **Shamsaei, A.**, Kealey, J., Tremblay, E., Miga, A., Mussbacher, G., Alhaj, M., Tawhid, R., Braun, E., and Cartwright, N.: “Towards Advanced Goal Model Analysis with jUCMNav”. In: *3rd Int. Workshop on Requirements, Intentions and Goals in Conceptual Modeling (RIGiM’12)*, Florence, Italy, LNCS 7518, Springer, pp. 201-210 (October 2012) [8]
 3. Tawhid, R., Alhaj, M., Mussbacher, G., Braun, E., Cartwright, N., **Shamsaei, A.**, Amyot, D., Behnam, S.A., and Richards, G.: “Towards Outcome-Based Regulatory Compliance in Aviation Security”. In: *20th IEEE Int. Requirements Engineering Conference (RE’12)*, Chicago, USA. IEEE CS, pp. 267-272 (September 2012) [127]
 4. Braun, E., Cartwright, N., **Shamsaei, A.**, Behnam, S.A., Richards, G., Alhaj, M., and Mussbacher, G.: “Drafting and Modeling of Regulations: Is It Being Done Backward”. In: *5th Requirements Engineering and Law (RELAW 2012)*, Chicago, USA. IEEE CS, pp. 1-6 (September 2012) [21]
 5. **Shamsaei, A.**, Amyot, D., and Pourshahid, A.: “A Systematic Review of Compliance Measurement Based on Goals and Indicators”. In: *Governance, Risk and Compliance on Information Systems (GRCIS’11)*, London, UK, Springer, LNBIP, Vol. 83, pp. 228-236 (June 2011) [119]
 6. **Shamsaei, A.**: “Indicator-based Policy Compliance of Business Processes”. In: *CAiSE’11 Doctoral Consortium*, London, UK, CEUR-WS, Vol. 731 (June 2011) [121]
 7. **Shamsaei, A.**, Pourshahid, A., and Amyot, D.: “Business Process Compliance Tracking Using Key Performance Indicators”. In: *Business Process Design (BPD 2010)*, Hoboken, NJ, USA, Springer, LNBIP, Vol. 66, pp. 73-8 (September 2010) [118]
 8. **Shamsaei, A.**: “Business Process Compliance Tracking Using Key Performance Indicators”. *CASCON 2010*, Poster, Toronto, Canada (November 2010) [122]

1.7. Thesis Outline

This research is structured in eight additional chapters. Chapter 2 elaborates on background and domain knowledge required to understand this thesis. Chapter 3 presents the result of the systematic literature review. The Indicator-based Policy Compliance Framework is introduced in Chapter 4, together with a discussion of the method steps, inputs and outputs. A test scenario from the human resource domain is elaborated in Chapter 5 to illustrate the method and its benefits. In Chapter 6, real-life scenarios related to aviation security policies (including BI portals) are used to validate the proposed methodology. In chapter 7, the new profile for GRL, with suitable stereotypes, well-formedness constraints, and a modified analysis algorithm defined for GRL model families is formalized. Chapter 8 provides further evaluation by comparing IPCF to related work, assessing it against existing criteria for compliance management systems, and by reviewing tool support. Finally, conclusions and future work are discussed in Chapter 9.

Chapter 2. Background

This chapter reviews some of the background and domain knowledge required for the reader to better understand the technical parts of this thesis. The chapter starts with an overview of the results of some surveys on the cost of business process compliance and regulations violation in section 2.1. Section 2.2 then continues by describing different categories of *authoritative rules* that govern business processes. Section 2.3 explains common performance and quality metric development methodologies. Section 2.4 presents work related to the Semantic of Business Vocabulary and Business Rules (SBVR). Section 2.5 describes the User Requirements Notation (URN), while sections 2.6 and 2.7 briefly describe related work on the use of URN for business processes compliance and Key Performance Indicators (KPIs). An overview of work related to goal model families is presented in section 2.8. Finally, section 2.9 discusses Business Intelligence (BI) as a supporting tool used as an input to compute the indicators required by URN models and as an output for reporting to stakeholders.

2.1. Reports on Compliance

Companies invest much financial resources to make their business processes compliant with regulations. The following surveys and statistics show the importance of compliance for companies as well as the value of any tool that can help companies reduce their costs.

According to a 2010 survey by the Illinois Banker Association [55], among the 128 banks who responded, over 54% spend 5% of their annual operating expenses on compliance and internal audits. Over 40% of these banks spend between 5% and 20% on compliance, while over 4% spend more than 20% on compliance.

According to another survey in 2003 [70], 47% of hospitals with a number of beds greater than 400 spend between \$100,000 and \$500,000 on HIPAA (Health Insur-

ance Portability and Accountability Act) compliance while about 20% of these hospitals spend more than \$1,000,000.

The cost of a HIPAA violation [101] with wrongful disclosure for an individual can be up to 50,000\$, or one year in prison, or both. The fine can go up to 100,000\$ or five years in prison when the violation is done under false pretences. Many hospitals may consider non-compliance as a cost-saving option. However, HIPAA compliance is not just about penalties, as compliance can also help hospitals create and improve the health care system.

According to another survey by Financial Executives International (FEI) [30] done in 2007, based on 168 companies with a market capitalization above \$75 million, the total average cost for section 404 of SOX (Sarbanes–Oxley Act) compliance was \$1.7 million during the 2007 fiscal year. The SOX violation penalties differ depending on the SOX section [143]. Penalties can be up to \$1,000,000 or up to 20 years of prison.

A different survey from the IT Policy Compliance Group [60], published in 2007, reports that while “the amount spent on compliance and data protection is a very small percentage of the financial value that is at risk”, nearly 90% of business do not meet data-handling regulations properly, with as a consequence an increased risk of data breach.

According to a 2011 survey by Thomson Reuter [130], 71% of the 337 global compliance professionals who responded to the survey said that “they foresaw that an increase in time and resource would be required to work with regulators and exchanges to ensure they were adequately prepared to meet regulatory requirements”. Another report published in March 2011 [112] highlights the impact of ongoing regulation on companies, as well as the lack of effective and efficient way to deal with governance, risk and compliance. That report presents the results of a survey conducted among more than two thousands compliance officers and senior governance professionals. Table 1 lists some of the survey questions and responses.

Hence, to avoid undesirable non-compliance consequences, it is critical to implement business processes that are compliant with regulations and policies. Furthermore, to help organizations reduce their costs, it is important to build the right tools and methodologies for them to achieve their compliance goals more easily.

Questions	Strongly Agree	Agree	Disagree	Strongly Disagree
Amending policies and procedures to comply with the latest regulatory changes takes up too many staff hours and is too costly.	18%	48%	32%	2%
Keeping up to speed with the ever-changing rules, which govern my industry, is increasingly challenging. In fact, it is getting more difficult.	44%	48%	7%	1%
Regulators do not spend enough time finding out how to regulate effectively. They should talk to a broader range of people about how to make regulation efficient and effective.	36%	51%	12%	1%

Table 1, Survey Result of Governance, Risk and Compliance

2.2. Authoritative Rules

A business process can be governed by four categories of *authoritative rules* [50]. The following subsections review each of these categories.

2.2.1 Regulations and Laws

The first category is regulations and laws that are imposed by governments. Regulations are divided in to a number of policies, and each policy consists of rules [65][124]. Violating rules from this category can cause important consequences, including financial penalties, loss of reputation, lawsuits, and even imprisonment. Examples of typical regulations include:

- *Personal Health Information Protection Act* (PHIPA) [47], which describes health custodian responsibilities in terms of collecting, using, and disclosing Personal Health Information (PHI) in Ontario, Canada.
- *Health Insurance Portability and Accountability Act* (HIPAA) [132], in the USA, which has two titles. Title I intends to provide health insurance for people who lose or change jobs. Title II defines the requirements “for the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers” [132].

- *Sarbanes-Oxley Act* (SOX) [129], also known as the Public Company Accounting Reform and Investor Protection Act, which describes specific mandates and requirements for financial reporting in the USA.
- *Basel II* [13], which describes international standards for banking and finance that bank regulators can use. It was first published in June 2004.
- *Gramm-Leach-Bliley Act* (GLBA), which as the Financial Services Modernization Act of 1999 “provides limited privacy protections against the sale of the private financial information” [128].

2.2.2 Policies

The second category of authoritative rules is the policies that give direction to business processes in organizations (e.g., Human Resource Policy). In this thesis, policies are seen as parts of laws and regulations, or they can be defined internally in an organization.

Policies are usually divided into a number of sub-policies. Furthermore, sub-policies can be decomposed into operational rules. For instance, an HR Policy is divided into sub-policies like Hiring Policy and Job Posting, and the latter can further be divided into two sub-policies such as Internal Job Posting and External Job Posting. Ultimately, this leads to rules that are so fine-grained that they can be used at the operational process level.

In addition, policies can also help organizations be compliant with different laws and regulations. For instance, there are three areas of legal concern that human resource management (HRM) must comply with [53]: equal opportunity, affirmative action, and sexual harassment. Internal human resource policies and rules are usually written considering these legal concerns and are considered as an internal control. As illustrated in Table 2 several other laws in the USA impact staffing in an organization.

Law	Date	Description
Age Discrimination in Employment Act	1967, amended in 1978 and 1986	Prohibits age discrimination against employees between 40 and 65 years of age and restricts mandatory retirement.
Occupational Safety and Health Act	1970	Establishes mandatory safety and health standards in organizations
Mandatory Retirement Act	1978	Prohibits the forced retirement of most employees before the age of 70.
Family and Medical Leave Act	1993	Permits employees in organizations with 50 or more workers to take up to 12 weeks of unpaid leave for family or medical reasons for each year.

Table 2, Some Federal Laws for HRM Practices [53]

2.2.3 Service Level Agreement (SLA)

The third category is Service Level Agreements (SLA), used to assure compliance of services between companies or between companies. For instance, a service level agreement for internet access and hosting services between the Allstream company and its customers is listed in [3]. This document contains service level principles, which Allstream shall provide to the customers. The following example illustrates what is typically included in such SLA. “This SLA is only applicable to those Customer Sites and Dial Access POPs within Canada where applicable Allstream service and technology exist and where Allstream is permitted by law, to provide service” [3]. The SLA also includes services covered by this agreement (e.g., ISDN Internet Access, ASDL internet Access). In addition, all excluded items are listed in this agreement, for example “The failure of Customer premise equipment (including but not limited to routers and integrated modems) not supplied by Allstream as part of the service” [3].

2.2.4 Standards

These authoritative rules guide organizations on how to deal with governance, risks, and controls. In addition, some standards attempt to define procedures that can help organizations comply with policies. Some examples of standards are:

- ITIL (*Information Technology Infrastructure Library*) [59], developed by the British government, which defines best practice processes for IT service management.
- COBIT (*Control Objectives for Information and Related Technology*) [28], used to measure ITIL, which addresses what needs to be controlled and how to measure the success of those controls.

2.3. Methodologies to Extract Metrics/Indicators

This thesis' framework uses indicators as one of its main inputs in order to measure the compliance level of organizations. This thesis does not propose a new way of discovering valid indicators; one assumption is that indicators are provided as input. However, since indicator development is a challenging task and since there already exist many frameworks to help identifying metrics (and hence indicators), this section elaborates on common methodologies to extract metrics/indicators.

Metrics provide a mechanism for assessing the state of an entity or process. However, the identification of the metrics is not simple, since there are too many metrics that can be generally identified [102]. The software industry has developed many frameworks to help identifying a minimum number of metrics that organizations need to assess their entities and processes. Examples of such frameworks are the Goal Question Metric (GQM) approach [14], Practical Software and Systems Measurement (PSM) [26], and the Software Metrics a Rigorous and Practical Approach [36]. Each of these frameworks is briefly reviewed in the following subsections based on the recent literature review of Villar [135].

2.3.1 Goal Question Metric (GQM)

Basili *et al.* [15] created the Goal Question Metric (GQM) approach, which defines a measurement model over three levels based on a top-down hierarchical structure. At the conceptual level (goals), a set of measurement goals is developed. Each GQM goal statement contains five facets, including the object (product or process under study), purpose (motivation behind the goal), focus (the quality attribute of the object), environment

(context and scope) and viewpoint. At the operational level (questions), a set of questions is defined to clarify measurement goals. At the quantitative level (metrics/indicators), a set of measurable metrics is associated to each question. The same indicator can actually partially answer more than one question. This approach can be described as a six-step framework [14][15]:

1. Develop a set of business goals and their related measurement goals;
2. Generate quantifiable questions that define the developed goals;
3. Identify metrics that can better answer the questions;
4. Develop a mechanism for data collection;
5. Gather, validate and analyze the collected data for decision-making; and
6. Analyze data to assess whether a goal is addressed or not;

The main benefit of this approach is the achievement of measurement goals, however, there are some weaknesses reported for this approach. One of the major drawbacks is the possibility of identifying more metrics than is possible to collect and analyze. Berender *et al.* [18] propose an extension of the GQM approach to solve this problem by using prioritization tools for limiting the number of metrics. Another issue that reported by Kurian [72] is that the steps of this approach are not iterative. This means that goals and questions are supposed to be added at once. In other words, no goal or question can be added along the way. Villar addresses such issues in an adaptation of the GQM approach to healthcare [135].

2.3.2 Practical Software and Systems Measurement (PSM)

The Practical Software and Systems Measurement approach focuses on satisfying the information needs for project management purposes. PSM, sponsored by the Department of Defense and the US Army, provides a systematic method for software measurement. It is increasingly accepted in industry around the world. PSM defines two key concepts, the measurement information model and the measurement process model. The former defines the basic terminology for measurement concepts; it also defines the relationships between information needs and measurable entities [26]. The measurement process model provides guidelines for measurement activity and task execution. This model consists of four activities: Establish and Sustain Commitment (concerned with establishing required sup-

port from management at various levels), Plan Measurement (concerned with understanding the information needs for the project and defining suitable measures), Perform Measurement (concerned with executing the information model and producing the result), and Evaluate Measurement (concerned with evaluating the measurement process) [26].

One of the shortcomings of PSM is that “PSM does not define all measurement procedures such as those needed to address project-specific information needs, different software domains or individual system technologies” [100].

2.3.3 Software Metrics - A Rigorous and Practical Approach

Fenton and Pfleeger [36] created the Software Metrics a Rigorous and Practical Approach. This approach combines GQM with the Capability Maturity Model (CMM) in order to address some of GQM’s issues (i.e., identifying more metrics than are possible). CMM gives information on the availability of metrics based on the project’s state. This approach can be described as a six-step framework:

1. Identify a set of entities and their attributes;
2. Identify a set of measurement goals;
3. Generate quantifiable questions that define the developed goals;
4. Identify metrics that can better answer the questions. This is achieved by measuring the attribute of one or more entities. If no attribute is available for an entity, it is not possible to conclude that the project is feasible and can provide necessary information for measurement. Therefore, the next step is taken into account to solve this issue;
5. The process maturity level discloses what metrics are available for measurement at certain time; and
6. Finally, validate the metrics.

One of the shortcomings of this approach is that it focuses on processes and not really on people [11].

2.4. Semantics of Business Vocabulary and Business Rules

Semantics of Business Vocabulary and Business Rules (SBVR) [95] is a standard developed by the Open Management Group (OMG) in 2005. It intends to provide a format that enables business people to define and formalize business vocabularies and business rules. SBVR defines a base business vocabulary that includes terms (designation for a noun concept), names (instance of a particular term), fact types (an association between two or more terms), and keywords (quantification, logical and modal operation) that can be used to create business rule. How to create a business rule with SBVR is illustrated in Figure 2. This example, extracted from the SBVR specification document, is concerned with a car rental company [95].

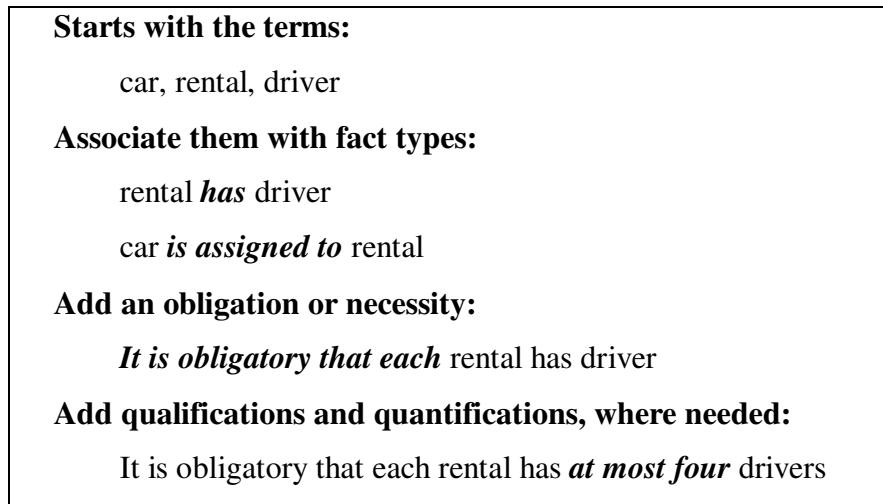


Figure 2, Sample example for Business Rule Definition with SBVR

According to the SBVR standard, there are two types of rule statements: structural rules, which define rules about how the business chooses to organize the things it deals with, and operational rules that conduct business activity which can be directly violated by the people involved [95].

However, in this thesis, rules and policies are extracted at a higher level of granularity compared to what is done with SBVR. The rules are extracted from regulation documents and the same wording is used to reflect the rules. That is, we are not formalizing the content of the rules themselves, as we focus mainly on the structure of regulations and ways of measuring whether a rule is complied with or not. According to informal feed-

back gathered from some regulators, the latter would prefer to see the exact wording of the regulation in the model rather than having it translated to another language (e.g., based on SBVR). In addition, as will be discussed later in section 4.2.2, the procedure for mapping regulations to GRL models is discussed. In order to avoid yet another conversion between regulation/policy documents and SBVR, and then an additional mapping from SBVR to GRL, we chose not to use SBVR altogether.

2.5. User Requirements Notation

The User Requirements Notation (URN) is the first international standard (ITU-T Recommendation Z.151 [57]) that combines goal-oriented modeling and scenario modeling. URN supports the elicitation, analysis and validation of requirements at early stages. URN can be used for describing reactive and distributed systems. In addition, it can also be used to describe business processes [137]. URN enables requirement engineers to discover requirements for a system and review them for completeness and correctness [4]. This notation has been used in the past in the domain of compliance [41] (see section 2.6) and to measure the satisfaction level of goals and the performance of business processes [106] (see section 2.7).

URN combines two complementary modeling languages: the Goal-oriented Requirement Language (GRL) and the Use Case Map (UCM) notation. *URN links*, indicated by small triangles (►), can link any two URN model elements. Through URN links, traceability can be established between GRL model elements and UCM model elements. GRL models objectives, non-functional requirements and alternatives. It answers the *why*, *what*, and *who* questions about a process. On the other hand, UCM models functional/operational requirements and focuses on alternative architectures. It answers *what*, *where*, *when* and *who* questions about a process.

URN is defined formally in the standard using a metamodel. A subset of the URN metamodel is presented in Appendix D, for reference.

2.5.1 Goal-oriented Requirement Language

The Goal-oriented Requirement Language (GRL) is a graphical goal modeling language rooted in the NFR (Non-Functional Requirements) and i^* frameworks [140]. GRL combines components of i^* , such as actors, intentional elements and links, with evaluation mechanisms inspired from the NFR framework. GRL connects requirements to business objectives. In addition, it helps capture stakeholder goals, non-functional requirements, and alternatives means of achieving stakeholder goals. Some of the main advantages of GRL over other goal notations are that it is combined with the UCM scenario modeling language and it supports qualitative and quantitative modeling analysis, including solution comparison. In addition, GRL supports multiple diagrams based on one model, which helps reduce the complexity of diagrams and reuse elements consistently in multiple diagrams.

GRL consists of three main concepts: intentional elements (softgoal, goal, task, resource, and belief), intentional links (contribution, correlation, and decomposition/means-end), and actors. In the performance extension of the standard GRL used in this thesis [105], a new intentional element called *indicator* (or KPI) is also included. The notation elements are summarized in Figure 3.

In GRL, a *softgoal* is an intention or quality that cannot be fully achieved (e.g., Be Secure), whereas a *goal* can be fully satisfied. *Tasks* represent activities or solutions used to meet softgoals or goals. Intentional elements can be connected to each other using *contribution links* with different *contribution types* that can be qualitative (*make*, *help*, *some+*, *break*, *hurt* and *some-*) or quantitative (an integer number between -100 and $+100$). Contribution links of type *make*, *help* and *some+* all have a positive contribution whereas *break*, *hurt* and *some-*, all have a negative contribution. Some goals do not have direct contribution to others but they can have positive or negative side-effects shown using correlation links (also with contribution types). *Decomposition* links can be used to connect elements and sub elements using AND, OR and XOR decomposition relationships. Intentional elements can be assigned to stakeholders shown as *actors*. *Dependency links* can be used to show that an actor depends on another actor to meet a goal, satisfy a softgoal, perform a task, provide a resource, etc.

Finally, a *GRL strategy* describes a particular configuration of alternatives and initial satisfaction values in the GRL model, while a *GRL evaluation mechanism* propagates this information to the other intentional elements of the model (through their links) and compute their satisfaction values. The evaluation values can be provided manually (as part of a strategy definition) or automatically obtained from a data source such as a Business Intelligence system. In addition, GRL supports an *importance* attribute for intentional elements, which is used to compute the overall satisfaction level of their actor. Different bottom-up evaluation algorithms exist for GRL, including qualitative, quantitative, and hybrid propagations [6].

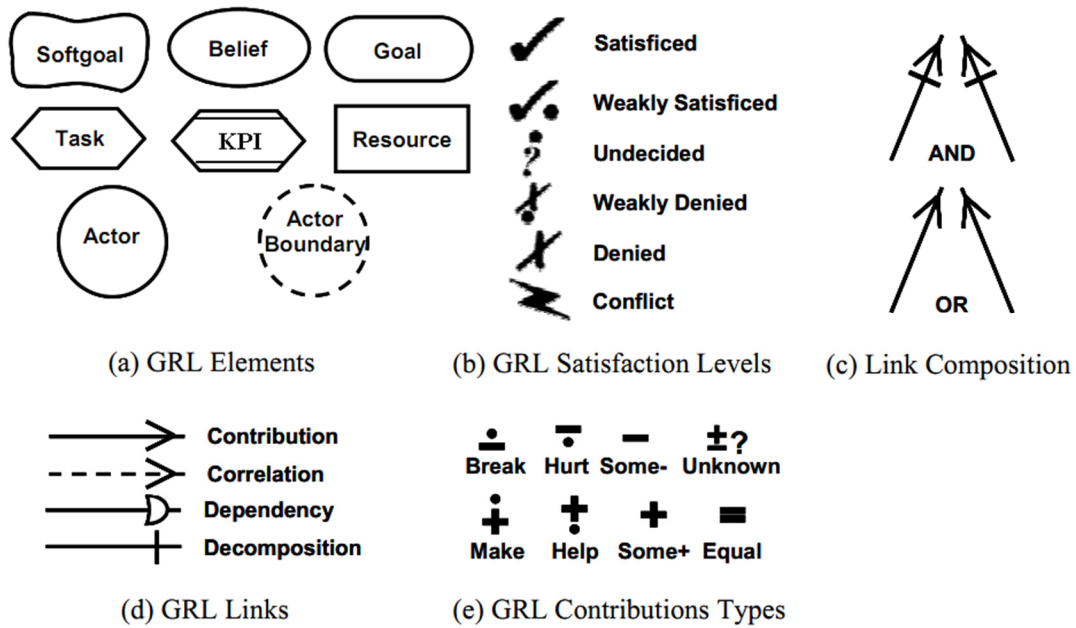


Figure 3, Summary of the GRL Notation Elements [4]

Figure 4 illustrates a GRL model with quantitative evaluation results for the HR Manager. This model consists of five KPIs and seven softgoals, some of the latter with non-null importance factors shown between parentheses. One of the softgoals (Improve compensation packages) is AND-decomposed into three sub-softgoals and the sub-softgoals are fed by KPIs. The KPIs values are entered manually as part of strategy definition and initial evaluation values are mapped to satisfaction levels using a tool-supported GRL evaluation algorithm (quantitative bottom-up propagation). The rest of the model is evaluated based on these values.

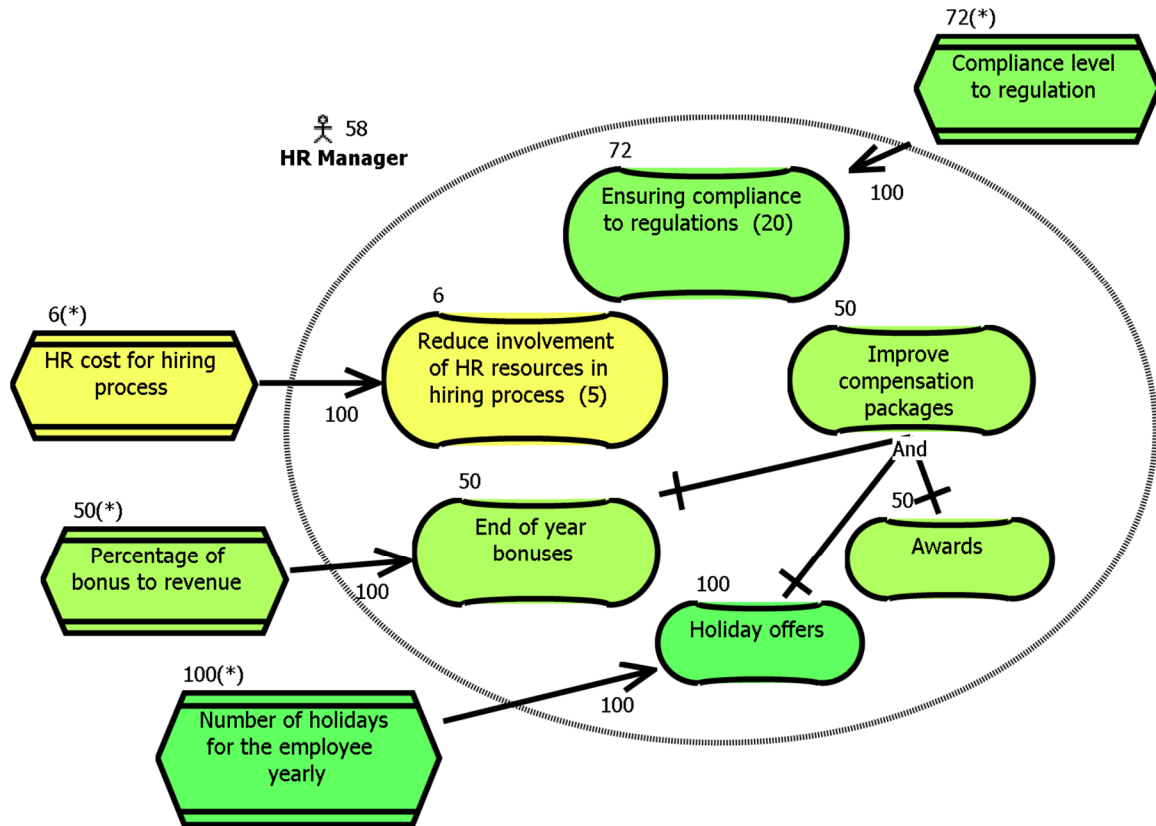


Figure 4, Sample GRL Model

There are other goal modeling notations, such as i^* , NFR, TROPOS, KAOS. However, GRL was selected as the goal modeling language in this thesis because of its several advantages over other popular goal modeling languages [5]:

- i) GRL is standardized as part of the User Requirements Notation (URN) [7][57];
- ii) GRL is combined with a business process notation (UCM) as part of URN;
- iii) GRL supports the concept of Key Performance Indicator (KPI) [105], useful to measure compliance in units that people doing inspection/audit activities can actually understand;
- iv) it is possible to tailor (i.e., profile) the language through metadata, URN links and constraints, and
- v) a tool that supports these concepts is available [62] and enables the creation of evaluation algorithms [5] that exploit various concepts.

2.5.2 Use Case Maps

The Use Case Map (UCM) scenario notation is another part of URN. This notation is used to model functional/operational requirements and casual relationships between responsibilities that can be optionally allocated to components. UCMs can also capture business processes while connecting them to their objectives, expressed in GRL.

A *map* contains any number of paths and components. A *path* is triggered by a start point (●, e.g., Hiring process in Figure 6) and results in an end point (■, e.g., New employee hired). To represent actions or tasks that are performed during the process, *responsibilities* (✕, e.g., Determine need for new position) can be defined. UCM supports both concurrent paths ($\neg\vdash$) through *AND-forks* and *AND-joins* and guarded alternative paths ($\neg\lhd$) with *OR-joins* and guarded *OR-forks*. *Waiting places* and *timers* model the concept of delay and timed synchronization. UCM models are usually composed of a root *map* that can further decomposed into sub-maps. A *stub* (◇, e.g., Confirm job) is a path element that contains sub-maps called *plug-in maps*, which are used to organize complex processes in hierarchies of sub-processes. *Dynamic stubs* can contain many plug-in maps, whose guarding conditions determine which ones are selected at run-time. Finally, different types of *components*, and especially *actors* (□, e.g., Hiring Manager), can be used to separate different parts of a process based on organizational units or roles. Figure 5 provides a summary of the UCM notation elements. Recall that URN links are indicated by small triangles (▶); this is a URN symbol common to both GRL and UCM.

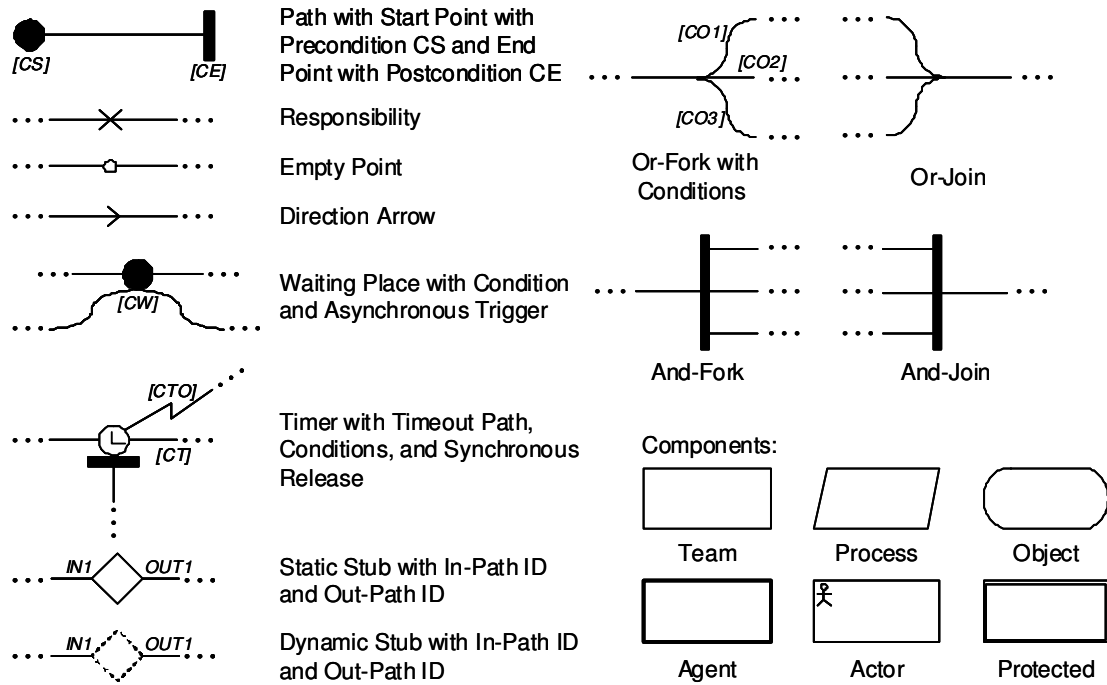


Figure 5, Summary of the UCM Notation Elements [4]

UCM supports the definition of *scenarios*. A scenario defines a specific path through the UCM model by providing initial values for variables used in guarding conditions and by specifying which start points are initially triggered. A *path traversal mechanism* can then simulate the progress of a scenario definition and highlight the specific scenario path taken among all possible scenarios.

Figure 6 illustrates a sample UCM model with one of its plug-in maps. The root map has one start point and one end point. In addition, it has four static stubs that are used to encapsulate the underlying process behavior. The Confirm Job stub has one input and one output associated with the start point and end point of its sub-map, respectively. The sub-map contains three responsibilities and one Or-Fork controlled by appropriate conditions. This process is elaborated in more detail in Chapter 5.

In this thesis, UCM is used to model business processes in our framework, since it is supported by URN [7][57] as well as jUCMNav [62]. In theory, it would be possible to use other business process modeling notations such as the Business Process Modeling Notation (BPMN) [94], or Unified Modeling Language (UML) activity diagrams [96] in

conjunction with GRL. However, the integration between GRL and UCM both at a conceptual level (i.e., URN metamodel) and at a tool level (i.e., jUCMNav), together with the fact that UCM is also a competitive workflow/process modeling notation [88], makes UCM the best option to pursue the research objective of this thesis.

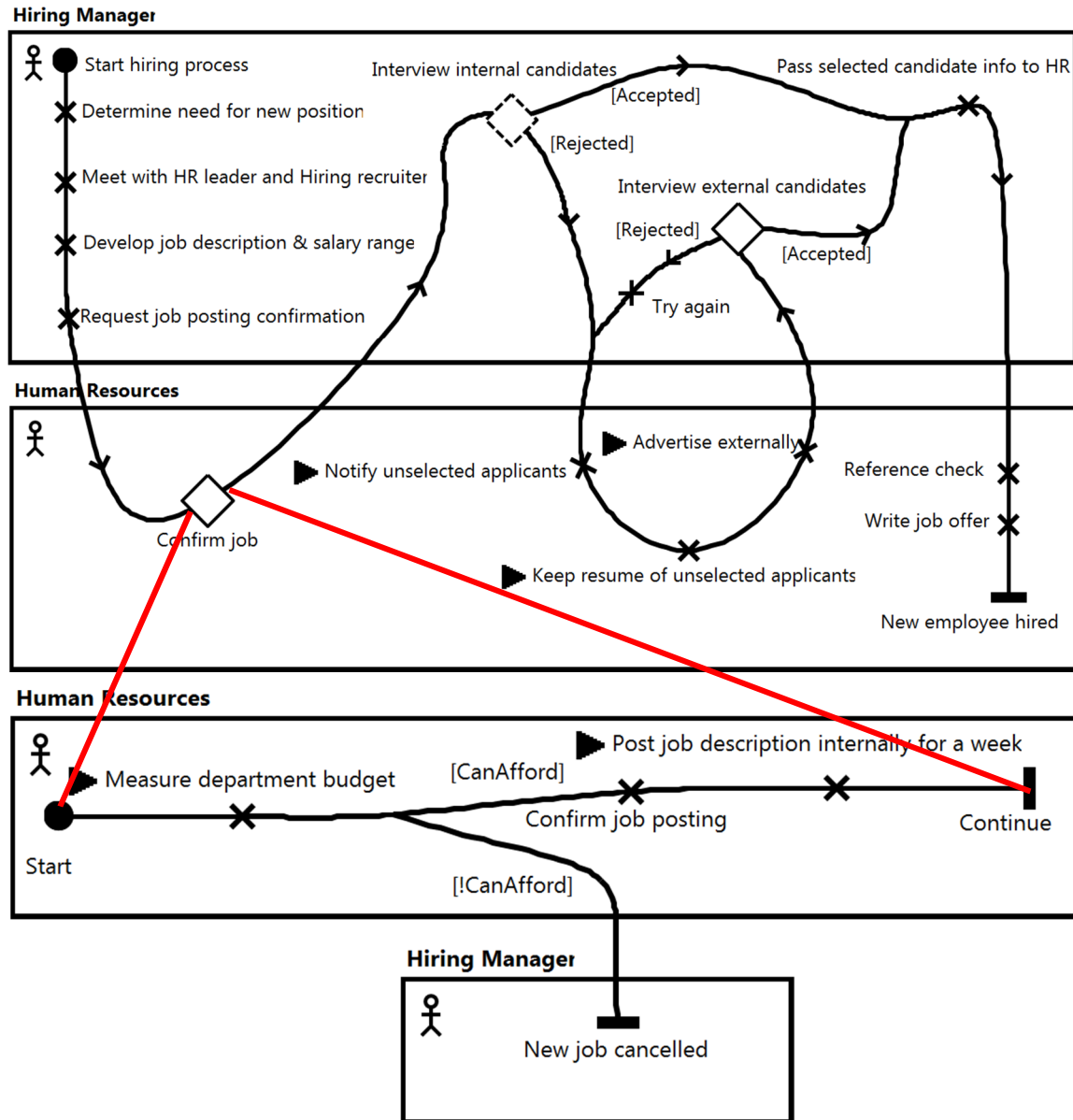


Figure 6, Sample UCM with a Plug-in

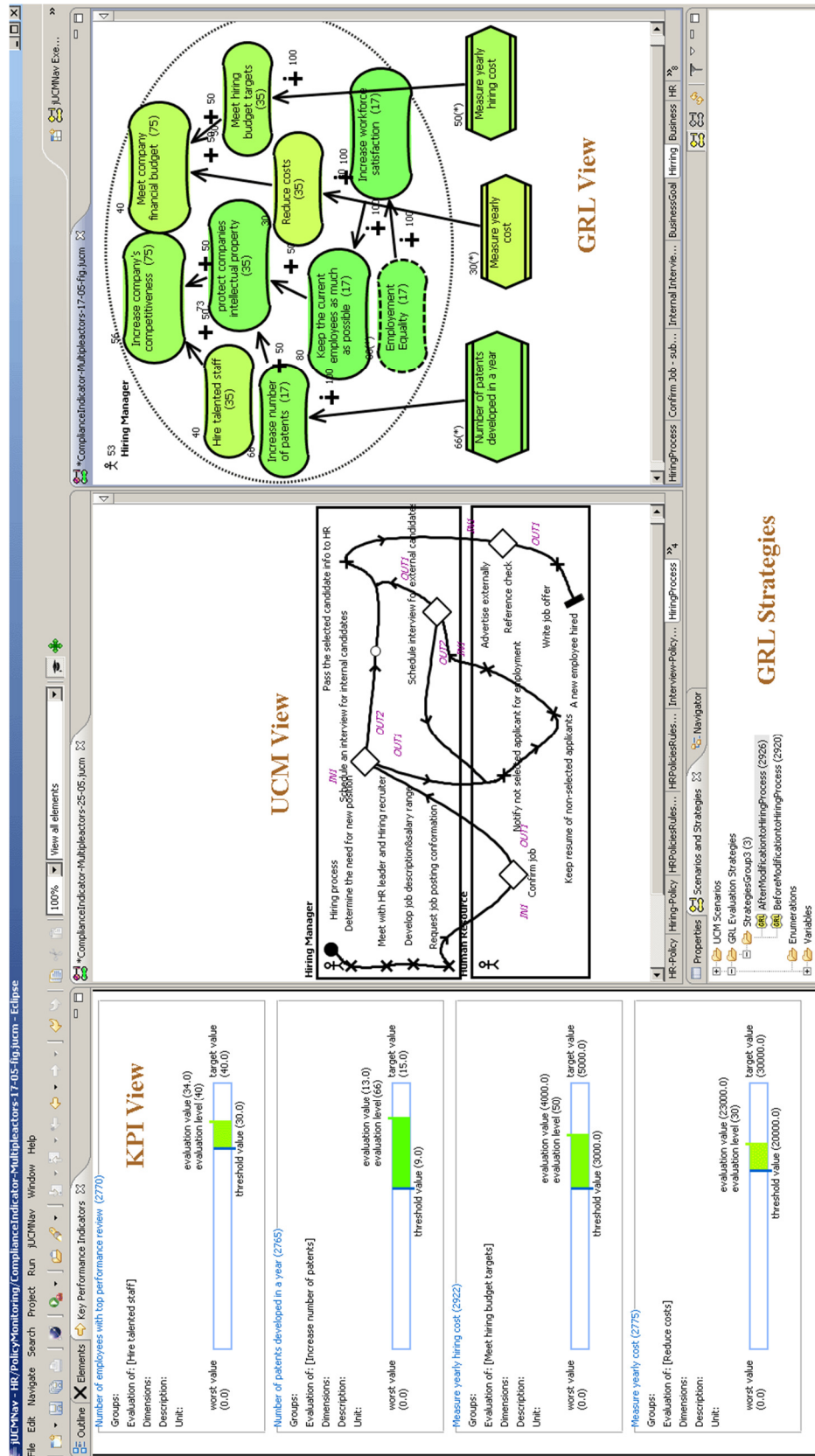


Figure 7, jUCMNav Views

2.5.3 Tools Support - jUCMNav

URN models can be created, managed and analyzed with jUCMNav [62], a free, Eclipse-based open source tool built using the Eclipse Modeling Framework (EMF) and the Graphical Editing Framework (GEF).

jUCMNav supports both GRL and UCM modeling as well as traceability between GRL and UCM model through *URN links*. This tool also supports GRL strategies (with several evaluation algorithms) and UCM scenarios (with one traversal mechanism) to help modelers analyze and validate URN models.

Figure 7 illustrates both the GRL and UCM views provided in jUCMNav. Support for KPI extensions and views is also provided.

2.6. URN for Compliance

URN has been used in the past in the field of compliance by Ghanavati *et al.* [41]. They proposed a URN-based requirements management framework for tracking compliance with legislation [39][40]. This framework can also be used to manage change and maintain compliance when privacy legislation is amended or when business processes evolve. This framework was used on an example from a major teaching hospital in Ontario (Canada) to enable health information custodians (HIC) track compliance with privacy legislation (PHIPA). Ghanavati *et al.* used URN to create models for the healthcare organization (in GRL) and business processes (in UCM) linked to a *separate* model for privacy legislation in GRL. With this framework, one can define and analyze different types of traceability, compliance, and responsibility links between organization and legislation models. The authors described a metamodel that defines *traceability* links between GRL elements of organization and legislation models, *compliance* links between the GRL model and actual policy and legislative documents, and finally *responsibility* links between the UCM elements of the organization model and GRL elements of the legislation model. These models are imported to IBM DOORS, a market-leading requirements management tool, and the links discussed above are established between them.

More recently, Ghanavati *et al.* [42] built on their previous work by adding the notion of contribution level for different link types. Using quantitative and qualitative

values for different links and with the help of GRL quantitative and qualitative analysis algorithms, they are able to determine the satisfaction level of organization and legal goals.

Regulations and laws sometimes impose constraints on organizations and stakeholder goals. It is very important to have a modeling tool to capture these constraints and enable organizations to deal with their objectives, which possibly conflict with legislation. In [43][44], Ghanavati *et al.* propose a revised framework in which they still use GRL to formally model laws and regulations, but this time with UCM in the legal model to capture some of the sequencing and priorities in laws that GRL does not support well. Although the modeling notation (URN) they use in their framework is the same as in the framework proposed in this thesis, the latter not only establishes traceability links between organization and policy models but also *measures* the level of compliance of business processes against policies with KPIs, and determines the impact of compliance-related process modifications on business goals.

2.7. URN and Key Performance Indicators

KPIs have been used in the past to measure the satisfaction level of goals and the performance of business processes. Pourshahid *et al.* [105][106] have extended URN to support KPIs as a new type of intentional element (). Indicators are usually linked to other intentional elements in GRL through contribution links, and to business processes in UCM through URN links. GRL strategies are used to evaluate the satisfaction level of intentional elements, including KPIs. Each GRL strategy initializes the KPI value sets. Each KPI contains four new values, not found in other types of intentional elements: the *Target Value* allows users to specify the target of a KPI, the *Threshold Value* identifies the least acceptable value for a KPI, the *Worst Value* identifies the maximum level of dissatisfaction, and the *Evaluation Value* is the actual measured value of a KPI. Any *Evaluation* value between the *Threshold* and *Target* values is acceptable (satisfaction) but values between the *Threshold* and *Worst* values are not acceptable (dissatisfaction). The evaluation values can be entered manually like other value sets (which is useful for the analysis of what-if situations) or automatically obtained from a data source such as a

Business Intelligence system. A GRL KPI maps the evaluation value to a satisfaction level: -100 for the worst value, 0 for the threshold, 100 for the target, and the other values are computed by linear interpolation between the target and threshold values (positive satisfaction), and between the threshold and worst values (negative satisfaction) [107]. The resulting satisfaction level can then be propagated to other elements in the goal model according to the goal evaluation algorithms presented in [6]. Furthermore, Pourshahid *et al.* recently proposed a new formula-based algorithm that allows one to aggregate several KPIs into one KPI using a mathematical formula [108]. This work brings a lot of flexibility to the supporting tool used in this research.

In Pourshahid *et al.*'s work, a framework for business process management has been suggested that helps organizations model and validates business processes from performance and compliance points of view. Although compliance validation has been suggested, KPIs have not been used for measuring the compliance level of business processes. However, Pourshahid *et al.* [104] used Aspect-oriented URN to improve business processes using KPI results and business process redesign patterns.

Note that the International Telecommunication Union has recently approved, in October 2012, a new official version of the URN standard that covers indicators. The indicator concept is hence now standardized in the Goal-oriented Requirement Language.

2.8. Goal Model Families

Modeling goal models with variations (e.g., parts of the goal model only apply to some category of objects) is a complex activity that is not currently supported by GRL. Such variation modeling leads to what is called goal model *families* in the literature. Since there are regulations that apply to different types of organizations, goal model families are required in the context of this thesis. This section discusses work related to this topic.

Recently, there has been much effort devoted to the modeling of variability in goal models. Ali *et al.* [2] present contextual goal models that extend TROPOS with variation points where the context may influence the choice among the available alternatives. They also use tagging with conditions on goals and links (decomposition, dependency, contribution). However, they are more interested in describing runtime adaptation based

on a logic-based representation of goals and conditions than in capturing families of related goal models with the automatic adjustment of quantitative contributions. They do not have graphical tool support either.

Lapouchnian *et al.* [73] proposed a framework for capturing, modeling, and analyzing domain variability for goal models. They label model elements with contextual tags, for elements that need to be visible in the model. A Boolean variable is assigned to each tag, identifying whether a tag should be active or not. They also propose an algorithm for extracting the parts of the goal model that are dependent on the context variability. Furthermore, they extend the i^* notation to represent and support variations in goal models [74]. Variations of a goal model can be generated from a single context-parameterized i^* model based on the current active contexts.

Goal-oriented languages have also been used to support feature models for software product line (SPL). Borba *et al.* [20] have conducted a comparison between existing goal-oriented techniques for feature modeling in SPL. In particular, Silva *et al.* [123] proposed an extension to i^* that enables modeling common and variable feature of SPL with cardinalities using tasks and resources of a goal model to capture features. Yu *et al.* [141] proposed a tool-based method to create feature models from a goal model. Mussbacher *et al.* [89] proposed an SPL framework based on Aspect-oriented URN (AoURN) that allows capturing features and reasoning about stakeholders' needs. They mapped SPL concepts into AoURN concepts and applied their framework to the Via Verde SPL to evaluate the proposed solution. Goal models are often used in the literature to express the tradeoffs about non-functional aspects when selecting particular configurations of software products. However, they are not really about families of goal models.

The concept of family of goal models has not really been discussed in a legal compliance context.

Although there has been some effort to support families in some of the other modeling languages like i^* , GRL, which was selected as the modeling language for this research for the reasons stated in section 2.5.1, does not support this concept. Therefore, required support for families will be added in this thesis (to be discussed in Chapter 7).

2.9. Business Intelligence

Business Intelligence (BI) is used to analyze business data and help organizations to better understand their business and make better decisions. BI technologies help decision makers assess how well a business is doing [138].

Business Intelligence brings many benefits that can help businesses [126]. For instance, BI users, particularly executives and managers, can get faster and quicker answers to business questions by looking at a customized dashboard rather than spending hours reading volumes of printed reports. Furthermore, BI has the ability to combine multiple sources of data with various formats. This feature is very important, especially in large organizations where not all data is stored in the same format or in the same database. Another important advantage of BI is the trending ability, which can help understand what happened to the business over time and explain *why*, to some extent.

Business Intelligence tools are widely used for reporting and analysis. Some of the well-known BI tools are: SAS (Statistical Analysis System), IBM Cognos, SAP Business Objects, Microsoft BI, and Oracle BI. Common functions of business intelligence technologies include querying and reporting, dashboard assembly, data mining, business process performance, and online analytical processing [138].

URN can be combined with Business Intelligence technologies. Business Intelligence tools can provide the infrastructure needed for extracting compliance indicator values from complex data sets and data sources. This thesis uses IBM Cognos as an example of such tool; another BI tool could have been used, but IBM Cognos and local expertise were readily available. This thesis will also show how a tool such as IBM Cognos can be used to generate reports on the status of organization business process compliance for stakeholders.

2.10. Summary

This chapter reviewed the background information required to understand this research. First, it started with an overview of the result of some surveys on compliance in the financial and healthcare sectors. It highlighted the organizations' costs to make their busi-

ness processes compliant with legislation. Then, this chapter briefly explained the definition of different categories of authoritative rules with some examples for each category, followed by an introduction on methods for defining metrics and indicators. Rule formalization in SBVR was also considered but SBVR is not used in this thesis as this research focuses more on regulation structure than on the content of rules themselves. In addition, this chapter gave an overview of the User Requirements Notation, a standard that combines goals with scenarios for business process modeling and analysis. Furthermore, this chapter studied related work regarding business process compliance and KPI-based performance management with URN. It also discussed alternative goal and process modeling languages, with an emphasis on work related to goal model families. Finally, it gave an overview of Business Intelligence and of its usage, benefits, and tools, with a particular attention to the compliance context.

The next chapter provides an in-depth literature review of the use of goal modeling and indicators for legal compliance measurement.

Chapter 3. Systematic Literature Review

This chapter provides a systematic literature review of compliance measurement based on goals and indicators that was conducted in order to investigate the research hypothesis.

3.1. Introduction

Nowadays, there is much ongoing research on Business Process Compliance (BPC). However, the lack of comprehensive techniques for *measuring* the level of business process compliance against policies while considering *processes* and *goals* motivates the conduct of a systematic literature review in this area. The objective of this review is the systematic selection and characterization of literature that focuses on BPC. The research questions addressed in this chapter are:

- What are the methods based on Key Performance Indicators (KPIs) used for measuring the compliance of business processes against policies and laws?
- What goal-oriented modeling methods are used for compliance measurement?

In recent years, some systematic literature reviews have been produced in the field of compliance management [1][27]. Otto *et al.* [97] explain different areas for modeling regulations and monitoring compliance. The research question that they answer is “what efforts have been made to model legal texts for use in requirements engineering and system development”. Abdullah *et al.* [1] and Cleven *et al.* [27] focus on regulatory compliance in the field of information systems. However, these last reviews are limited to the information systems domain or focus on the compliance assessment of business process instances with process definitions (without consideration for legal aspects or means to reason about trade-offs with other organization goals). Hence, they do not really help answering this chapter’s research questions.

This chapter’s review follows the method proposed by Kitchenham [67] for systematic literature reviews. The method is divided into three main phases, shown in Figure

8. The first phase is the selection of the related work, the second is the analysis of the selected material, and the third is the detailed review of relevant papers.

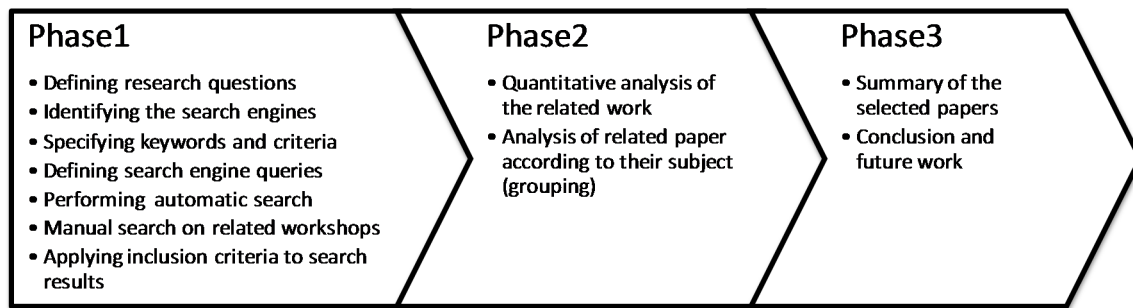


Figure 8, Literature Review Research Method

Since the original systematic literature review was done in 2010, a quick search (using business process compliance measurement as the keywords) was done on Google Scholar for papers related to business process compliance measurement and compliance framework. In addition, the latest work of several well-known researchers in this area was checked to update the current status on compliance measurement. A few papers were found, which are explained in sections 3.4.1 and 3.4.2. However, the figures (Figure 9, Figure 10, Figure 11, and Figure 12) and tables (Table 3, Table 4, and Table 5) in this chapter were produced in 2010 when the systematic literature survey was done. The new papers are not added to the result of the systematic literature survey.

3.2. Phase 1: Selection of Related Work

This phase identifies the search engines, selection criteria, and inclusion criteria.

3.2.1 Identification of Search Engines and Other Sources

Four popular IT search engines were considered for this review, including SpringerLink, IEEE Xplorer, and the ACM Digital Library. Google Scholar was also included in order to cover a broader range of domains (e.g., management and auditing) and venues. In addition, a manual search was done for the following workshops: *i** Workshop (for goal modeling) and GRCIS (for regulatory compliance). The initial selection was also extended with relevant articles cited in the papers found. The review was not scoped to a particular time period. The data set consisted of 142 papers from the search results and 62 pa-

pers from the manual inspection. Since not all papers found by the search engines were related to the selected research questions, selection criteria, discussed in the next section, were defined to filter out the first set of results.

3.2.2 Selection Criteria

Papers were sought that focused on goal modeling approaches and/or indicators for measuring compliance of processes with regards to regulations or policies. Five main sets of keywords were chosen for defining the search engine queries as well as the final filtering of the search results. The reviewed articles should at least focus on *Compliance*, *Business Process*, *Legal/Law/Policy*, *Indicator*, and *Goal Modeling*.

Using these five selection criteria, keywords and queries for the search engines were formally defined. The main abstract query is (goal AND compliance AND (law OR legal OR policy) AND (“performance indicator” OR KPI OR “compliance indicator”) AND “business process” AND model), used for all search engines except for Google Scholar. As the latter returned thousands of unrelated papers with the aforementioned keywords, it was decided to narrow down the results by replacing “business process” keyword with “business process compliance”. In addition, a simpler query (“Business process compliance” AND “Goal” AND (“KPI” OR “Indicator”)) was performed on all four search engines, but most articles found were the same as in the first set of queries, and only 8 new articles were found. A manual search of the two related workshops led to an additional 56 papers. The search results are reported in Table 3. Note that duplicates were removed from this table in the order in which the search engines and workshops were explored. For instance, the 20 papers for ACM reported here were neither in Springer’s list nor in IEEE’s, but the ACM search engine reported other papers already covered by the two engines previously used. Appendix A lists the papers selected through these research engines.

	Springer	IEEE	ACM	Google Scholar	GRCIS	iSTAR	Simpler Query	Cited	Total
Search Result	44	45	20	25	19	43	8	0	204
Finally Selected	2	7	4	8	6	2	0	9	38

Table 3, Automatic and Manual Search Results

3.2.3 Inclusion/Exclusion Criteria and Procedures

In this step, each of the 204 papers was reviewed based on the abstracts and conclusions.

A paper was included if any of the following conditions were true:

- It was related to compliance of processes or legal/policy compliance;
- It used indicators for any kind of measurement, not just BPC (e.g., for process performance or for assessing the security of a complex process); or
- It was related to stakeholder or organization goals (goal-oriented).

Category	Paper	Goal	Business Process	Compliance Modeling	Process Modeling	Law/Legal /Policy/Rule	Compliance	Indicator/KPI
Compliance framework and standards	[110]	No	No	No	No	Yes	Yes	No
	[63]	No	Yes	No	Yes	Yes	Yes	No
	[64]	No	Yes	No	Yes	Yes	Yes	No
	[66]	No	Yes	No	Yes	Yes	Yes	No
	[65]	No	Yes	No	Yes	Yes	Yes	No
	[78]	No	Yes	No	Yes	Yes	Yes	No
	[69]	No	No	No	No	No	Yes	No
	[22]	No	Yes	No	No	Yes	Yes	No
	[134]	No	No	No	No	Yes	Yes	Yes
Measure of compliance levels	[37]	No	No	No	No	Yes	Yes	No
	[87]	No	Yes	No	Yes	Yes	Yes	No
	[77]	No	Yes	No	Yes	Yes	Yes	No
	[124]	No	Yes	No	No	Yes	Yes	Yes
	[113]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Discovery and controls of non-compliant business processes	[38]	No	Yes	No	No	No	Yes	No
	[90]	No	Yes	No	No	Yes	Yes	No
	[115]	No	Yes	Yes	Yes	Yes	Yes	No
	[81]	Yes	Yes	Yes	Yes	Yes	Yes	No
	[40]	Yes	Yes	Yes	Yes	Yes	Yes	No
	[41]	Yes	Yes	Yes	Yes	Yes	Yes	No
	[114]	No	Yes	No	No	Yes	Yes	Yes
	[10]	No	Yes	No	Yes	Yes	Yes	No
	[136]	No	Yes	No	Yes	Yes	Yes	No
Goal-oriented techniques and KPI	[16]	No	Yes	No	Yes	Yes	Yes	No
	[105]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	[104]	Yes	Yes	No	Yes	No	No	Yes
	[92]	Yes	Yes	No	Yes	Yes	No	Yes
	[19]	No	No	No	No	No	No	Yes
	[83]	No	No	No	No	Yes	No	Yes
	[31]	No	Yes	No	No	Yes	No	Yes
	[86]	Yes	No	No	No	No	Yes	No
	[84]	Yes	Yes	No	Yes	No	No	No
Others	[103]	Yes	No	No	No	No	No	Yes
	[17]	Yes	Yes	No	Yes	No	No	No
	[82]	No	Yes	No	Yes	No	No	Yes
	[98]	No	Yes	No	No	Yes	Yes	Yes
	[79]	No	No	No	No	No	Yes	Yes
	[80]	No	No	No	No	No	Yes	Yes

Table 4. Selected Papers and Criteria

The last two aforementioned criteria were defined to improve understanding of the other applications of goal-oriented and KPI-based approaches. Furthermore, a paper was excluded if any of the following conditions were true:

- It discussed compliance but not in relation to business processes or to the legal/policy domain (e.g., network compliance); or
- The paper was not written in English.

Finally, after considering all the papers against the above criteria, 38 papers were selected for the next phase for further analysis and detailed review. Table 4 lists all 38 papers, the criteria (keywords) they satisfy, and the five categories to be introduced in section 3.3. Figure 9 illustrates the distribution of articles by subject.

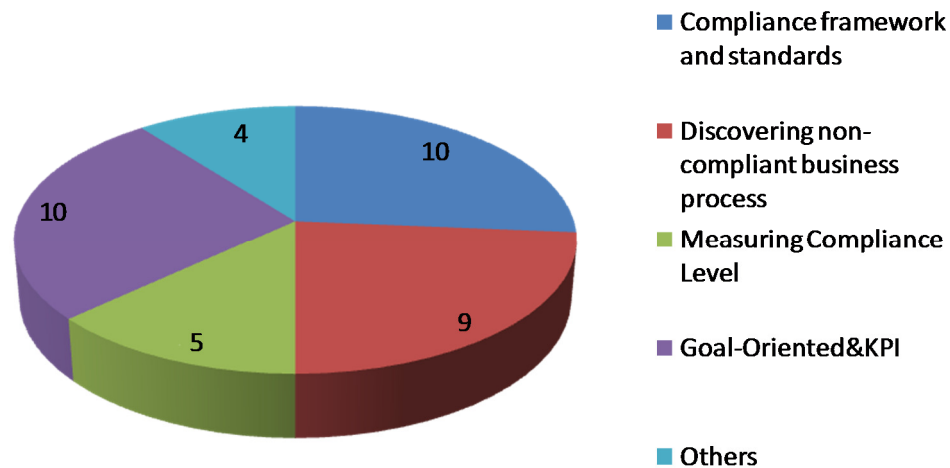


Figure 9, Distribution of Articles by Subject

3.3. Phase 2: Analysis of Related Work

3.3.1 Quantitative Analysis of the Related Work

Distribution of Articles over Years: The selected articles that met the criteria were surprisingly only published in last five years, which shows a growing interest in this topic in recent years. Figure 10 clearly shows that a large proportion of papers were published in 2008 and 2009. The lower numbers in 2010 could be due to the fact that the search for papers was done in the second half of 2010 and may not have found all the papers published in that period of time.

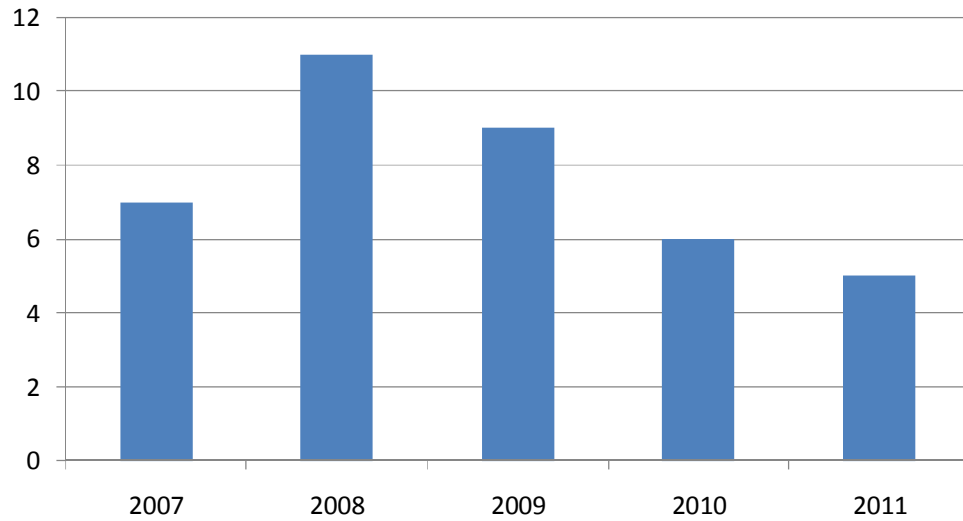


Figure 10, Distribution of Articles by Year

Distribution of Articles by Region: The review results depicted in Figure 11 indicate that 13 different countries contributed in this area. Germany has the largest number of contributions, followed by Canada and then (*ex equo*) Australia and Italy. This figure simply highlights some facts and does not formulate any theory about the geographical distribution of teams who are working on compliance.

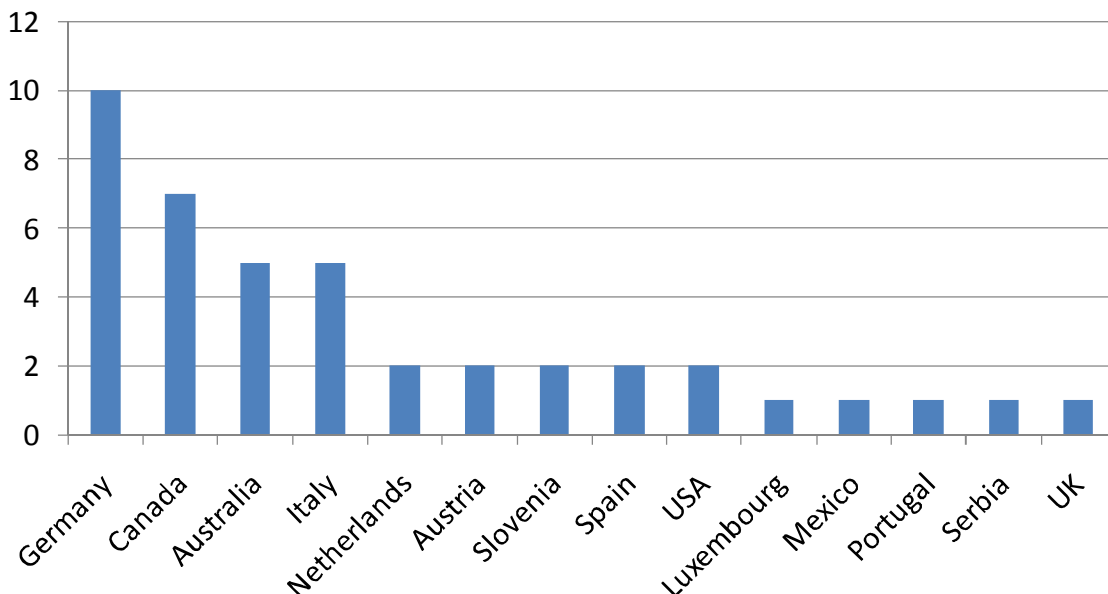


Figure 11, Distribution of Articles by Region

Contributors and Location: The total number of contributions from each university/research center is presented in Table 5. Additional information (e.g., authors and affiliations) can be found in Table 52 of Appendix A. Table 5 only illustrates locations that have more than one contribution.

Location	Contribution
SAP Research Center CEC Karlsruhe	4
University of Ljubljana	2
University of Ottawa	5
University of Queensland	3
University of Trento	5
University of Vienna	2
University of Wollongong	2

Table 5, Contributions and Locations

3.3.2 Analysis of the Papers Based on their Content

After careful analysis of the papers' contents, the papers were grouped into five categories in view of their subject and of the research questions.

- **Compliance frameworks and standards:** This category includes papers that suggest a framework for regulatory compliance or compare standards (see section 3.4.1).
- **Measurement of compliance levels:** Approaches that not only discover non-compliant business processes but also measure their compliance level qualitatively and/or quantitatively (see section 3.4.2).
- **Discovery and control of non-compliant business processes:** Approaches for discovering and controlling non-compliant business processes that however do not suggest solutions for measuring compliance levels (see section 3.4.3).
- **Goal-oriented techniques and KPI:** Papers using goal-oriented techniques and KPI measurements for applications not related to compliance (see section 3.4.4).
- **Others:** Papers related to compliance not appropriate for any of the previous compliance related categories (see section 3.4.5).

The review focuses on research related to business process compliance based on indicators and goal-oriented approaches. As illustrated in Figure 12, Ghanavati *et al.* [40][41] and Marino *et al.* [81] propose goal-oriented approaches for business process compliance. Rodriguez *et al.* [114] and Silveira *et al.* [124] suggest business process compliance man-

agement using KPIs. Popova and Sharpanskykh [103] propose a framework for modeling organization goals based on KPIs. In [92], Nigam *et al.* model the high-level business goals that drive operational goals as well as the KPIs to manage and monitor operational artifacts. Pourshahid *et al.* [105] use KPIs to validate process performance. However, none of these research contributions focuses on all the three areas of interested, except the work from Rifaut and Dubois [113]. The latter authors discuss a goal-oriented and KPI-based approach to model and measure business process requirements including regulatory compliance. However, this chapter’s research questions cannot be answered through this framework (the details of this paper are presented in section 3.4.2).

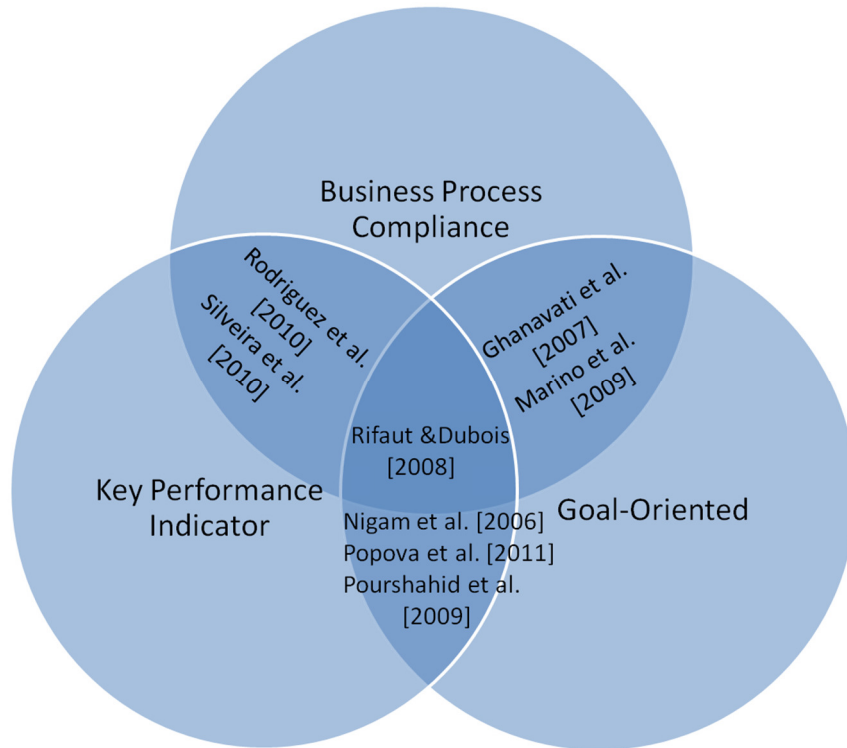


Figure 12, Analysis of Papers Based on Groupings

3.4. Phase 3: Summary of Selected Papers

3.4.1 Compliance Frameworks and Standards

There are numerous methodologies and standards for IT security and governance that help companies increase IT efficiency and meet regulatory requirements. Radovanovic *et*

al. [110] compare several of them. They claim that out of 1865 companies, 69% use COBIT for IT governance, 11% use ITIL for its best practices in IT services management, and 12% use ISO 27002 for IT security. These standards are used for internal audits and IT process improvement, as well as addressing legal requirements such as protection and non-disclosure of personal data and the Sarbanes-Oxley Act (SOX).

Karagiannis *et al.* [63] propose a six-step business process modeling approach for SOX regulatory compliance. This approach relies on detecting risks in processes (related to a particular section of the SOX regulations) and addressing them by defining controls. In addition, they design extensive test cycles to verify compliance. If the test results show a gap, then a redesign step is considered to address the detected issues. They also propose the use of a business process management platform called ADONIS as the supporting tool for the methodology [64].

Kharbili and Stein [66][65] define high-level requirements and an architecture for compliance management. They introduce a three-layered architecture: 1) one to document and model policies, 2) one for design-time artifacts such as process models and business rules, and 3) one for the execution of both processes and rules. Furthermore, they propose transforming regulations into semantic policies, transforming semantic policies into semantic business rules, and then transforming the latter into operational rules that can be used to automate processes. They also discuss eight dimensions used to assess compliance management systems (CMS, Figure 13), to be applied to IPCF in section 8.2. A general search was done in the literature to find papers related to compliance management framework properties, and this was one of the only two papers that were found. This is the reason why CMS properties are used to evaluate IPCF in section 8.2.

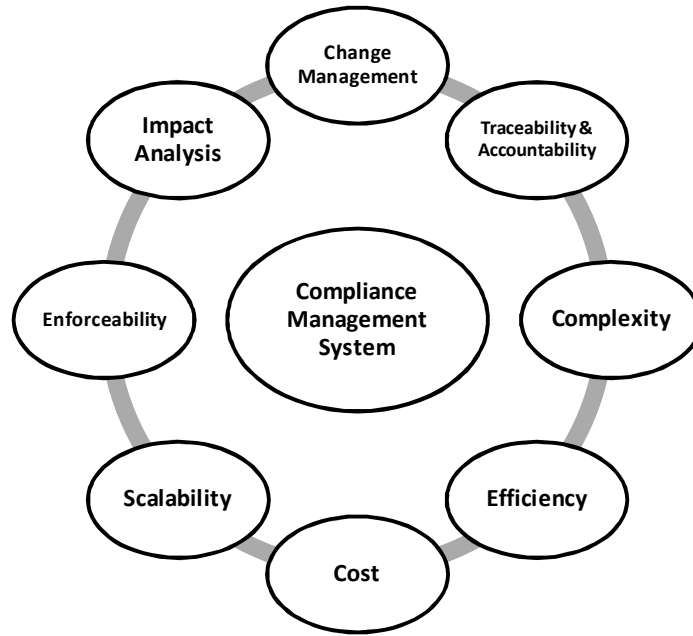


Figure 13, Compliance Management System (CMS) Properties

Ly *et al.* [78] propose fundamental requirements for process management systems' compliance with rules/policies. In addition, they assess the existing frameworks with respect to the proposed requirements.

Koliads and Ghose [69] describe a compliance program, i.e., a set of management processes that helps organizations with regulation compliance. In their context, a compliance program should be able to discover compliance obligations and to report on the overall compliance of the organization. In addition, such program should have a mechanism for improving non-compliant processes and be able to identify, measure, and mitigate risks.

Cabanillas *et al.* [22] describe all the features based on literature review that a Business Process Compliance Management System (BPCMS) should support during all business process lifecycle, including design, analysis, configuration, enactment and evaluation. They present the existing approaches and frameworks that already cover the features of full compliance coverage for business process lifecycle. In addition, they identify the areas that are not addressed yet and that need further research. This was the second and last paper found in the literature that discusses the desired features of a BPCMS. These features are applied to evaluate IPCF in section 8.3.

Vicente *et al.* [134] describe a set of high-level concepts and domain definitions in the area of governance, risk and compliance (GRC). They propose a conceptual model for these areas based on the available literature review and frameworks. They define the relations between these three conceptual models and finally suggest an integrated conceptual model. They compare their conceptual model with the Open Compliance and Ethics Group (OCEG capability model) [109] and a quality model suggested by Moody *et al.* [85] to evaluate their model.

Finally, Foorthuis and Bos [37] describe key concepts regarding compliance, such as actors, norms, policies, conformity, conformance, and compliance. They also propose a framework for categorizing various tactics for achieving compliance in organizations.

The last three papers are not part of the data set returned by search engines. These papers were added to the literature survey after it was initially performed.

3.4.2 Measurement of Compliance Levels

Morrison *et al.* [87] define a method for measuring the degree of compliance of processes with respect to both crisp and imprecise compliance requirements. Their method relies on creating a compliance scale model that allows measurement of both qualitative and quantitative values for a particular process instance. Although this method can assess the level of compliance of a process, it requires much preparatory work to determine the compliance scales.

Lu *et al.* [77] propose a method for measuring BPC against control rules defined using control objectives from different sources (e.g., regulations or partner contracts) and are modeled using the Formal Contract Language (FCL). They define concepts of ideal semantics for control rules in order to categorize various degrees of compliance between processes and rules. They categorize them into four groups: ideal, sub-ideal, irrelevant, and non-compliant situations. They calculate both ideal and sub-ideal compliance degrees of businesses processes against control rules to evaluate how well the process model supports control rules.

Silveira *et al.* [124] suggest a compliance governance dashboard, with key compliance indicators used to measure the compliance level of processes. Their CGD consists

of different levels of abstraction. The top-level page shows the most critical regulatory and policy indicators, the compliance level of the main processes, as well as an overall compliance level for the organization. One can drill down to see more details and analyze the compliance of individual process atomic units in various business units. Furthermore, one can view compliance violation reports consisting of all the information reported to internal and external auditors.

Rifaut and Dubois [113] propose a method to combine and model the regulations and business requirements for processes. They combine tabular requirements with i^* goal models, where they model *purposes*, and decompose them all the way down to indicators used to assess and measure the success of processes. This framework can be used prior to the design and implementation of a process, as well as later on for monitoring and controlling the compliance of processes. The author suggests a method [111] to simplify the process of modeling regulations and the arguments for claiming compliance, and of supporting discussions between regulators and regulatees along the way. To do so, the method takes advantage of the Measurement Framework, hence making it a structured approach. Furthermore, the i^* notation is used to model a generic and reusable measurement model based on ISO15504 [58], a specific measurement model of the process being studied, and also the model of the implemented process.

Greke *et al.* [38] propose an algorithm for measuring the compliance degree and maturity of processes with reference models. They evaluate their approach by measuring the compliance level of a German passenger airline with the IT Infrastructure Library (ITIL) reference model. The last two papers were not part of the data set returned by search engines. These papers were added later to the literature survey.

3.4.3 Discovery and Control of Non-Compliant Business Processes

Namiri and Stojanovic [90] propose a formal logic-based framework for managing BPC. They identify significant accounts (e.g., inventory) with major impact on financial reporting. Then, they identify all relevant risks (e.g., customer order rejection) and processes (e.g., warehousing and purchasing process). Finally, they define a set of controls for these

risks, and suggest properties focusing on relationships between the accounts, controls, processes, and risks.

Sadiq *et al.* [115] propose a structured approach bringing together compliance control objectives and process models. Control objectives are modeled through a modal logic based on FCL. They also propose four types of control tags (flow, data, resource, and time) used to visually annotate process models and illustrate the aspects of a process controlled by control objectives.

Marino *et al.* [81] check BPC at design time to detect sources of non-compliance. They define control objectives, derived from both regulations and business objectives/goals, at a high level and refine them into lower-level functions and procedures (activity controls) implemented in the form of control processes. In addition, they propose an algorithm used to perform bottom-up satisfaction analysis of control objectives. A second algorithm is suggested to detect the impact of process activities on the control objects in terms of satisfaction and compliance.

Ghanavati *et al.* [40][41] propose a requirements management framework for BPC based on the User Requirements Notation [57]. In this framework, the legal requirements and organization goals are modeled using URN's Goal-oriented Requirement Language and business processes with URN's Use Case Maps. In addition, the models are linked to policies and legal documents using a commercial requirement management system. Several types of links between organizational and legal models are defined to detect non-compliant processes and react to changes in the law and processes.

Rodriguez *et al.* [114] build on the results obtained from CGD [124] using a decision tree algorithm and data mining to analyze, predict, and explain non-compliant process instances. They successfully apply their method to a drug dispensation process.

Awad *et al.* [10] propose a method for automatic detection and resolution of compliance violations in process models using patterns. This is a great step toward addressing maintenance issues in the process compliance space. Weber *et al.* [136] propose an approach for validating a process against a set of predefined constraints. The objective of this work is to detect states of the process execution violating the defined rules.

Becker *et al.* [16] propose a pattern-matching approach to check business process compliance. They use the Semantic Business Process Modeling Language (SBPML) to model business processes and the pattern matching method that is used for process model checking. Furthermore, they define compliance rules in SBPML. Their pattern-based approach checks for occurrences of compliance rule violations in the process model. They apply this approach to the example of a credit approval process from a bank scenario.

Finally, Papazoglou *et al.* [99] propose a business process compliance framework that includes a pattern-based declarative language to be used by business analysts to define compliance requirements. They use temporal logic to generate formal expressions from these patterns to enforce the compliance requirements.

The last two papers are not part of the data set initially returned by the search engines. These were added manually following the initial completion of the systematic review.

3.4.4 Goal-oriented Techniques and KPI

Pourshahid *et al.* [105] extend URN to validate processes from both performance and compliance points of view. In addition, they use aspect-oriented extensions to URN to improve processes dynamically using KPIs and redesign patterns [104].

Nigam *et al.* [92] suggest an artifact-centric approach for BPM. They model the high-level business goals that drive operational goals as well as the KPIs used to manage and monitor operational artifacts. In addition, they formally introduce the concept of a management rule, defined to react to events occurring in the organizations. Boehmer [19] also uses efficiency and effectiveness KPIs to evaluate and measure the value of an investment to prevent risk in the implementation of an Information Security Management System based on ISO 27001. Martin and Refai [83] propose a framework for measuring and monitoring IT security performance using metrics.

Dang *et al.* [31] describe an ontological framework for designing healthcare processes, resources, and rules. Their framework contains five different views of a hospital

as well as the relations between components of these views. A KPI view is used to monitor and evaluate performance from different perspectives.

Morandini *et al.* [86] summarize three goal-oriented research areas ongoing at the University of Trento, i.e., system requirements for compliance with laws, the selection of the best design patterns during system design, and self-adaptive systems using software agents that select alternative paths at run-time to achieve system goals.

Martinez *et al.* [84] propose a goal-based approach (using TROPOS) to monitor and assess the impact of processes on enterprise and actor goals. Furthermore, Popova and Sharpanskykh [103] recently proposed a framework for modeling organization goals based on KPIs. However, they have not used this framework for compliance management. Behnam *et al.* [17] use a goal-driven development method, considering both organization and system goals, to design and develop patient surveillance software for monitoring adverse events (again, without KPIs).

3.4.5 Others

Compliance plays a critical role in outsourcing environments where trust between clients and contractors can be an issue. Massacci and Yautsiukhin [82] use indicators to assess the security of a complex process in such situations. They use Key Assurance Indicators (KAI) to show how client goals are met, and Key Security Indicators (KSI) to measure the security techniques utilized by contractors. According to Pasic *et al.* [98], KAI can be used to evaluate process compliance and KSI can illustrate the quality of the control processes used to achieve compliance.

Mahnica *et al.* [79][80] discuss the compliance of AGIT (AGile software development) against COBIT with regards to indicators. AGIT models consist of indicators for the performance of a Scrum software development process. The authors compare AGIT indicators with COBIT indicators to check whether the latter are measurable using AGIT. Finally, they propose adding new indicators to AGIT to cover the gaps discovered.

3.5. Summary

This chapter reports on a systematic literature review that addresses two questions: *Have KPIs been used for compliance measurement?* and *Are there any goal-oriented methods for compliance measurement?* Although the answer is yes to both questions, no available solution yet combines goals with KPIs for measuring the overall compliance of organizations.

The 38 selected papers were grouped into five categories. The first one focuses on compliance frameworks, reference models, and standards, and it can be used as general guidelines for assessing compliance management frameworks. The next category targets the measurement of compliance levels of processes. The two papers most related to the thesis research topic are from Silveira *et al.* [124], who suggest a dashboard/KPI approach to measure the overall compliance of an organization, and from Rifaut and Dubois [113], who propose a goal-oriented process assessment model capturing and measuring process requirements. Although the approach in [113] addresses both research questions posed in this chapter, the paper does not identify how KPI values are measured and does not suggest a method for measuring the overall compliance level of the organization. In the category related to non-compliant business processes, some papers propose logic-based frameworks for modeling controls and rules whereas others use goal-oriented languages such as URN or *i**. The goal-oriented and KPI category covers papers with approaches in research areas not related to compliance. Finally, the last category discusses papers related to compliance that are not appropriate for any other category.

Research on BPC has increased significantly in the past 5 years. Much of the research uses control objectives as a means of expressing compliance goals for business processes, while internal controls are used as means to make processes compliant. Also, several goal-oriented and measurement (KPI)-based approaches to manage and control compliance in organizations have been proposed. These two types of approaches are similar in the sense that in both cases, regulation requirements are imposed on processes as process objectives. None of these approaches, however, provides a final qualitative indicator on the compliance level of organizations. This would be a key enabler for upper management to analyze the current state of the organization and plan for the future. As a

result, an important item for the research agenda in this area is the qualitative measurement of the level of compliance in organizations. Tackling the combination of KPIs with goal-oriented approaches, possibly using business intelligence applications for visualization and reporting to provide the infrastructure for measuring and monitoring the compliance level of organizations, is hence an important topic that deserves attention. In summary, they are two aspects that motivate one to use combination of KPIs and goal-oriented measurements:

1. From a legal model perspective, goal elements and their links reflect the structure of legal and policy documents from a high-level view down to the rule level, and the KPIs allow one to measure the compliance level of rules that then propagate up to the goal level. This information is quite valuable to regulators.
2. From a business point of view, having goals and KPIs together in this context allows one to measure the impact of changes done to business processes to satisfy legal compliance requirements on the high-level business goals of the regulated organization.

In both cases, this hierarchical structure helps analysts to focus on the abstraction level they want and to either understand the overall satisfaction of goals at a high level or drill down to details at a KPI level in order to find the root cause of unsatisfied goals.

The next chapter gives an overview of the new compliance framework proposed in this thesis, which combines goal modeling with indicators.

Chapter 4. Indicator-based Policy Compliance Framework

This chapter describes the proposed *Indicator-based Policy Compliance Framework* (IPCF), together with the inputs, outputs and steps of its compliance method. This framework builds on the *User Requirements Notation* (URN) and *Key Performance Indicators* (KPIs). Section 4.1 provides an overview of the framework while sections 4.2 to 4.5 elaborate on each of its four compliance method steps.

4.1. Framework Overview

The Indicator-based Policy Compliance Framework is composed of:

- A modeling language, i.e., URN augmented with KPIs and new stereotypes, and constrained by well-formedness rules;
- A compliance method that involves modeling, analysis, improvements and monitoring; and
- Tool-support based on jUCMNav and on BI tools.

The main objective of this framework is to provide a modeling approach and guidelines enabling organizations to measure the current compliance level of their processes, track down and address compliance problems, and also evaluate the impact of changes on the overall compliance level of the organization. In order to meet this objective, IPCF's compliance method requires the following inputs, as illustrated in Figure 14:

- The policy/regulation model, including sub-policies, rules and key performance indicators modeled with standard GRL extended with KPIs;
- The organization's goal model (in GRL) and business process model (UCM); and
- The importance level of high-level business goals.

The expected outcomes of the compliance method are as illustrated in Figure 14:

- Compliance level measures for policies and rules;

- Compliance changes after business process or policy modifications;
- Impact of compliance-related process modifications on business goals; and
- Prioritized list of non-compliant processes.

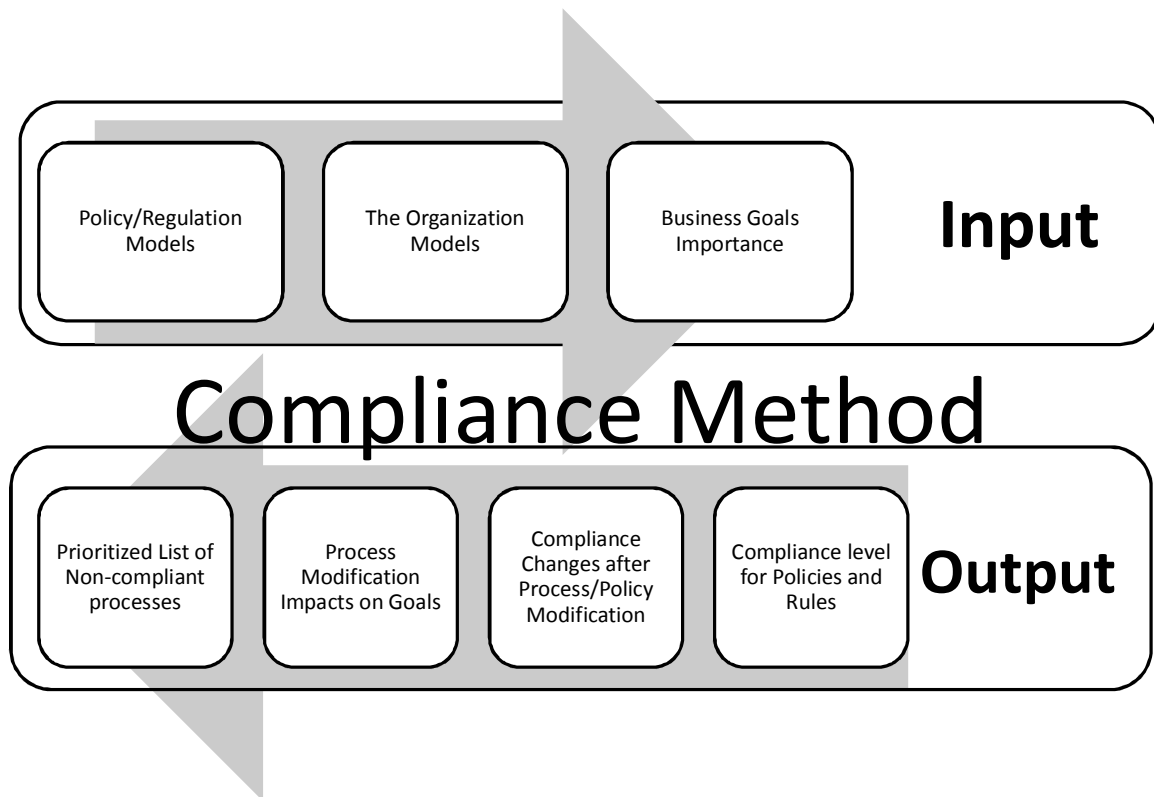


Figure 14, Framework Inputs and Outputs

As illustrated in Figure 15, the method is iterative and consists of four main steps: modeling, evaluation, improvement and monitoring. The details of each step are discussed in the next sections.

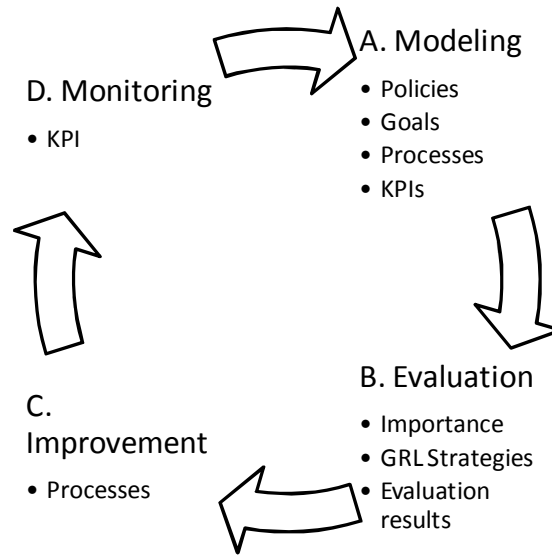


Figure 15, Method Steps

4.2. Step A: Modeling

In this step, the elements illustrated in Figure 16 are modeled. Policies are modeled starting at a high level, possibly from laws and regulations, or from internal policies. Then, they are decomposed down to the level of operational/control rules. The assumption here is that the regulation documents fit into the metamodel discussed in Figure 17 and can be modeled using the guidelines discussed in section 4.2.2. These rules control the processes required to be compliant with the policies. A set of KPIs is defined for each rule, which will enable measuring the level of compliance for the rules by comparing the desired target value with the current value of each KPI. Furthermore, organization goals and business processes are also modeled, hence providing a more holistic view of the context where policies are used. Rules are associated with related organization business processes through URN traceability links. Furthermore, a set of KPIs is defined and connected to the business goals to help analyze the impact on the organization goals due to changes made to business processes for improving the compliance level. The KPI set defined for the legal side of the model and the KPI set defined for the business side of the model are not identical and each achieves a different objective. While the former is used to measure the compliance level, the latter is used to measure the satisfaction of business objective.

This step helps simplify traceability between policies, business processes, and organization goals.

Organization goals, policies, and rules are modeled using the GRL notation while business processes are modeled using the UCM notation. The KPIs are, however, modeled using an extension of URN introduced in [105]. Finally, the business processes in the organization model are associated with related business goals and KPIs using URN links. The same method is used to associate the control rules in the policy model with corresponding business processes in the organization model.

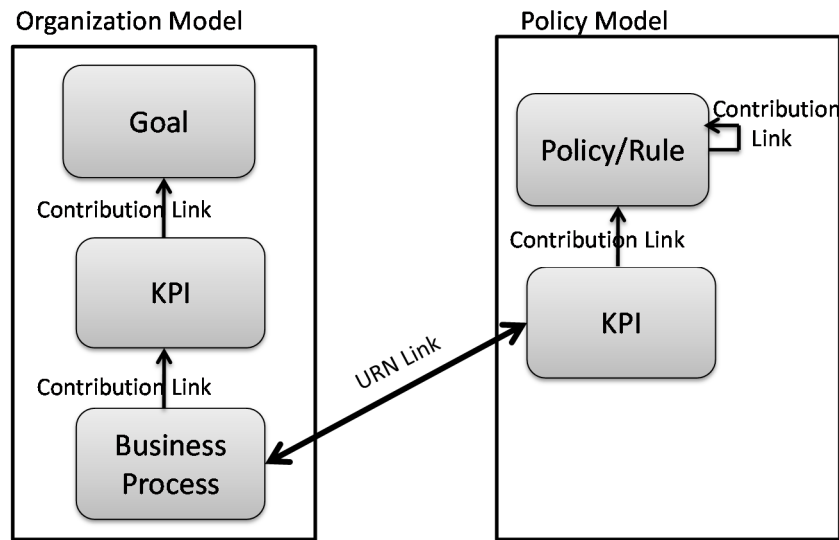


Figure 16, Elements of the Framework

The URN standard offers lightweight profiling mechanisms to extend the language with metadata (name-value pairs that can be used to capture stereotypes), URN links (for ad-hoc typed relationships), and concerns (groupings of model elements). The precision of policy models can be improved by adding well-formedness constraints to the meta-model elements of the framework. In addition, by defining appropriate stereotypes for GRL intentional elements (e.g., policies and rules), the traceability between GRL models and legal documents will be improved. However, the use of these stereotypes is optional in the GRL model. For example, any GRL intentional element in a «Policy» diagram, such as goals and softgoals, which maps to a policy statement in the source document will be

tagged as a «Policy» and any goal that maps to a rule statement in the source document will be tagged as a «Rule».

The rest of this section focuses on the systematic modeling of *policies and regulations* with GRL, as this is a contribution of this thesis. The modeling of *organizations* with GRL and UCM is discussed at length in related work by Weiss and Amyot [137] and by Pourshahid *et al.* [105][107]. The only specific item added to these general guidelines is the explicit use of an actor named *Business* in the GRL model of the organization, which contains the top-level goals (or softgoals) of the organization.

4.2.1 Regulations Structure

In order to map the structure of regulations, laws, and policies to stereotyped GRL elements, several such documents were studied:

1) PHIPA regulation [47] has the following structure:

- Part
 - Sub-part
 - Section
 - Rule Statement
 - Condition

2) HIPAA regulation [52] has the same structure as above:

- Part
 - Sub-part
 - Section
 - Rule Statement
 - Condition

3) SOX regulation [29] has the following structure:

- Title
 - Section
 - Rule Statement
 - Condition

4) Basel II regulation [13] has the following structure:

- Pillar
 - Sub-Pillar

- Section; some sub-pillars, in addition to sections, also consist of rule statements.
 - Rule Statement
 - Condition
- 5) Gramm-Leach-Bliley regulation [13] has the following structure:
- Chapter
 - Sub-Chapter
 - Section
 - Rule Statement
 - Condition
- 6) The sample Human Resource Policy has the following structure:
- Policy
 - Sub-Policy
 - Section
 - Rule Statement
 - Condition
- 7) Several Transport Canada policies have the following structure:
- Part
 - Sub-part
 - Rule Statement (Organization type for some rules)
 - Condition

We use the concept of *Term* to refer to the various structural elements in policies and regulations. The following terms can hence be observed in these documents:

Parts/Title/Pillar/Chapter/Policy: Regulations are divided into *parts* or, as observed in some other regulations, into titles, pillars, chapters, or policies. For example, HIPAA is divided into three parts, including part 160-General Administrative Requirements, part 162- Administrative Requirements, and part 164-Security and Privacy. In addition, Basel II consists of three pillars, Minimum Capital Requirements, Supervisory Review Process, and Market Discipline.

Sub-part/Sub-pillar/Sub-chapter/Sub-policy: Each part (or equivalent) is divided into *sub-parts* or, in some regulations, into sub-pillars, sub-chapters, or sub-policies. For instance, Part 164 of HIPAA regulation is divided into 5 subparts.

Section: Each subpart is often further divided into *sections*. For instance, subpart E of HIPAA part 164, about privacy of individually identifiable health information, is divided into 17 sections.

We generalize all these various kinds of elements that can form the hierarchical structure of the legal document to what we call a *Term*. All legal documents that we reviewed are constructed using a hierarchy of terms until they get to the leaf level, which describes the *Rule Statements* at a more measurable and actionable level.

Rule Statement: A rule statement is a special kind of term at the leaf level of a document. The lowest level *Terms* in a legal document can have various *Rule Statements* that may include various *Conditions*. For instance, section 164.500 (applicability) of HIPAA is divided into 3 rule statements (a, b, and c). In some regulations, higher level terms, such as subparts/sub-pillars/sub-chapters/sub-policy in Basel II, may also have rule statements.

Condition: Each rule may have some *Conditions* that describe preconditions required for a rule to be applicable in a particular situation. For instance, rule b of HIPAA's section 164.500 has several conditions. Conditions are sometimes called *Constraints* in legal documents, which represent basically the same concept.

Given the many differences in the structures of various regulations and policies, the Indicator-based Policy Compliance Framework does not impose any specific structural types as long as the document follows the aforementioned hierarchical structure and fits in the metamodel illustrated in Figure 17. Furthermore, stereotypes for GRL intentional elements, identifying various structural names in the document, possibly accompanied by OCL constraints meant to enforce well-formed rules for a given type of document, are used to capture and reason about structures.

Note that other concepts were observed by studying regulations and policies:

Stakeholder: An entity responsible for acting upon policies/rules.

Regulated Types: Some regulation elements are only applicable to specific types of organizations. For instance, some of Transport Canada's policies only apply to specific aerodrome categories (types), for reasons that cannot be disclosed.

Figure 17 formally captures the metamodel of the regulation structures discussed above. IPCF can be applied to the regulations that fit into this structure. The metamodel simply uses a String description to capture the textual content of terms (including rule statements) and of conditions.

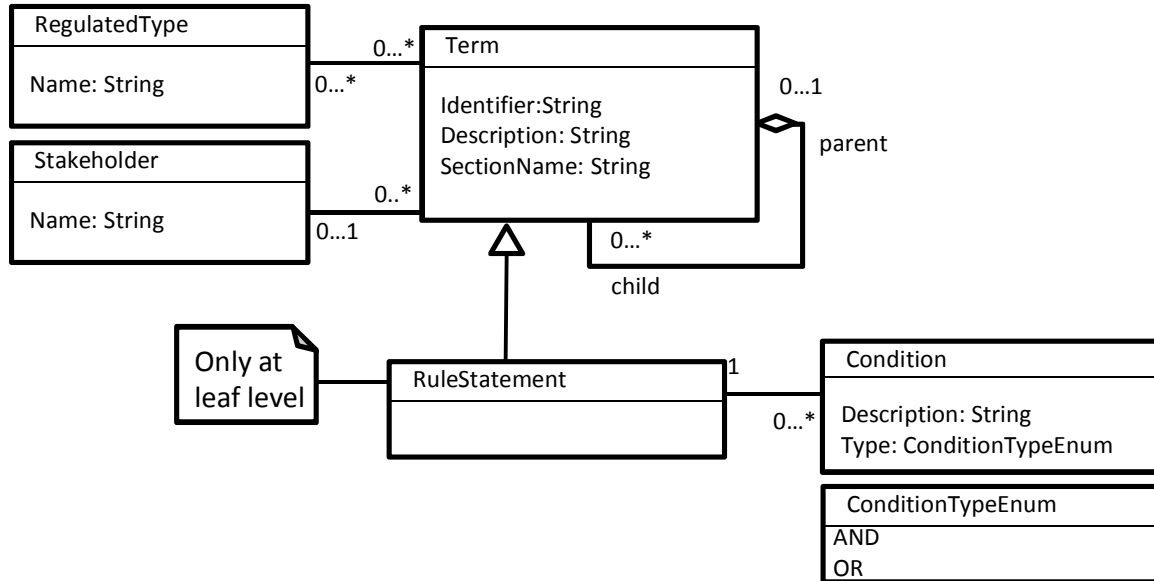


Figure 17, Regulations Structure Metamodel

4.2.2 Procedures to Model Policies/Regulations from Legal Documents

This section identifies the steps for extracting GRL models from regulation and policy documents. Several methods for extracting obligations and rights from legal documents have been proposed in the past. For instance, Breaux *et al.* [22] use semantic parameterization to extract rights and obligations from legal documents. They also propose a new tool (called Gaius T., see [68]) to support their methodology. They conducted two empirical studies to compare the performance of the tool for extracting legal instances (rights and obligations) with manual identification of these instances. However, such approaches are not well suited for the creation of GRL models as required in the Indicator-based Policy Compliance Framework, in part because the latter does not need to extract obligations and rights.

In order to be able to model legal text with GRL, legal *terms* and their relationships should be mapped to GRL modeling elements. A sample example from Canada's

Aeronautics Act [25] related to Emergency Exercises is used to illustrate these steps. The Aeronautics Act consists of different parts (Signs, Access control systems, Emergency plans and procedures, and Baggage handling system, just to name some). Several *rule statements* of Emergency Exercises, shown below, have been selected to illustrate the procedure. The three “schedules” these rule statements refer to are lists of aerodromes not included here.

Emergency Exercises:

- 8.** The operator of an aerodrome listed in Schedule A must, at least once every three years, carry out a live exercise involving the agencies identified in its emergency plan to test the effectiveness of the plan in relation to an act of unlawful interference with civil aviation. The operator of an aerodrome listed in Schedule B or C must carry out a live exercise at least once every five years.
- 9.** The operator of an aerodrome listed in Schedule A, B or C must, at least once a year, carry out a table-top exercise involving the agencies identified in its emergency plan to test the effectiveness of the plan in relation to an act of unlawful interference with civil aviation. However, the operator is not required to carry out a table-top exercise in any year in which it carries out a live exercise in accordance with section 8.
- 10.** The operator of an aerodrome that is not listed in Schedule A, B or C and that is an aerodrome where air carriers are served must, at least once a year, carry out a table-top exercise involving the agencies identified in its emergency plan to test the effectiveness of the plan in relation to an act of unlawful interference with civil aviation.
- 11.** The operator of an aerodrome must prepare a written report on each exercise it carries out in accordance with section 8, 9 or 10 and must make the reports available to the Minister on reasonable notice given by the Minister.” [25]

In order to help with the transformation from the legal text to the GRL model, one can first create an object diagram from the metamodel discussed in Figure 17. This additional step can help describe the legal document formally and reduce the fuzziness of the mapping process. Figure 24 is a subset of the object model (without descriptions, for simplification purpose) that can be created in the context of the aforementioned rule statements. Thereafter, the following steps can be used to create the GRL model.

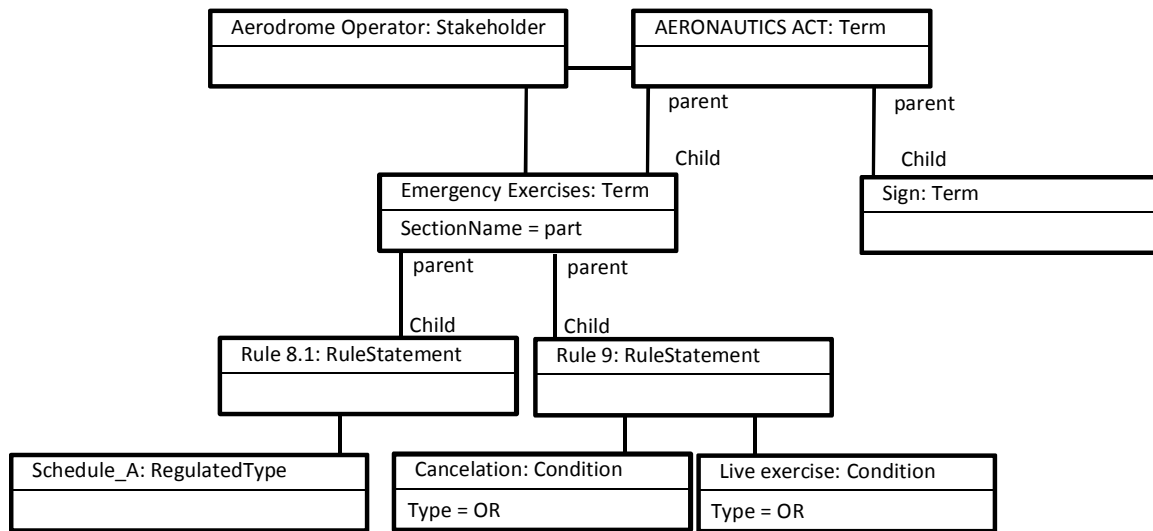


Figure 18, Object Diagram for a Subset of the Guideline Example (Aeronautics Acts)

Legal terms to GRL goals

- 1- All *terms* of legal text are mapped to *GRL goal* elements. For example, in the emergency exercises example (see Table 6), Emergency Exercises and Aeronautics Act will both be mapped to GRL goals.

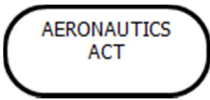
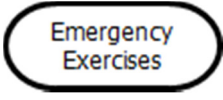
Regulation	URN
AERONAUTICS ACT	
<u>Emergency Exercises</u>	

Table 6, Regulation Modeling, Step 1

Document structure and sections

- 2- Although all hierarchical sections of the legal documents are described with terms in the metamodel (see Figure 17), some legal documents like the one in this example use specific names for terms. In such cases, even though GRL goals are used to model the terms, appropriate *stereotypes* may be used to reflect the structure of the document, as suggested in section 4.2.1. This specific name is captured in meta-model as *SectionName*, which is a property of the *Term*. For example, the three different parts of HIPAA are GRL goal elements that can be tagged with a «*part*» stereotype. While their children terms also become GRL goal elements, they are tagged with a «*subpart*» stereotype. In the Aeronautics Act example, Emergency Exercises can be tagged with a «*part*» stereotype (see Table 7).

Regulation	URN
<u>Emergency Exercises</u>	Emergency Exercises <<part>>

Table 7, Regulation Modeling, Step 2

Note that adding these stereotypes will improve the traceability between the model and documents, while improving the readers' understanding of where in the document structure each modeling element fits. Although legal documents tend to be very structured, GRL models are not inherently hierarchically structured. These stereotypes do not have an impact on the analysis of the model (in terms of compliance assessment) but can be useful to check correspondence between the model and the structural aspect of the source document, or to check relationships between structural information elements in the GRL model (e.g., through OCL constraints).

Document hierarchy

- 3- All the terms of the legal model (captured as GRL goals) that reflect different sections and the hierarchy of the legal and policy documents are connected through *GRL contribution links*, from the more detailed term to the more abstract term. The contribution value of contributions links is, by default, equal to $100 / N$ where N is number of GRL model elements contributing to the target element, see Figure

19 (a). When other terms like Signs, Access control systems and others are added to such model, the contribution value will be divided equally between the elements, i.e., 50 for two contributing elements, 25 for four elements, etc. (see Figure 19 (b)). These default contribution values can be changed if the modeler knows that some contributors weight more than the others. Deciding to choose a different contribution value than the default one is also another part of the process that requires human intervention and is not formalized (this information is not found in legal documents, and experts need to be involved). Different consensus and voting techniques developed in the requirements engineering domain could be used to choose appropriate contribution levels. For example, there could be two contributors where the respective weights are 60 and 40, as shown in Figure 19 (c). Furthermore, if terms are separated by an AND (or an OR) keyword, they should be connected to the parent term through a GRL AND-decomposition link (or a GRL OR-decomposition link) rather than through a contribution link.

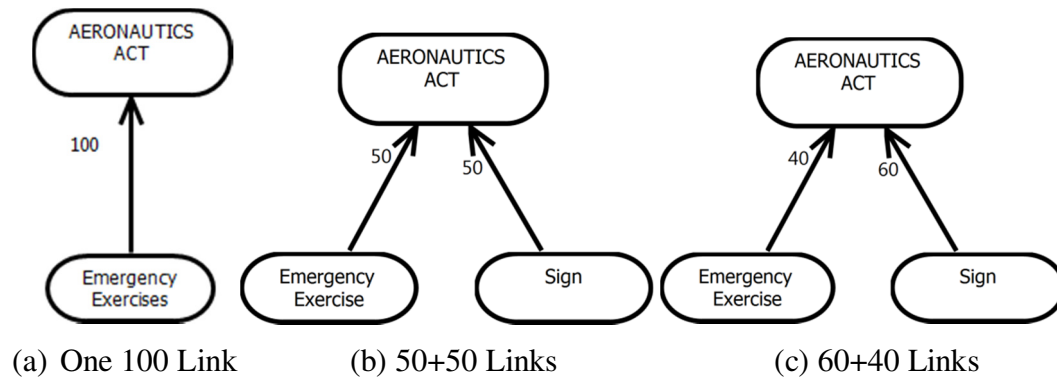


Figure 19, Regulation Modeling, Step 3

Rule Statements

- 4- *Rule Statements* inherit from *Term* and therefore are modeled as *GRL goals*. In the Emergency Exercises example, there are 4 *Rule Statements*, namely Rule 8, Rule 9, Rule 10, and Rule 11. Table 8 illustrates Rule 8 and Rule 9.

Regulation	URN
Rule 8	The operator of an aerodrome listed in Schedule A must, at least once every three years, carry out a live exercise involving the agencies identified in its emergency plan to test the effectiveness of the plan in relation to an act of unlawful interference with civil aviation. The operator of an aerodrome listed in Schedule B or C must carry out a live exercise at least once every five years
Rule 9	The aerodrome operator must at least once a year carry out a table-top exercise involving the agencies identified in its emergency plan to test the effectiveness of the plan in relation to an act of unlawful interference with civil aviation

Table 8, Regulation Modeling, Step 4

Stakeholders

- 5- A Term's *Stakeholder* is mapped to a *GRL actor* (see Table 9, first row). Such actor can contain the legal terms associated with it (see Table 9, second row).

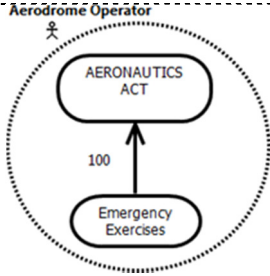
Regulation	URN
Aerodrome Operator	Aerodrome Operator 
Legal terms associated with an actor	Aerodrome Operator 

Table 9, Regulation Modeling, Step 5

Rule variations

- 6- A *Term* can explain variations of the requirement depending on the *RegulatedType*. In this case, instead of modeling the *Term* as one GRL goal, each variation is modeled as a separate GRL goal. As illustrated in Table 10, Rule 8 was initially modeled as one GRL goal according to step 4. However, since this term explains requirement variations for different regulated types (i.e., aerodrome types), two GRL goals are required.

Regulation	URN
Rule 8.1	Carry out a live exercise involving the agencies identified in the emergency plan to test the effectiveness of the plan in relation to an act of unlawful interference with civil aviation at least once every three years
Rule 8.2	Carry out a live exercise involving the agencies identified in the emergency plan to test the effectiveness of the plan in relation to an act of unlawful interference with civil aviation at least once every five years

Table 10, Regulation Modeling, Step 6

Conditions

- 7- A *Rule Statement* can have *Conditions*. A Condition is often documented in legal and policy documents at the Rule level using specific keywords like *if* and *unless*. In that case, the Condition is mapped to a *GRL resource* (see Table 11).

Regulation	URN
Part of Rule 9. However, the operator is not required to carry out a table-top exercise in any year in which it carries out a live exercise in accordance with section 8.	If not carrying out a live exercise in the same year

Table 11, Regulation Modeling, Step 7

- 8- A *Condition* is connected to a *Rule Statement* using a GRL *dependency link*, i.e., the *Rule Statement* is dependent on the *Condition* (see Figure 20).

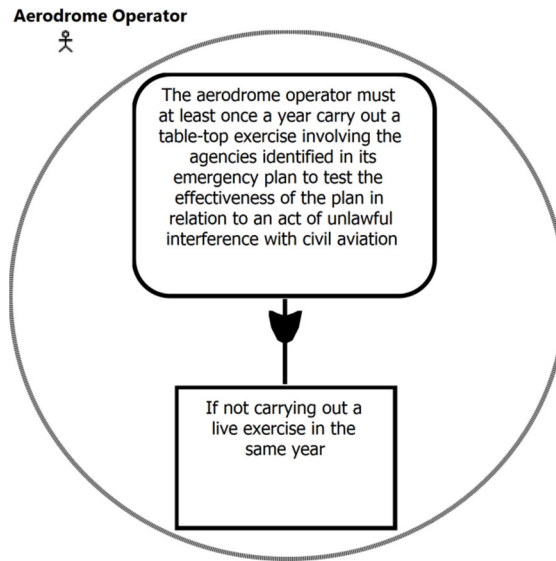


Figure 20, Regulation Modeling, Step 8

- 9- If a *Rule Statement* has more than one *Condition*, an intermediate *GRL resource* is added and connected to the *Rule Statement* first. This intermediate GRL resource is then decomposed into the *Conditions* using either *GRL AND decomposition links* or *GRL OR decomposition links*. Let us assume that another condition is applied to Rule 9, in order to be able to show an example for this step (Figure 22). The following condition is added to the rule:

“However, the operator is not required to carry out a table-top exercise in any year in which it carries out a live exercise in accordance with section 8 or if the table-top exercise is requested to be cancelled by the minister due to budget limitation in the year after the live exercise”

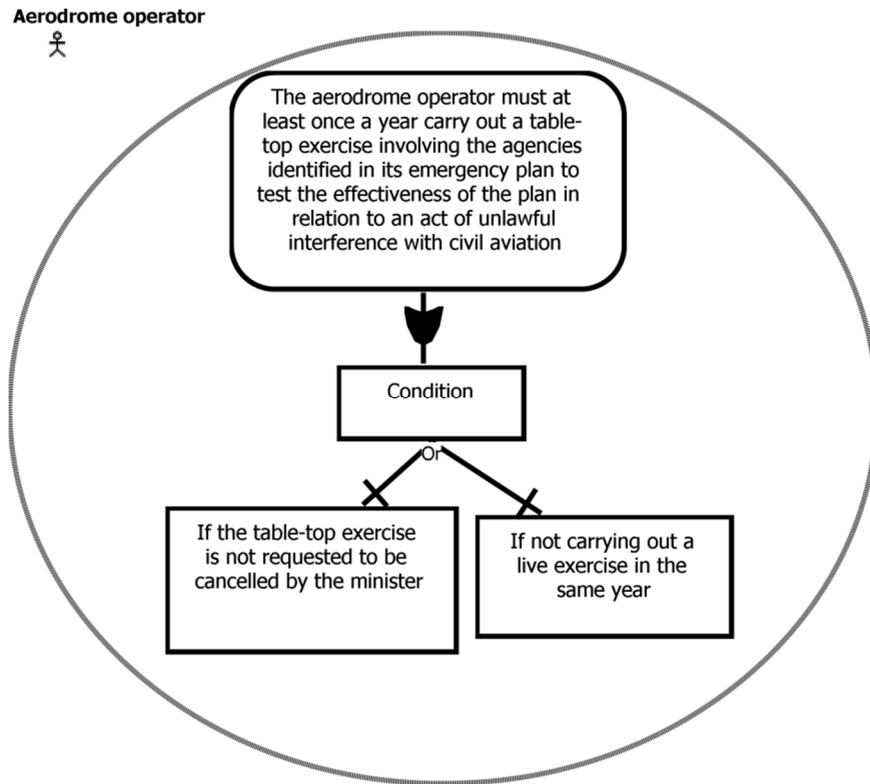


Figure 21, Regulation Modeling, Step 9

10- *GRL stereotypes* are used to distinguish the applicability of a *Term* or *Condition* to different types of organizations (i.e. *Regulated Type*). For instance, if a regulation in general is applied to three types of organizations (Schedules A, B and C), a Term or Condition that only applies to Schedule A organizations is tagged with stereotype «Schedule_A» (See Figure 22). A Term or Condition without any stereotype applies to all Regulated Types. If a Term or Condition is applied to more than one Regulated Type but not to all, it must be tagged with all required stereotypes individually (e.g. «Schedule_A»«Schedule_B»).

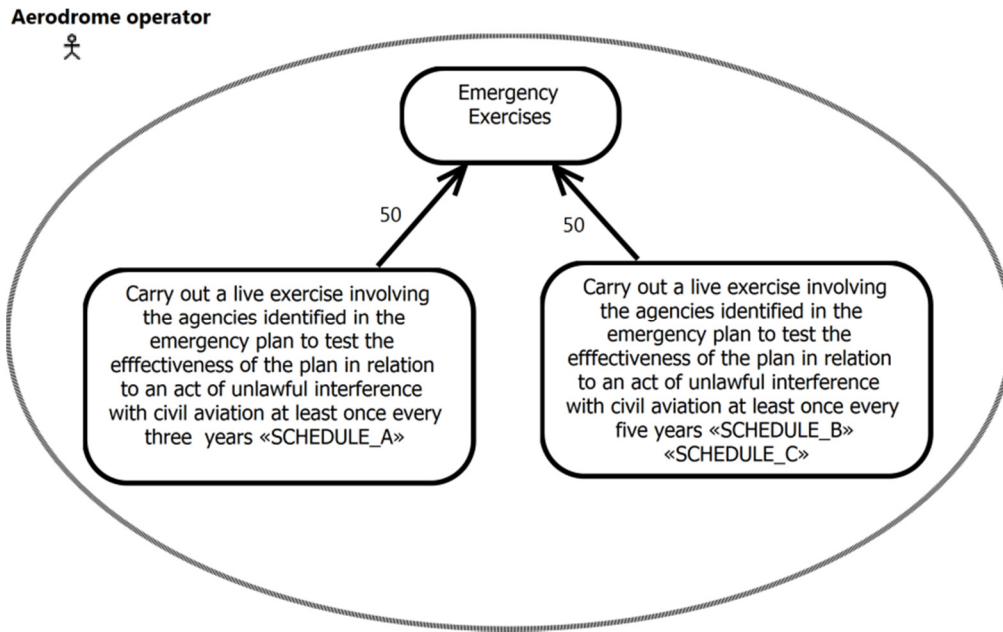


Figure 22, Regulation Modeling, Step 10

- 11- After selecting the appropriate KPIs for measuring the satisfaction level of a *Rule Statement*, a KPI is modeled as a *GRL KPI*. Note that selecting the KPIs is not formalized (as legal documents do not contain indicators), requires human smarts, and is expected to be done by analysts teamed with domain experts.
- 12- A *Rule Statement* can have multiple KPIs.
- 13- A KPI is connected to a target *Rule Statement* using a *GRL contribution link*, and its GRL contribution value is, by default, equal to $100 / N$ where N is the number of KPIs contributing to the target Rule (see Figure 23). Since KPIs are not specifically part of the legal documents, and since they are added to the model as part of IPCF, they do not need to be allocated to actors.

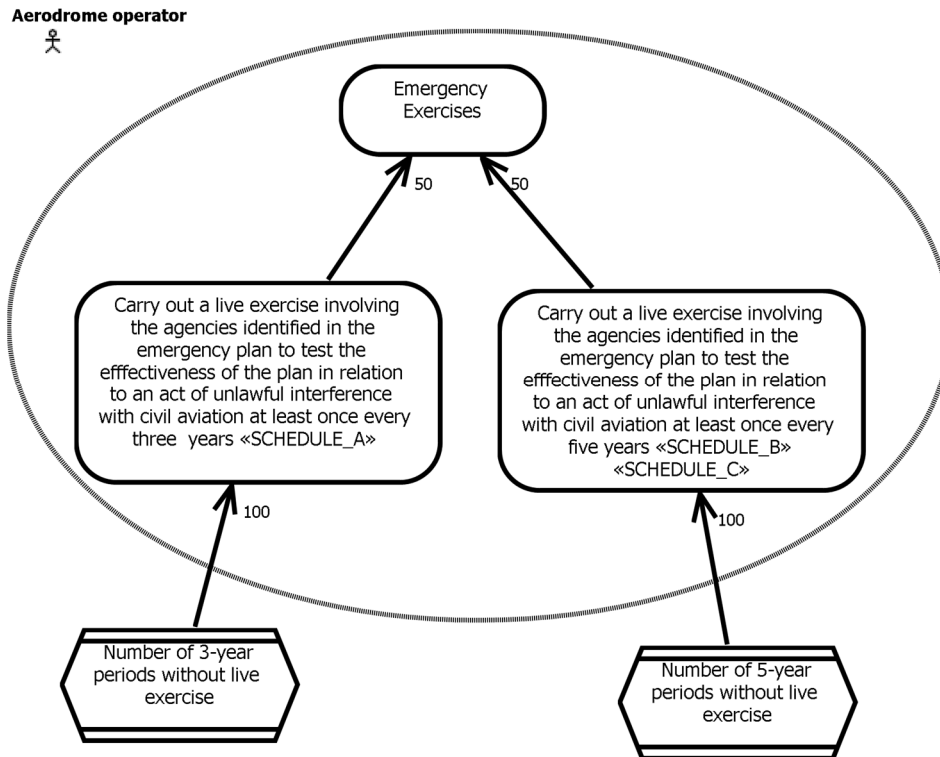


Figure 23, Regulation Modeling, Step 13

In summary, Figure 24 illustrates how the various elements of a regulation document are captured and mapped to a GRL model using the guidelines just presented. Furthermore, Appendix D discusses the relevant subset of the formal GRL metamodel (see Figure 117 and Figure 118). With the guidelines and a formalized legal document (as shown in Figure 17), one can start from a legal document and create the GRL legal model that can be used in IPCF.

Unfortunately, there are still aspects of this modeling procedure that cannot be fully formalized and that require interpretation and human intervention (i.e., finding and connecting suitable KPIs as well as determining contribution levels between terms connected by a parent-child relationship). The required information to automate this is absent from regulation and policy input documents.

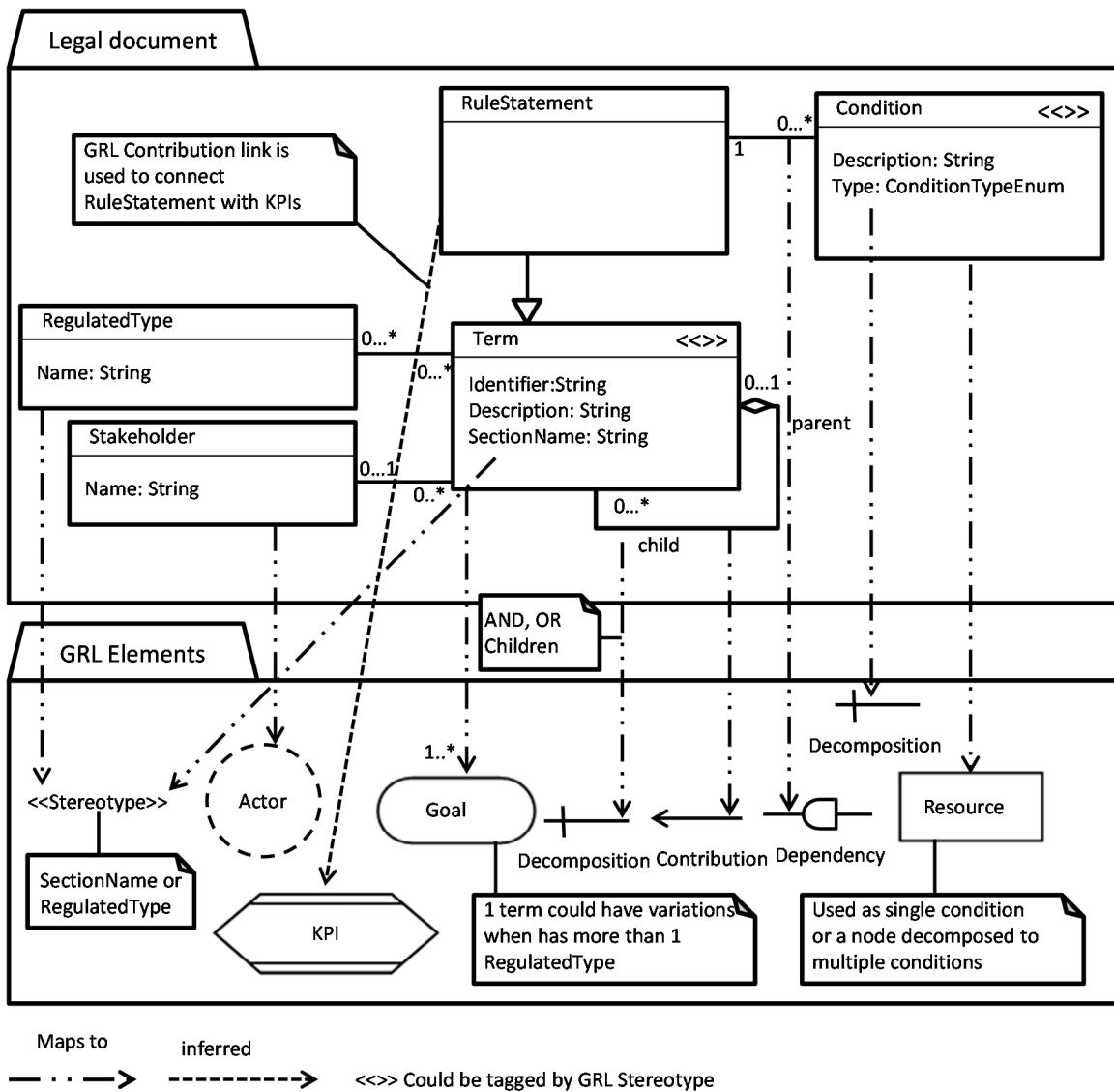


Figure 24, Mapping regulation metamodel to GRL model elements

4.2.3 Optimization Steps

The accuracy of the procedure discussed in section 4.2.2 was evaluated in an informal exercise by six people working for a regulator or studying at the University of Ottawa. They used the procedure to model specific parts of a sample public regulation. After reviewing the models produced in collaboration with the participants, several suggestions were received and helped improve the procedure and its guidelines. In particular, optimization steps were missing in the guidelines and the procedure just presented may not re-

sult in an optimized GRL model, as it may reflect badly structured regulations. Therefore some optimization steps are hence possible.

- 1- Term's children and Conditions may be decomposed with logical keywords (i.e., AND or OR). However, if the data captured by different Term's children or Conditions have a similar meaning (e.g., the same KPI is used to measure them), then they should be modeled with one single GRL goal rather than different GRL goals.
- 2- A Rule Statement may not be measurable. For example, its main purpose might be to give some guidelines or indicate some legal intent, without really being enforceable. Such a Rule Statement may be discarded from the GRL model, since it will not be part of the analysis. However, if the modeler wishes to keep the GRL model in line with the structure of the regulation (for traceability and completeness), the Rule Statement can be kept in the GRL model but excluded from the analysis by marking it with the stereotype «No».

Example

Another example from part 7 of Aerodrome regulations, which explains all the rule statements that a screening authority shall use for screening equipment, is illustrated in this section. Since the content of this regulation is not public, only the structure and the keywords that enable us to extract a GRL model are explained. In this part of the regulation one of the rules has the following structure:

“A screening authority shall use screening equipment unless X or Y and:

- (a) Condition a;
- (b) Condition b;
- (c) Condition c and;
- (d) Condition d.”

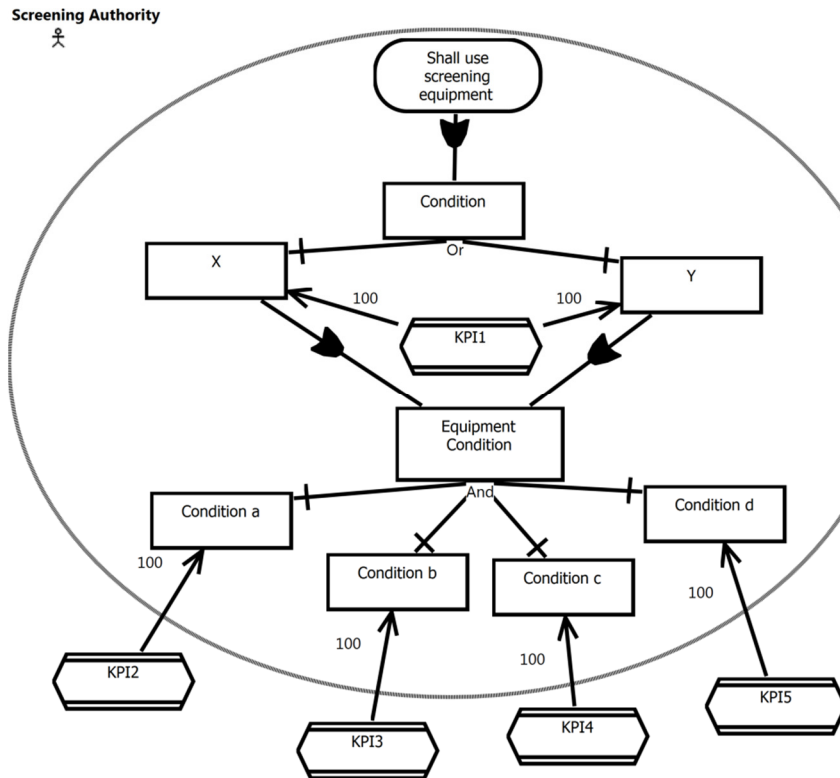


Figure 25, Extracting GRL models from legal documents, sample example

Figure 25, illustrates a first attempt at mapping this rule to a GRL model. After reviewing the model and going through the optimization steps, one could observe that condition X and condition Y are both measured using the same KPI and depend on the same condition. Therefore, they can be combined as one Condition. Figure 26 illustrates an optimized version of the model.

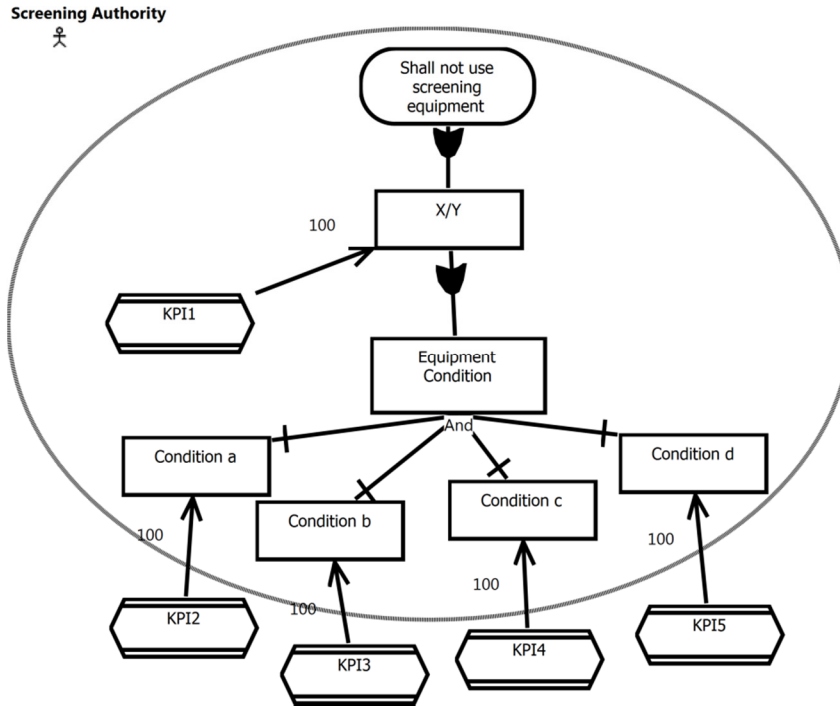


Figure 26, Optimized Sample Example

4.3. Step B: Evaluation

This step evaluates the model to find the overall compliance level of the organization with respect to one or multiple policies. This assessment is performed using the model designed according to the procedure in Step A combined with GRL strategies, often used to initialize the leaf elements of GRL models in order to compute the satisfaction level of the higher-level elements using a bottom-up propagation algorithm [6]. In this application, GRL strategies initialize the KPI value sets (i.e., target value, threshold value, worst value, and evaluation value). An evaluation value is the actual value of a KPI at the time of the evaluation. The evaluation values can be entered manually like other value sets (which is useful for the analysis of what-if situations) or automatically obtained from various data sources such as a Business Intelligence (BI) systems. A GRL KPI maps the evaluation value to a satisfaction level (on a scale from -100 to 100 , by linear interpolation considering the target, threshold, and worst values) that can then be propagated to other elements (rules, policies) in the goal model according to the goal evaluation algorithms presented in [6]. In addition, to find the compliance level of the organization with

respect to one or multiple policies, the satisfaction level of different stakeholders before performing any process modifications is determined. Therefore, the analyst initializes the KPI value sets that affect the organization goals to measure the satisfaction levels of different stakeholders.

In order to find out how organizations can select the most important compliance issues to be addressed given their limited resources, the importance values of the high-level business goals must be defined to ensure the compliance issues related to business processes supporting important and strategic goals of organizations are addressed first. The importance values are propagated, using a top-down importance algorithm, to business processes and associated policies/rules through the URN links, as illustrated in Figure 27. There might be situations where a rule is not connected to any business process (see for example section 6.2.2). In that case, since rules get their importance values from business processes, these importance values are set to 1 by default. In situations where a goal is linked to multiple business processes, the importance value is propagated equally to the associated processes.

As part of this approach, to calculate importance levels, an extra Business actor containing an extra Successful business softgoal with an importance value of 100 is added to the organization model. The algorithm calculates the importance for other intentional goals using their contribution links. Importance values are propagated down from high-level goals to business processes and rules according to the following formula. One assumption is that the intentional element for which the *Importance* is computed is the source of n contributions ($Contrib_1$ to $Contrib_n$) to other intentional elements.

$$Importance = \sum_{i=1}^n \frac{Contrib_i.Target.Importance \times Contrib_i.ContributionLevel}{n \times 100}$$

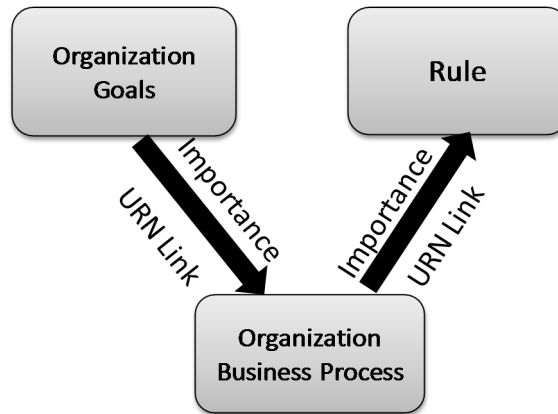


Figure 27, Importance Value Propagation

The importance algorithm calculates an initial importance value for each intentional element. These numbers can always be updated or overridden by analysts. In some regulations, the consequences that violating a rule can have can be captured, including financial penalties, loss of reputation, lawsuits, and even imprisonment. In that case, those rules can become more important and therefore their importance values can be increased.

Finally, these values are used to lay out the rules on a *quadrant diagram* based on compliance and importance levels. As illustrated in Figure 28, each rule is located in one of four quadrants. The axes of this quadrant view are the compliance and importance levels of the rules. This quadrant view allows analysts to *identify what is the most important rule that the organization is not compliant with*. The rules falling into the quadrant with high importance and low compliance levels have priority over other rules and will be likely improvement candidates, whereas rules in the quadrant with low importance and high compliance levels have the lowest priority. Using URN links, one can track down the associated business processes to those rules. Such information enables decision makers to more easily prioritize the improvement candidates for the improvement step. The y axis indicates the importance value that can be between 0 and 100. However, the maximum and minimum value of the y axis will be dynamic, depending on the importance value of the current rules. The top value represents the highest importance value of the rule.

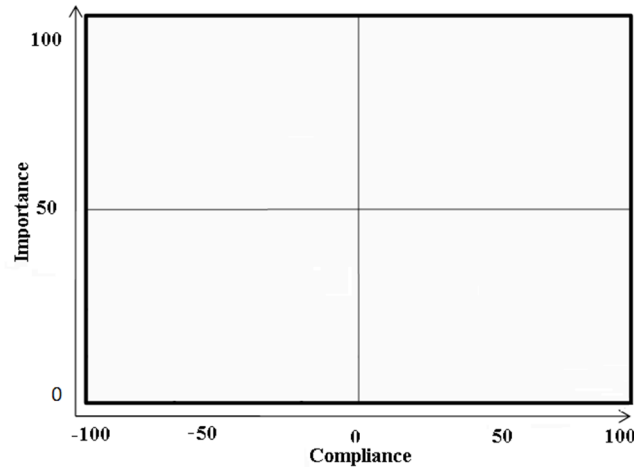


Figure 28, Rules Quadrant Diagram

4.4. Step C: Improvement

In this step, the analyst improves the business processes that are highlighted in the quadrant diagram based on their importance and level of compliance. In addition to improving business processes, it is also important to check whether the modifications meant to fix one problem affect negatively the compliance against other rules/policies and also the satisfaction of organization goals. Obviously, improving one business process does not always have a positive impact on other business processes. This evaluation can be done again with GRL strategies, through which one can simulate many what-if situations.

In addition to improvements to business processes, side effects on high-level organization goals and risks related to business process modifications need to be identified. For instance, modifications can improve business process compliance but they might increase the overall cost. A decision maker can evaluate whether it is worthwhile to improve the compliance level with such associated increase in costs.

4.5. Step D: Monitoring

The objective of the monitoring step is to observe whether the expected changes related to the modified processes are really happening, and to detect potential side effects on organization goals and compliance levels of other control rules in the organization. The set of KPIs that are defined in the modeling step and initialized in the evaluation step for

organization goals and compliance levels of other control rules should be monitored before (in the evaluation step) and after the process improvement, in order to be able to analyze the impact of business process modifications for improving compliance on the organization goals and policies. If the results are not the ones expected, corrective actions should be taken. If the results are satisfactory, then decision makers can move on to improve other prioritized processes. Updating the models to better reflect reality is also an option to consider at this point; the initial model may not have been good enough to support the previous decisions.

Note that KPI monitoring related to business processes and organization goals after process modifications requires real data, as well as a specific time period. However, due to lack of real data, the actual monitoring step of the IPCF cannot be taken into account in this thesis. Therefore, sample GRL strategies will be created to predict or assume the effect of process modifications on organization goals as well as on the compliance level of the organization. In fact, in this step, IPCF also support the analysis of different what-if scenarios.

4.6. Summary

This chapter gave an overview of the Indicator-based Policy Compliance Framework (IPCF) and described its inputs, outputs, and compliance steps. IPCM first requires the URN-based modeling of organization goals, business processes, policies and rules. A metamodel was introduced to formalize the structure of input legal documents, which are transformed to GRL models according to a set of guidelines. URN links are used to associate related business goals to business processes and policies. Then, the satisfaction level of each policy and its importance level are evaluated. The satisfaction level of different stakeholders before any process modifications is also evaluated. GRL strategies are used to initialize KPI values and evaluate the satisfaction level of policies and stakeholders. The improvement step helps determine, based on the results of the previous step, what business processes to improve to reach a higher compliance level while taking other organization objectives into consideration. Finally, the compliance and goal KPIs are monitored for predicting, observing and reacting to the changes. The models themselves are

improved as discrepancies between what-if evaluations and real observations are discovered.

The next chapter will illustrate IPCF through an academic but realistic case study in the human resource management domain.

Chapter 5. Human Resource Case Study

In this chapter, the compliance method of the Indicator-based Policy Compliance Framework is further illustrated using a case study. This case study focuses on a human resource policy described on the HRdownloads website [54] and replicated in Appendix B for convenience. There are about 50 policies listed on this website (e.g., Company Travel Policy, Hiring Policy, and Lieu Time Policy). The focus of this chapter is mainly on the Hiring Policy.

5.1. Step A: Modeling

This step is concerned with providing the inputs required for performing the analysis, including modeling the organization business process and goal models and associating business processes to related goals through URN links. In addition, policies and their rules, together with links between rules and related business processes, are modeled.

5.1.1 Organization Business Process Model

The Hiring Process is modeled using the UCM notation. This process, illustrated in Figure 29, has two actors: Hiring Manager and Human Resources (HR). It is also composed of three sub-processes modeled using UCM stubs with plug-ins: Confirm job, Interview internal candidates and Interview external candidates (see Figure 30 and Figure 31). Since the sub-processes for interviewing internal external candidates are very similar, only one of them is shown here.

The hiring process starts when a Hiring Manager determines the need for a new job position and discusses the job description and salary with the Human Resource (HR) department. HR employees are responsible for job confirmations, as illustrated in Figure 30. Depending on whether the department can actually afford any other employee, a new

job is confirmed or cancelled. Upon successful confirmation, it is HR's responsibility to advertise the job description internally for a week.

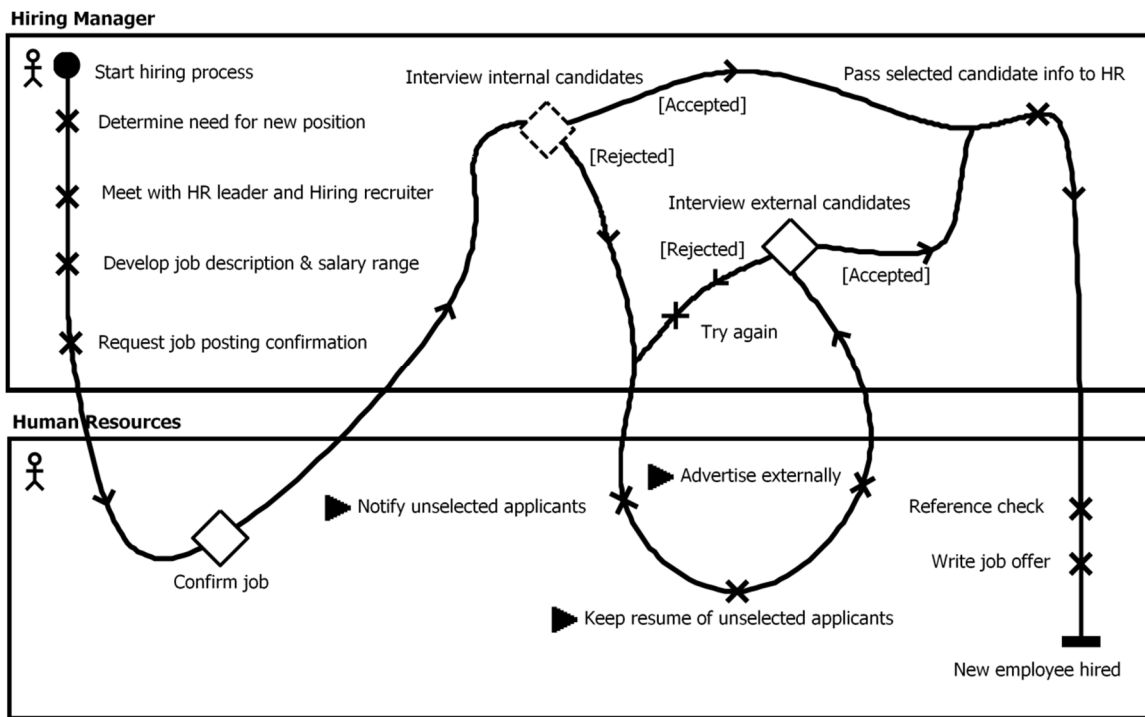


Figure 29, Hiring Process

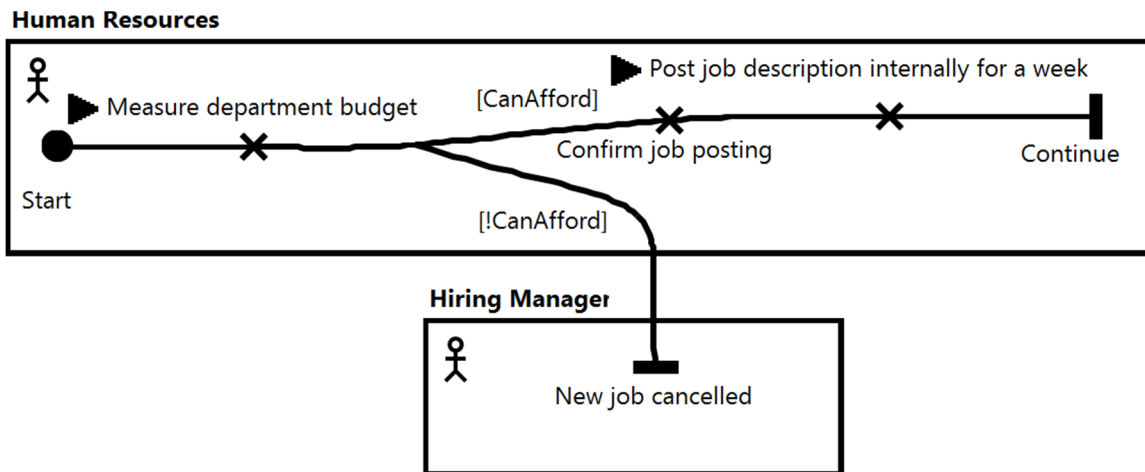


Figure 30, Confirm Job Sub-Process

Interviews are scheduled with internal candidates by the Hiring Manager (Figure 31). Selected internal candidates are interviewed by the Hiring Manager. If no internal candidate is qualified, then Human Resources are responsible for notifying the candidates and

keep their resume. Then, HR advertises the job externally and the Hiring Manager schedules interviews with external candidates until a successful candidate is hired.

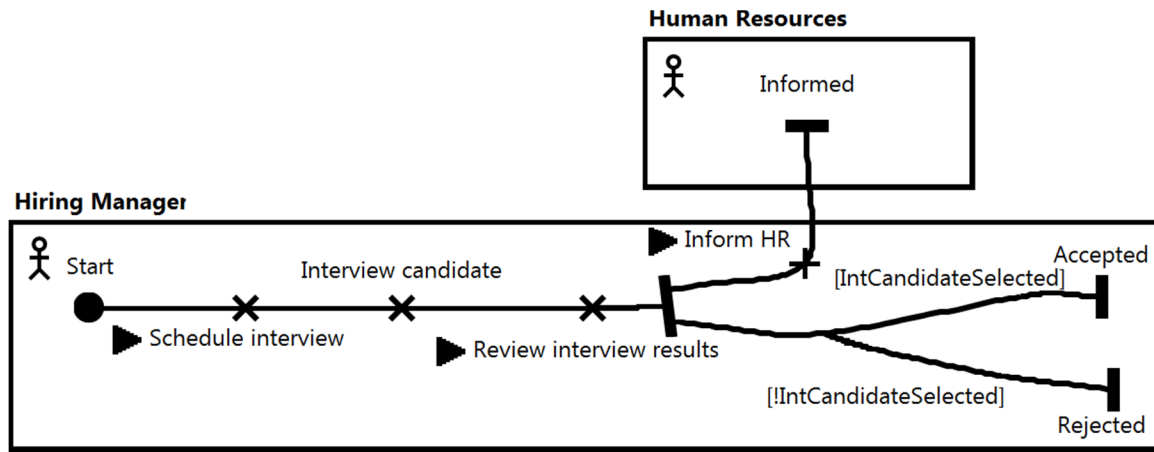


Figure 31, Interview Internal Candidates Sub-Process (As-Is)

5.1.2 Organization Business Goal Model

The organization's high-level goals are also modeled. This view is useful for analysts to know the context and better prioritize the processes and rules according to the organization's objectives. There are three types of actors involved in the organization: Hiring Manager, HR Manager, and Employees. In addition, an extra Business actor is added as part of the method for calculating the importance level, which is elaborated on further in section 5.2.

This step starts by the modeling of the various intentional elements contributing to a successful business. As indicated in Figure 32, five softgoals that affect the Successful Business softgoal are identified. All these softgoals are assumed to be equally important and all required for complete satisfaction. Therefore, they are all connected to Successful Business with quantitative contributions of 20. Numbers between parentheses inside each softgoal represent their importance levels.

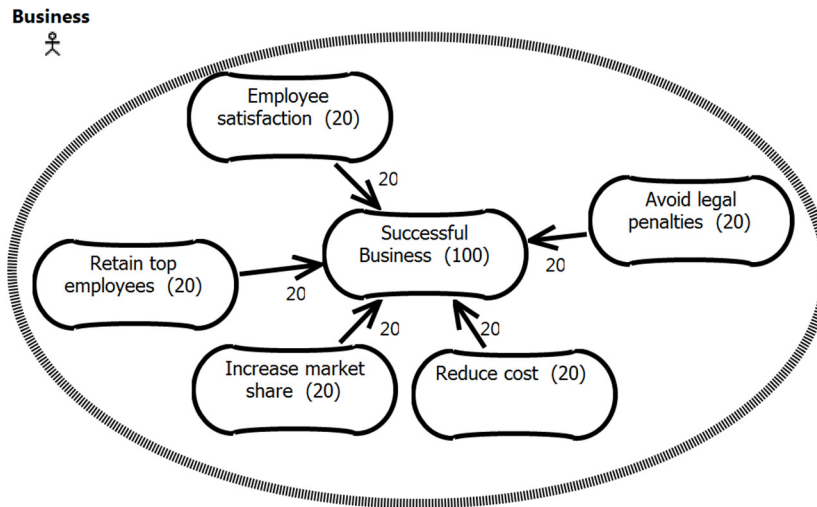


Figure 32, Business High-level Goal Model

Next, the goals of the different stakeholders (actors) that are involved in the organization and their impacts on the goals of an extra Business actor is modeled. Figure 33, Figure 34, and Figure 35 show the goals of the actors Employees, Hiring Manager and HR Manager, together with their contributions to Successful Business. Figure 21 describes that Employees would like to Work with managers they know and Change project once a year. These two softgoals are assumed to have contribution weights of 75 and 25 respectively on Employee satisfaction, which has a contribution level of 20 on Successful Business.

Then, several KPIs are defined to help analyze the impacts of the changes made to business processes for improving the compliance level on the organization goals. For instance, in order to measure the softgoal “Change project once a year”, the indicator “Number of projects involved in last 2 years” is used, where the target value is greater or equal to two, and the worst value is one.

URN links between the UCM diagrams and the GRL graphs, created using jUCMNav, are indicated by triangles next to labels on the graphical models (see Figure 34). For instance, there is a traceability link from the Employment equality softgoal in the Hiring Manager (Figure 34) to the Schedule interview responsibility in the Interview Internal Candidates sub-process (Figure 31). There is also a traceability link from the Meet

hiring budget targets softgoal in the Hiring Manager (Figure 34) to the Measure department budget responsibility in the Confirm Job sub-process.

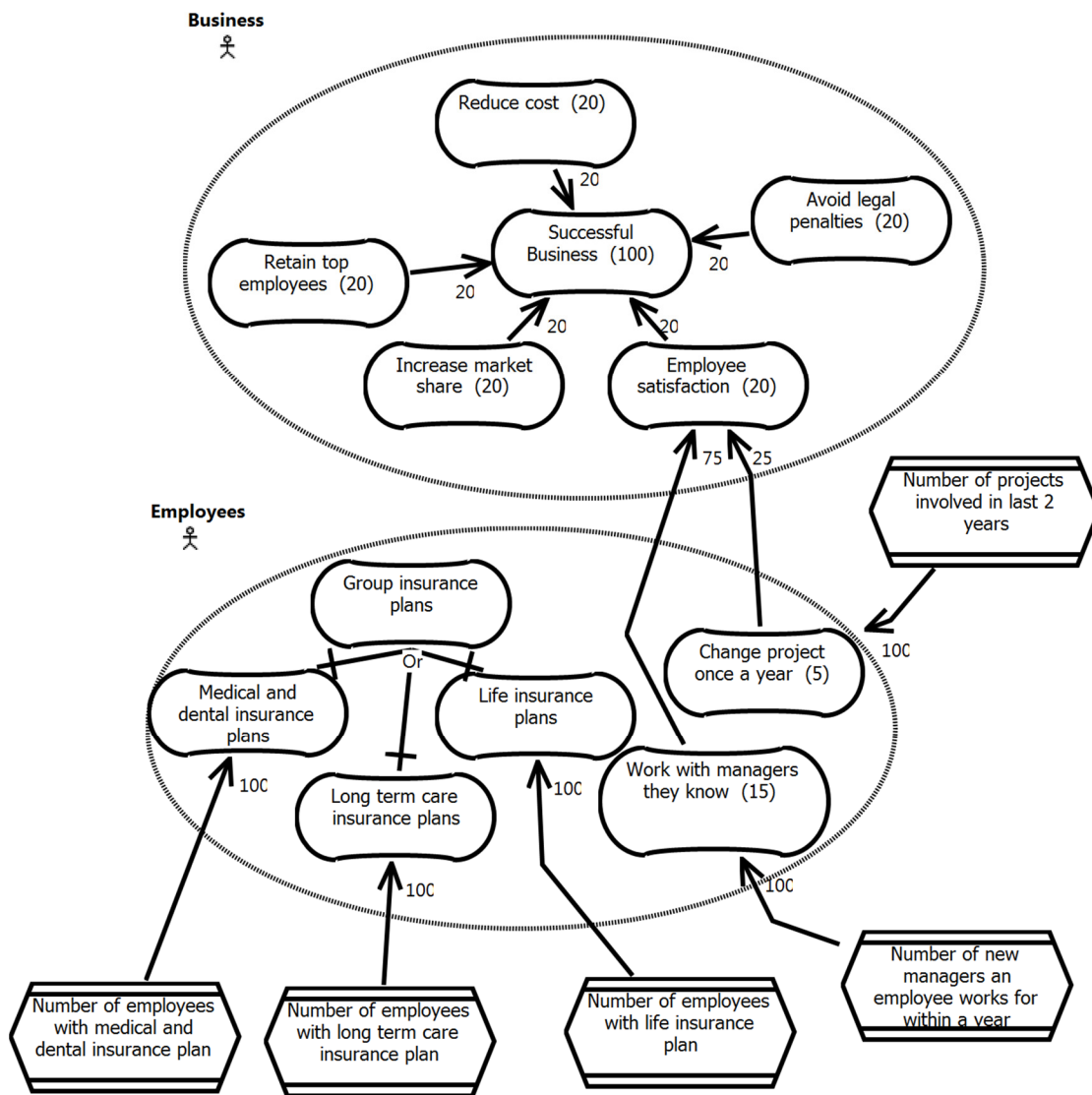


Figure 33, Employees' Business Goal Model, with Impact on Business Goals

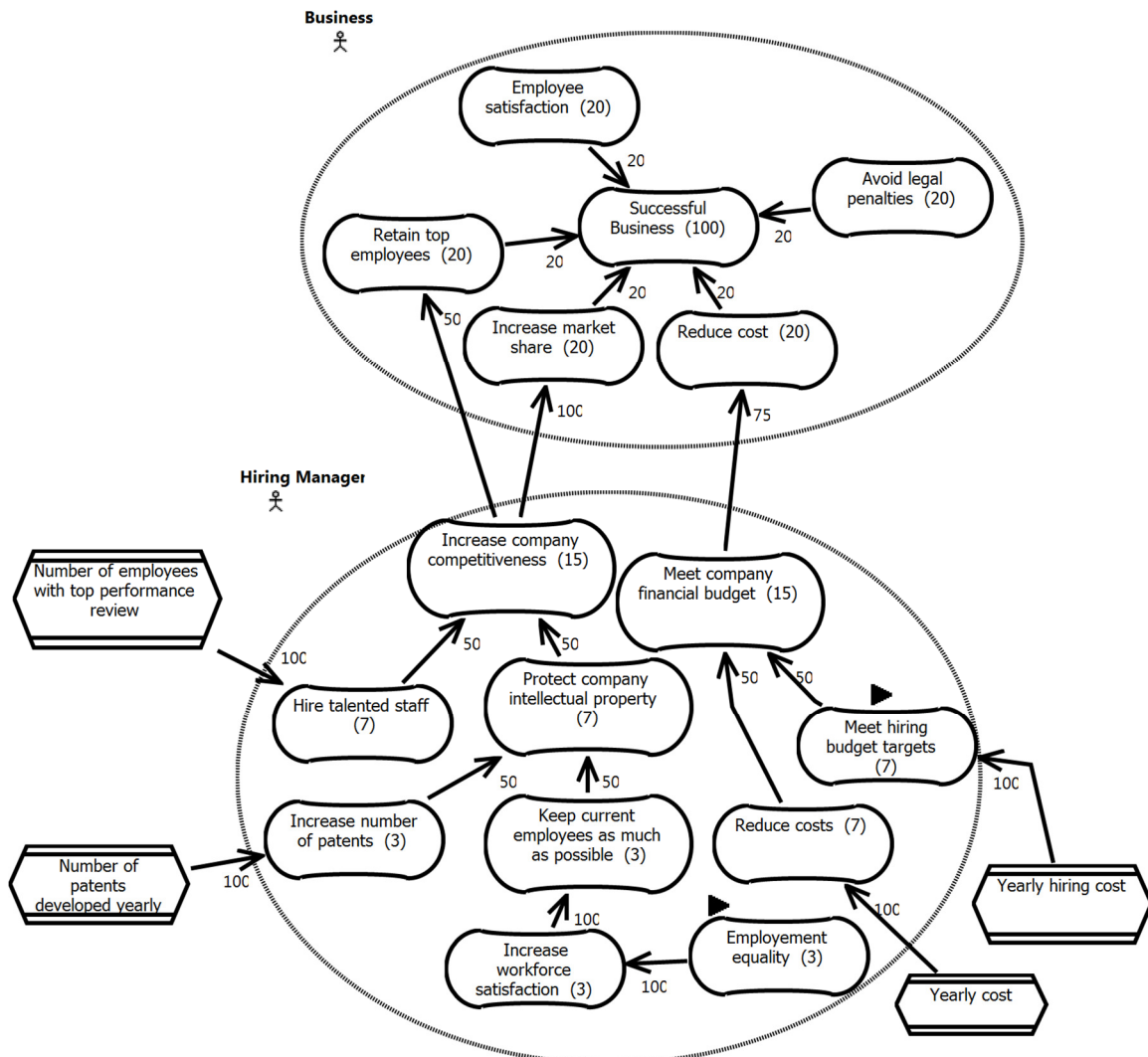


Figure 34, Hiring Manager's Business Goal Model, with Impact on Business Goals

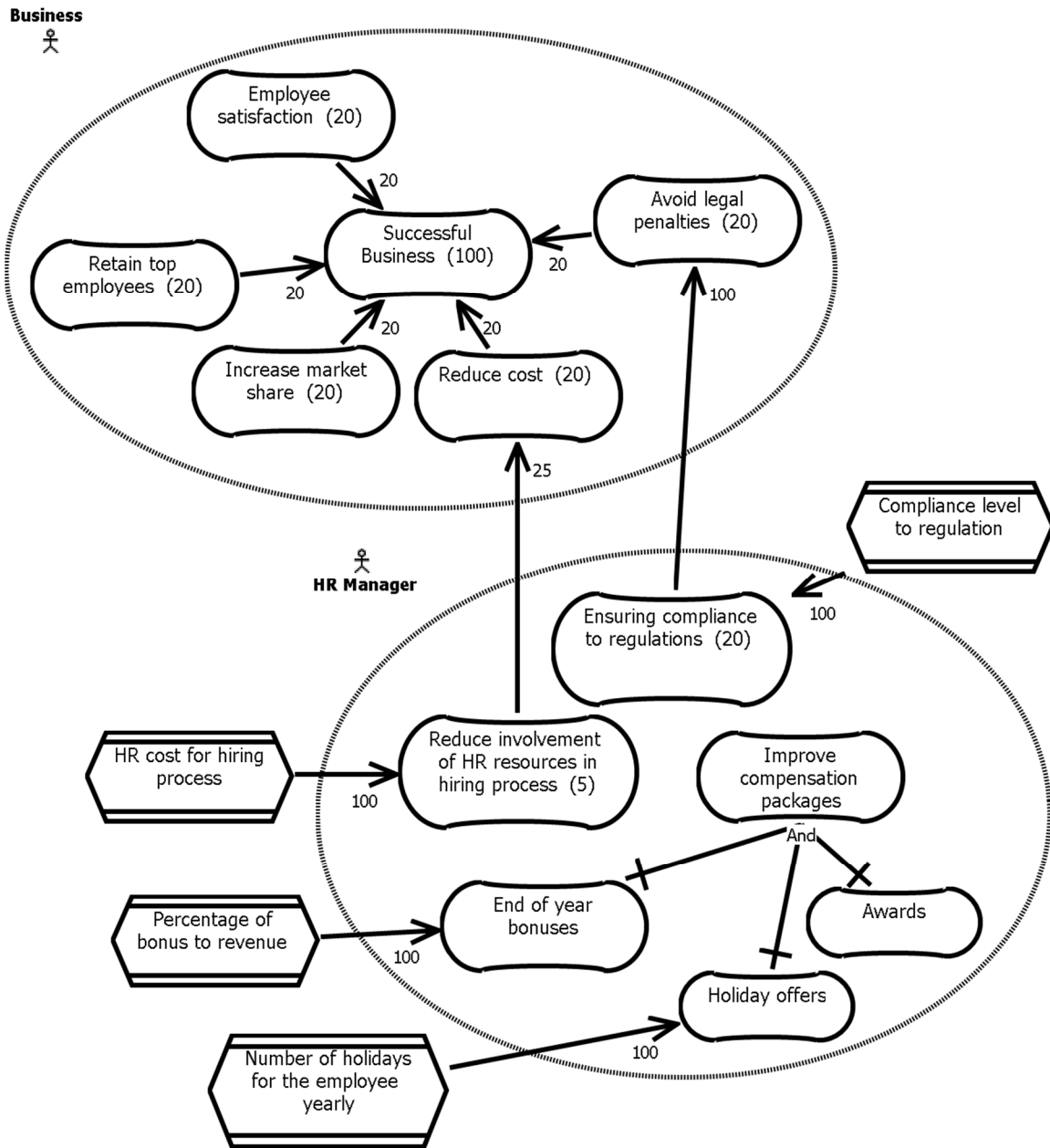


Figure 35, HR Manager’s Business Goal Model, with Impact on Business Goals

5.1.3 Policy Model

Next, policies are modeled with GRL according to the guidelines defined in the previous chapter. As illustrated in Figure 36, five sub-policies for HR Policy are modeled: Internet Acceptable Use, Workplace Health and Safety, Hiring, Performance Review, and Absenteeism Attendance. The assumption is that all sub-policies to have an equal impact on HR Policy, and hence the contribution links total weight (100) will be divided equality

between all five sub-policies. Therefore, each sub-policy has a contribution link with a weight of 20. This case study focuses on the Hiring policy, and only sub-policies for this policy are modeled. There are six sub-policies related to Hiring: Job Posting, Internal Transfers, References & Background Check, Offer of Employment, Interviews and Application Process. Again, all sub-policies are assumed to have about the same impact on the Hiring policy; one of the sub-policies' weight is 15 while the other sub-policies have a weight of 17 (for a sum of 100).

The modeling of sub-policies is continued until one reaches the rule level. Figure 37 shows two sub-policies for Job Posting, namely Internal Job Posting and External Job Posting. Two rules apply here to each sub-policy, and an identifier is assigned to each rule (R1 to R4, shown within comment boxes). These identifiers are used to reference the rules in the rest of this document. Finally, KPIs are defined for each rule. Table 12 gives the list of KPIs and rules.

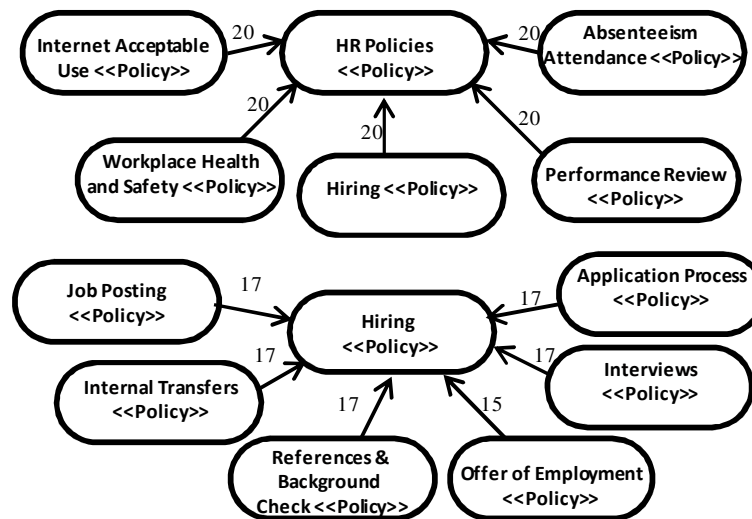


Figure 36, Sub-policies for Human Resources (top) and Hiring (bottom)

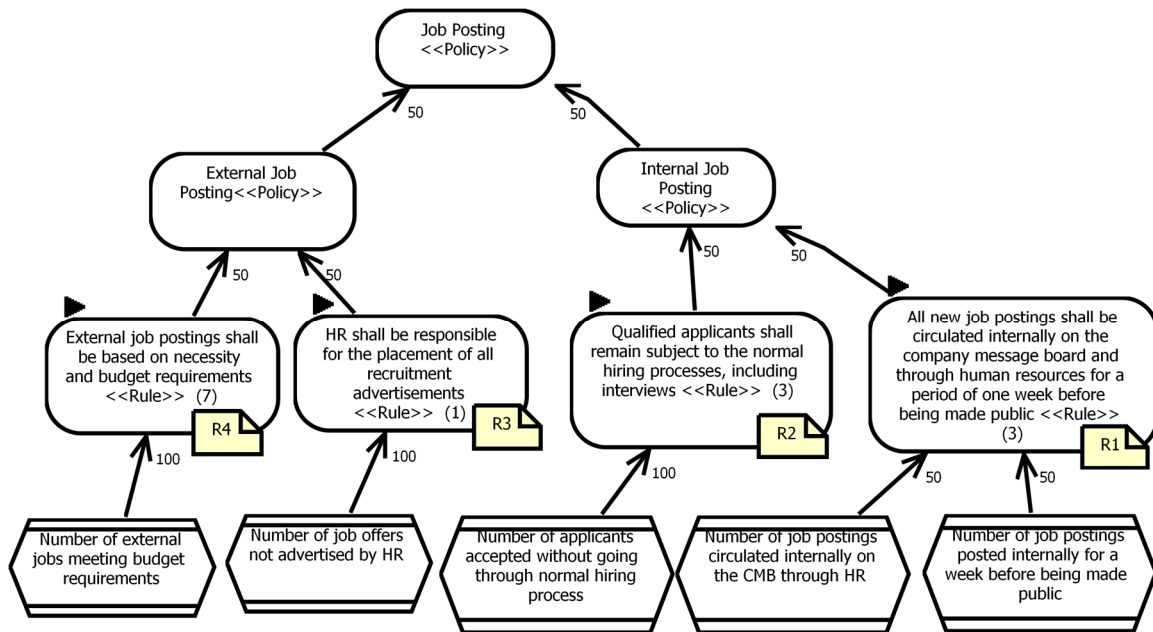


Figure 37, Rules and Key Performance Indicators for Job Posting

Rule	Key Performance Indicator
R1	Number of job postings circulated internally on the CMB through human resources
	Number of job postings posted internally for a week before being made public
R2	Number of applicants accepted without going through normal hiring process
R3	Number of job offers not advertised by human resources
R4	Number of external jobs meeting budget requirements

Table 12, Job Posting Rules and KPIs

Finally, traceability URN links between the rules from the policy model and processes (or process steps) from the organization business process model are created manually with jUCMNav, as specified in Table 13.

Business Process (or Step)	Rule
Measure department budget	R4
Post job description internally for a week	R1
Advertise externally	R3
Interview internal candidates	R2

Table 13, Mapping between Business Processes and Job Posting Rules

Next, the Interviews policy is modeled. As Figure 38 shows, there are four rules that apply here. An identifier is assigned to each rule (R5 to R8) for reference in the rest of the thesis. Then, KPIs are defined for each rule (except for R5, for which the organization does not have a reliable data source in this example). Table 14 illustrates the list of KPIs and rules.

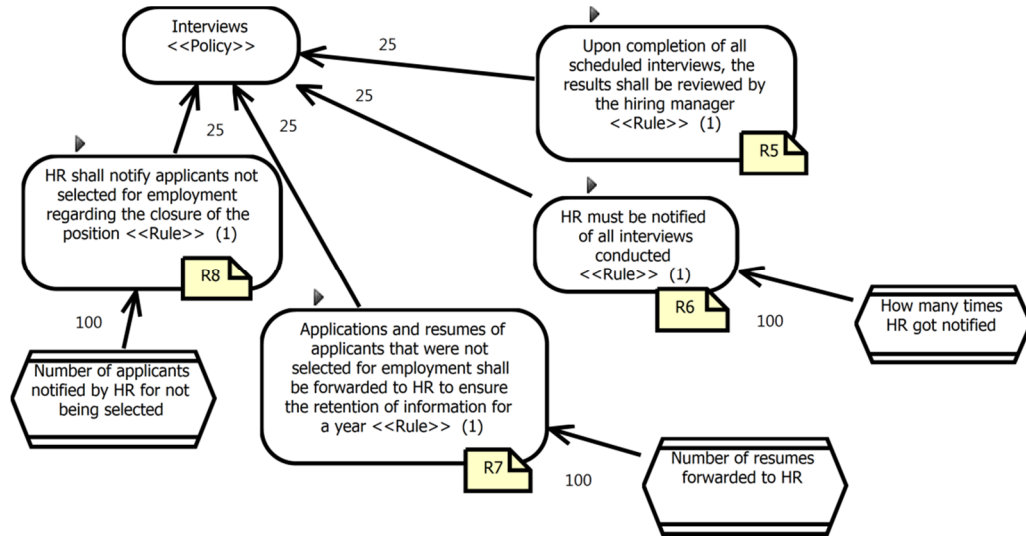


Figure 38, Rules and Key Performance Indicators for Interview

Rule	Key Performance Indicator
R5	None
R6	How many times HR got notified
R7	Number of resumes forwarded to HR
R8	Number of applicants notified by HR for not being selected

Table 14, Interview Rules and KPIs

Again, traceability URN links between the rules from the policy model and the business process model are created manually with jUCMNav, as specified in Table 15.

Business Process (or Step)	Rule
Review interview results (Figure 31)	R5
Inform HR (Figure 31)	R6
Keep resume of unselected applicants (Figure 29)	R7
Notify unselected applicants (Figure 29)	R8

Table 15, Mapping between Business Processes and Interview Rules

Since the Interviews policy is dealing with some retention policies regarding applications and resumes of applicants, and since some regulation and guidelines for record retention already exist, it becomes important to model these regulations in order to be able to assure there are no conflicts between internal policies of the organization and existing regulations and guidelines. Therefore, relevant retention guidelines of the government of Canada are modeled [76].

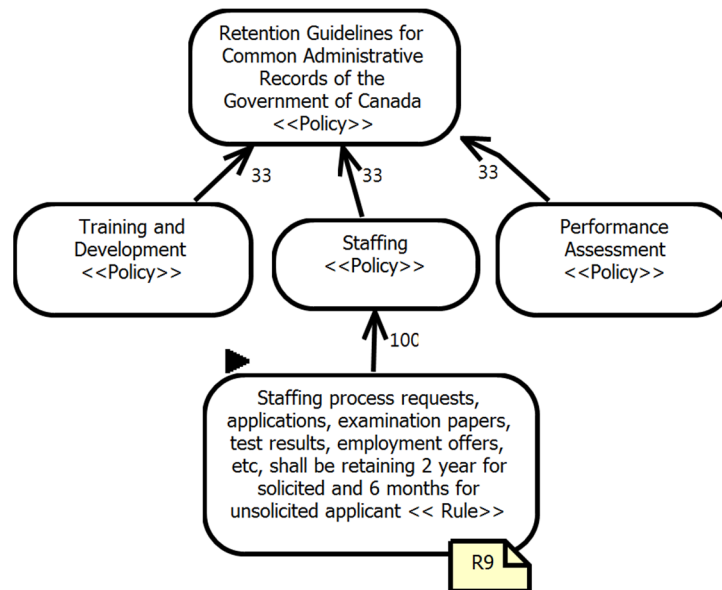


Figure 39, Retention Guidelines, Government of Canada

Table 16 shows the single link between the Retention Guidelines policy model and the business process model.

Business Process (or Step)	Rule
Keep resume of unselected applicants (Figure 29)	R9

Table 16, Mapping between Business Processes and Retention Guidelines Rules

5.2. Step B: Evaluation

In this step, GRL strategies are defined to evaluate the satisfaction level of policies/rules and the algorithm to evaluate importance levels of policies/rules is elaborated. The evalu-

ation results on a quadrant diagram based on satisfaction and importance levels are illustrated.

5.2.1 Evaluation of Satisfaction Levels

GRL *strategies* are used to evaluate the satisfaction level of policies and rules. As discussed in section 4.3, each GRL strategy initializes the KPI value sets [107]. In this case study, it is assumed that the company advertised for 10 new positions in a year. As explained in section 5.1, it is the responsibility of Human Resources to advertise for job offers based on the department's budget. All accepted applicants should go through the normal hiring process.

Target, Threshold, Worst, and Evaluation values for KPIs are defined in a sample strategy ("BeforeModificationtoHiringProcess"), as shown in Figure 40 and Table 17. These values are entered manually to initialize the KPI value sets in jUCMNav (see Figure 40). Each KPI evaluation value is mapped to a GRL evaluation level for each KPI [107]. These values are used to evaluate the satisfaction level of the other intentional elements as illustrated in Figure 41, using the standard quantitative evaluation algorithm supported by GRL and jUCMNav [6]. For instance, one KPI is defined for R2, "Number of applicants accepted without going through normal hiring process". It is expected that all applicants go through the normal hiring process. Therefore, the Target and Threshold values are both set to 0. The Worst value would be set to 10, meaning that all the new employees were hired without going through the normal hiring process. Finally, it is assumed that only 7 new employees went through the normal hiring process in the last year, the Evaluation value is set to 7.

Figure 41 illustrates the policies, sub-policies, rules and KPIs for the HR Policy. Figure 42 and Figure 43 highlight, in larger diagrams, the two main halves of Figure 41. As shown in Figure 43, the satisfaction level for HR Policies is 78, and Hiring Policy has the lowest satisfaction level among all sub-policies. Among Hiring Policy's sub-policies, Job Posting is the least satisfied with a value of 9. This policy is further divided into two sub-policies: Internal Job Posting, with a satisfaction level of -23, and External Job Post-

ing, with a satisfaction level of 41. Finally, among the 4 rules, R2 has the lowest satisfaction level (-70) and R3 has the highest satisfaction level (50).

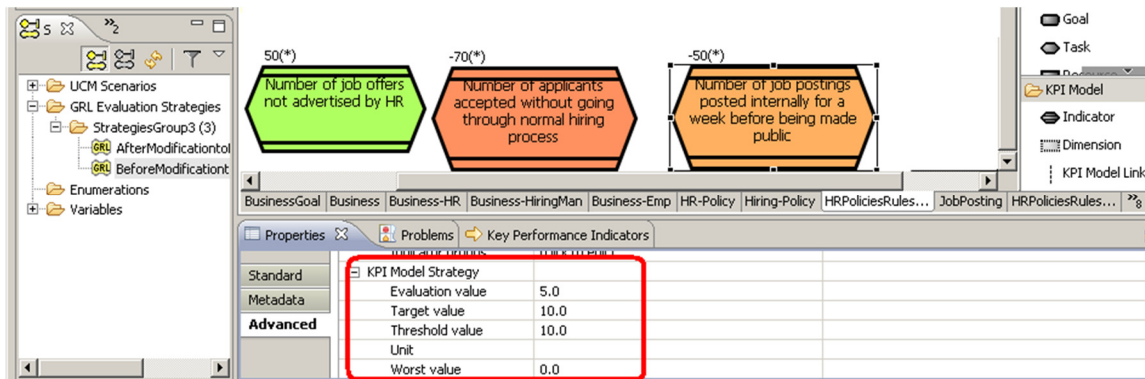


Figure 40, Initializing KPIs in jUCMNav

Rule	Key Performance Indicator	Target	Threshold	Worst	Evaluation
R1	Number of job postings circulated internally on the CMB through HR	10	10	0	10
	Number of job postings posted internally for a week before being made public	10	10	0	5
R2	Number of applicants accepted without going through normal hiring process	0	0	10	7
R3	Number of job offers not advertised by HR	0	2	10	1
R4	Number of external jobs meeting budget requirements	10	7	0	9
R5	<i>None (satisfaction level initialized at the rule level directly)</i>	-	-	-	-
R6	How many times HR got notified	50	42	0	44
R7	Number of resumes forwarded to HR	40	37	0	39
R8	Number of applicants notified by HR for not being selected	40	40	0	40

Table 17, List of KPIs and Value Sets for Rules

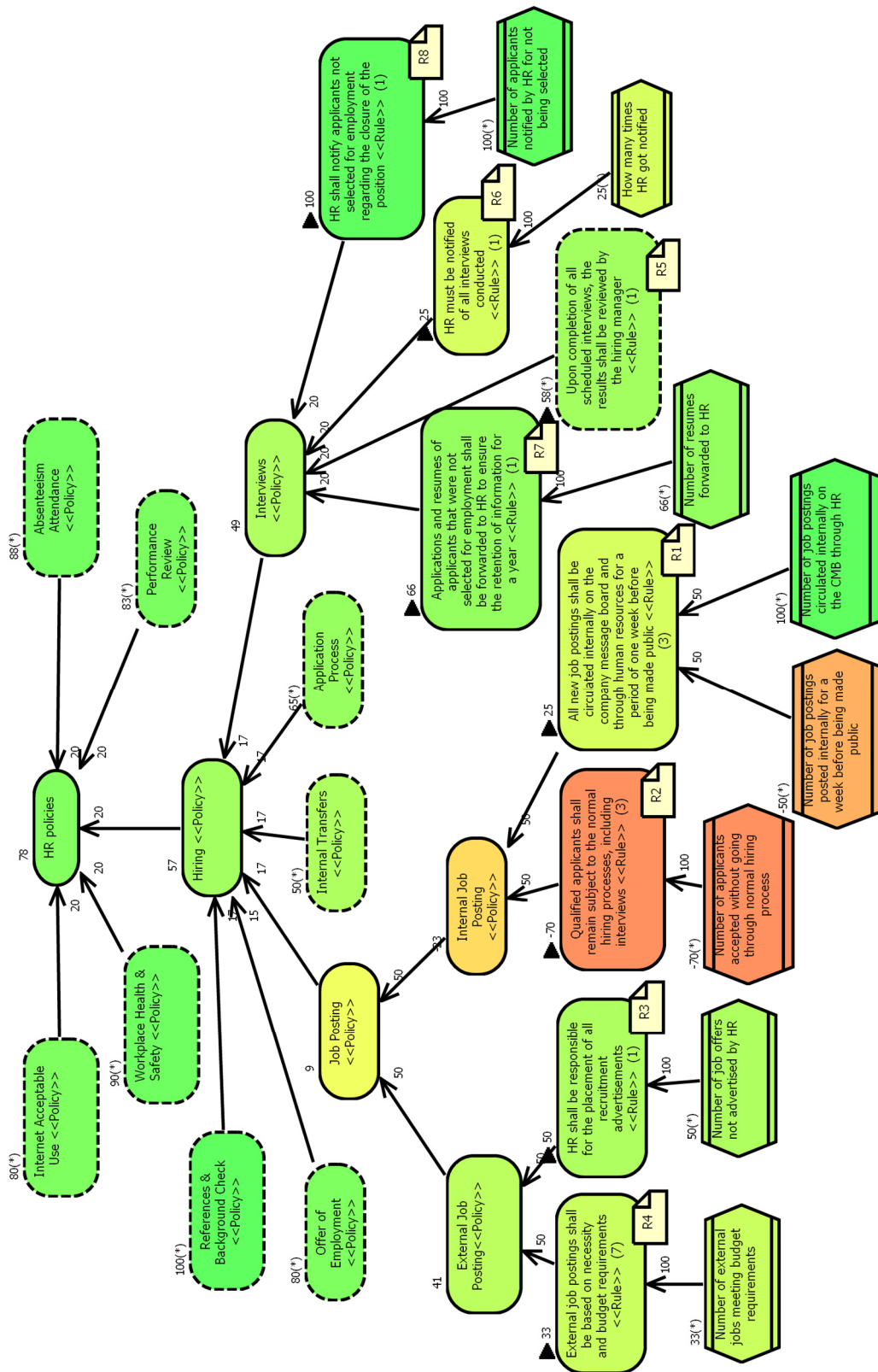


Figure 41, Policy and Rule Satisfaction Level

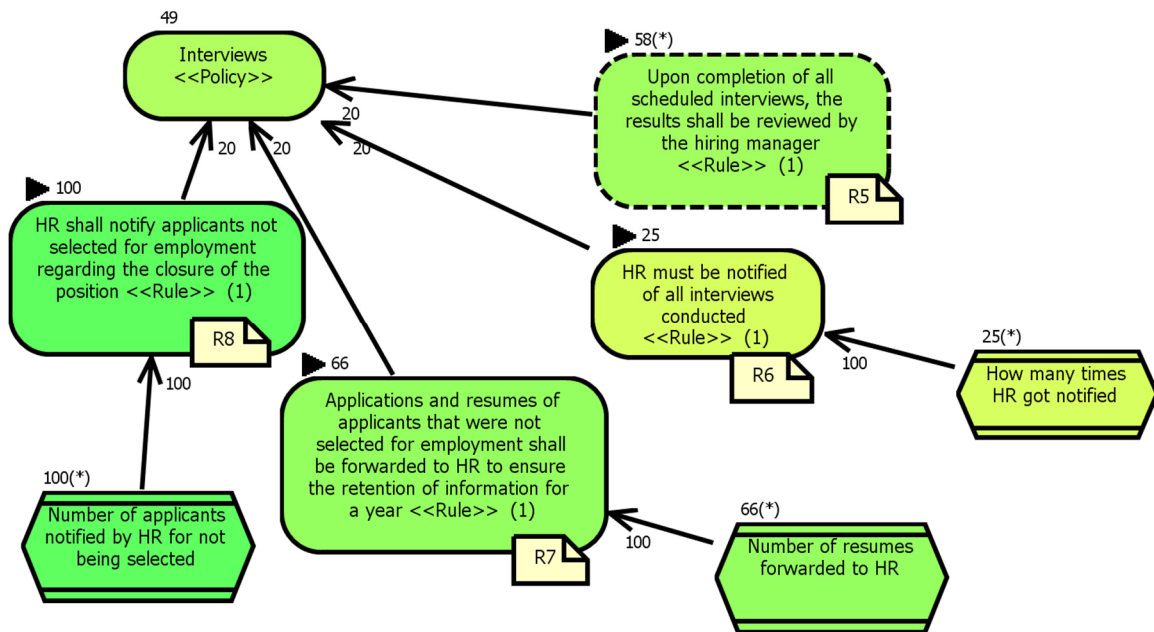


Figure 42, Interview Policy Satisfaction Level

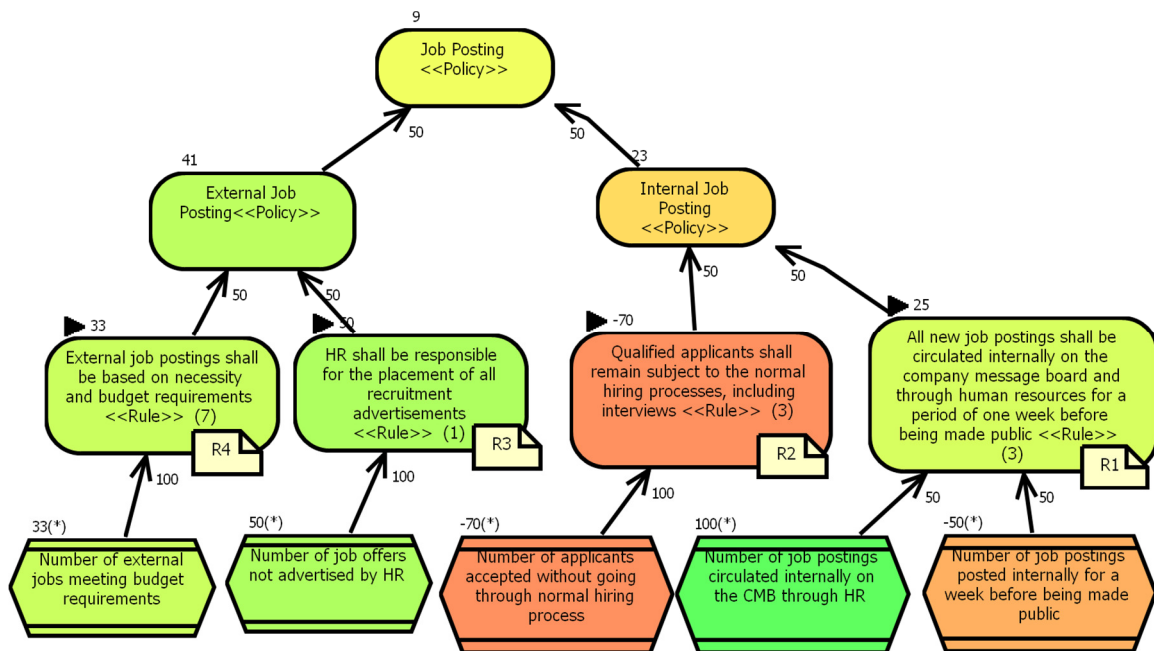


Figure 43, Job Posting Policy Satisfaction Level

5.2.2 Evaluation of Importance Values

In addition to satisfaction levels, the importance values of GRL intentional elements need to be evaluated in the model. As explained in chapter 4.3, an importance algorithm is used to calculate the importance level of intentional goals, business processes and rules.

For instance (see Figure 44), the importance value of rule R4 is 7. This value is propagated all the way down from Successful Business, which is the highest-level business goal (Figure 34) and is initialized with an importance value of 100. The importance of each source intentional element that contributes to a given target intentional element is proportional to both the importance level of the target and the weight of the element's contribution. For example, Reduce Cost is one of the Successful Business goals with a contribution level of 20. Therefore the importance value of this goal becomes $100 \times 20 / (100 \times 1) = 20$. This goal is connected to Meet company financial budget through a contribution link with a contribution level of 75. Consequently, the importance value of this intentional element becomes $20 \times 75 / (100 \times 1) = 15$. This goal is connected to Meet hiring budget targets and Reduce costs with contribution levels of 50. Hence, the importance value of these intentional elements becomes $50 \times 15 / (100 \times 1) = 7$. Integer values are used here, and no importance value can be less than 1.

The above importance value (7) is propagated to the responsibility Measure department budget, and then to rule R4, through URN links. The importance value of R1 and R2 (i.e., 3) is propagated all the way down from Employment equality. This value is propagated to Post job description internally for a week and Interview internal candidates, which are linked to R1 and R2 respectively through URN links. For the rules that do not get any value through this algorithm, a default importance value of 1 is given. For instance, all the rules related to the interview policy have an importance value of 1 (Figure 42), since they are not mapped to any organization goal.

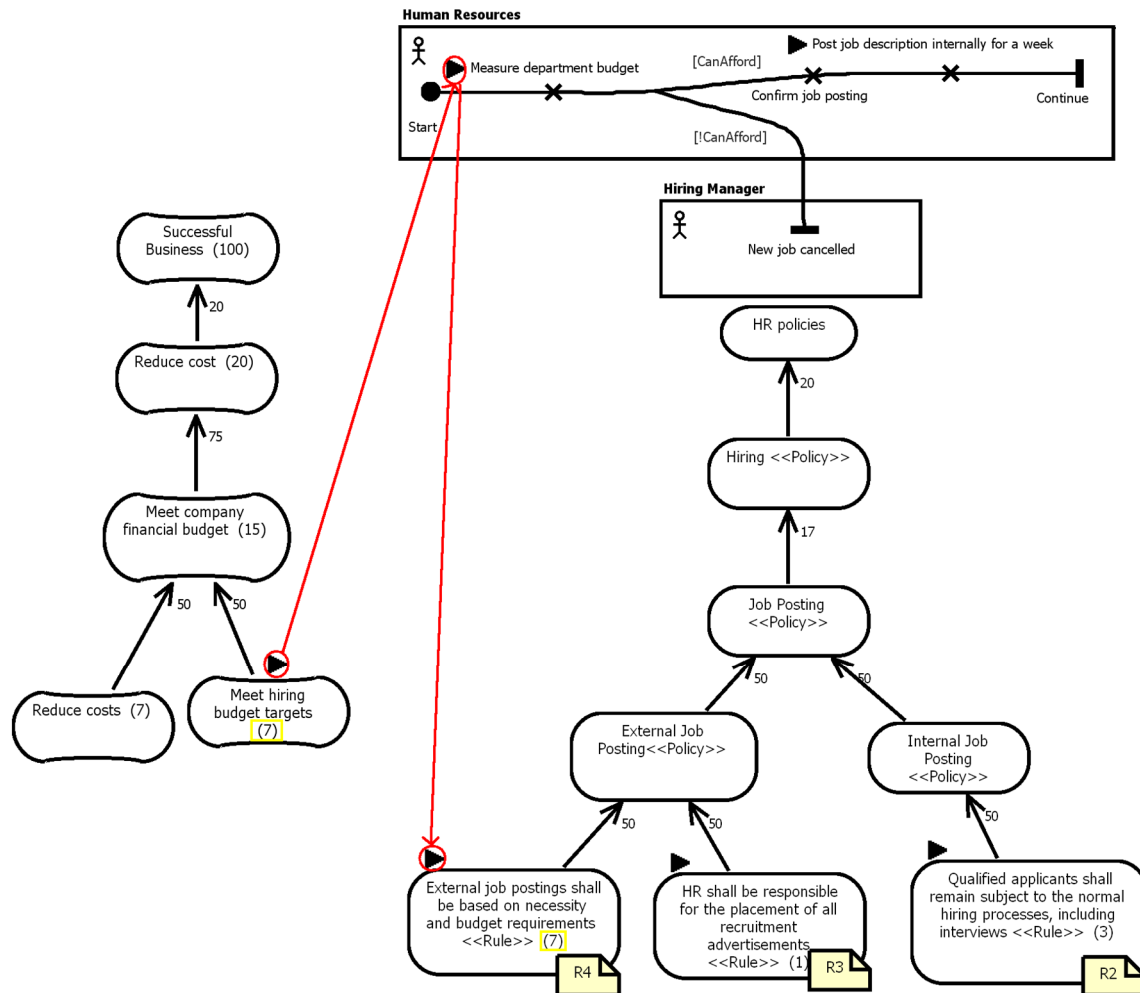


Figure 44, Importance Value Propagation from Business Goals to Rules

5.2.3 Importance/Compliance Quadrant Diagram Representation

Satisfaction and importance value are used to lay out the rules on a quadrant diagram. This quadrant allows one to *identify what are the most important rules with the lowest level of compliance*. This will allow the people in charge to easily prioritize the improvement candidates.

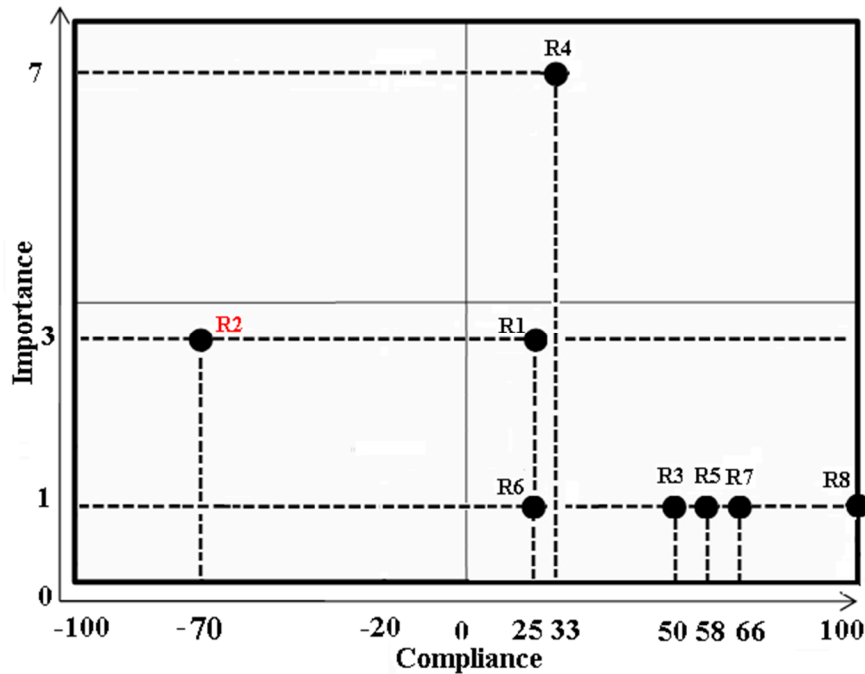


Figure 45, Importance and Compliance of Rules on a Quadrant Diagram

The business processes will be improved based on the results of the quadrant diagram in the Improvement step, to be presented in the next section. However, in order to be able to determine the impact of compliance-related process modifications on business goals of different stakeholders, the satisfaction levels of different stakeholders are determined before performing any process modification. Therefore, Key Performance Indicators are used to measure the satisfaction level of different stakeholders. These KPIs are illustrated in Figure 46, Figure 47, and Figure 48. The KPIs Target, Threshold, Worst and Evaluation values are described in Table 19. After providing these values to the model, the standard quantitative evaluation method is used to evaluate the satisfaction level of stakeholder goals. As a result, Employees (Figure 46), HR Manager (Figure 47), Hiring Manager (Figure 48) and the extra Business actor (Figure 49) have satisfaction levels of 87, 77, 32 and 49 respectively (Table 18).

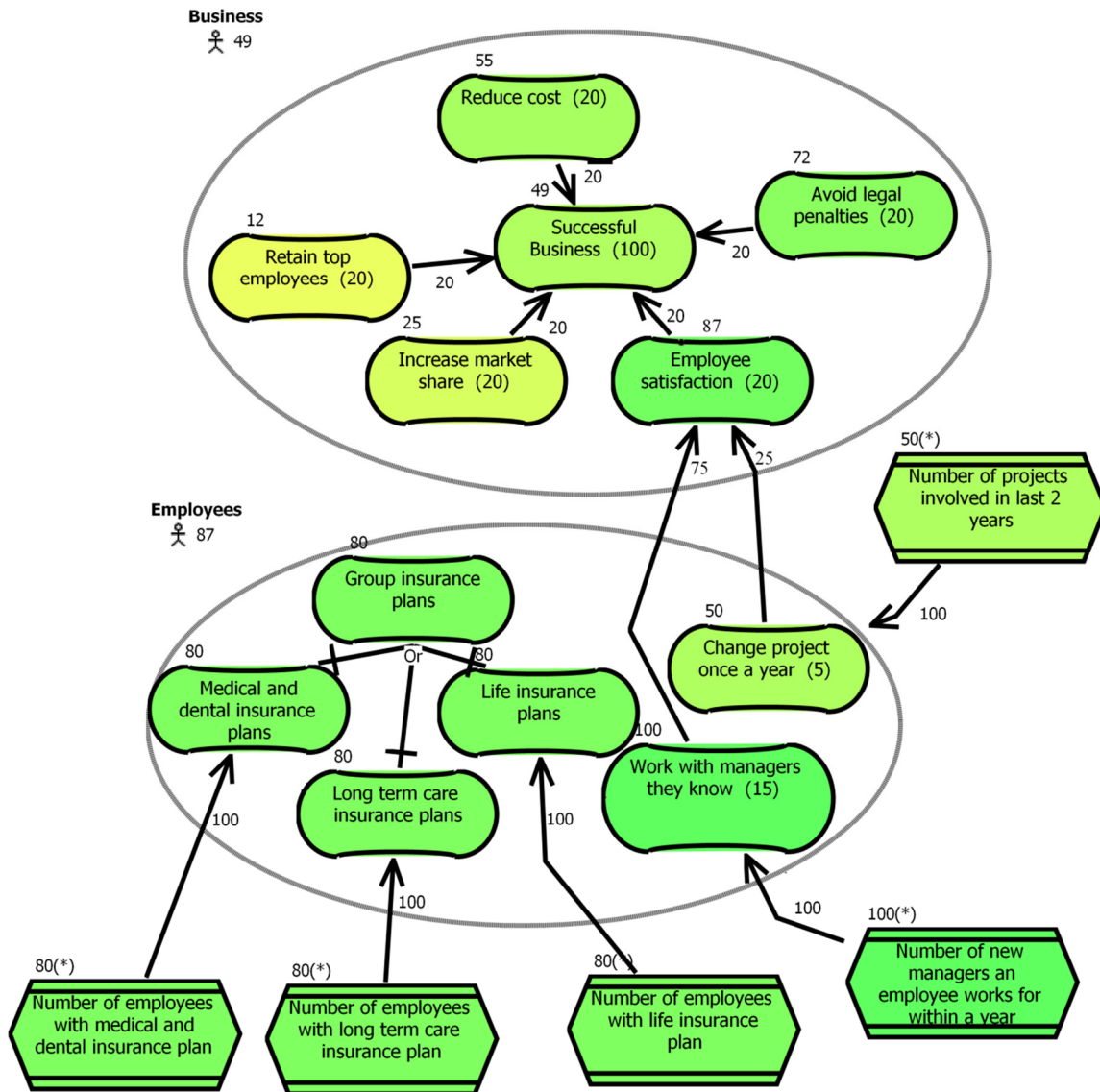


Figure 46, Employees' Satisfaction Level before Process Modification

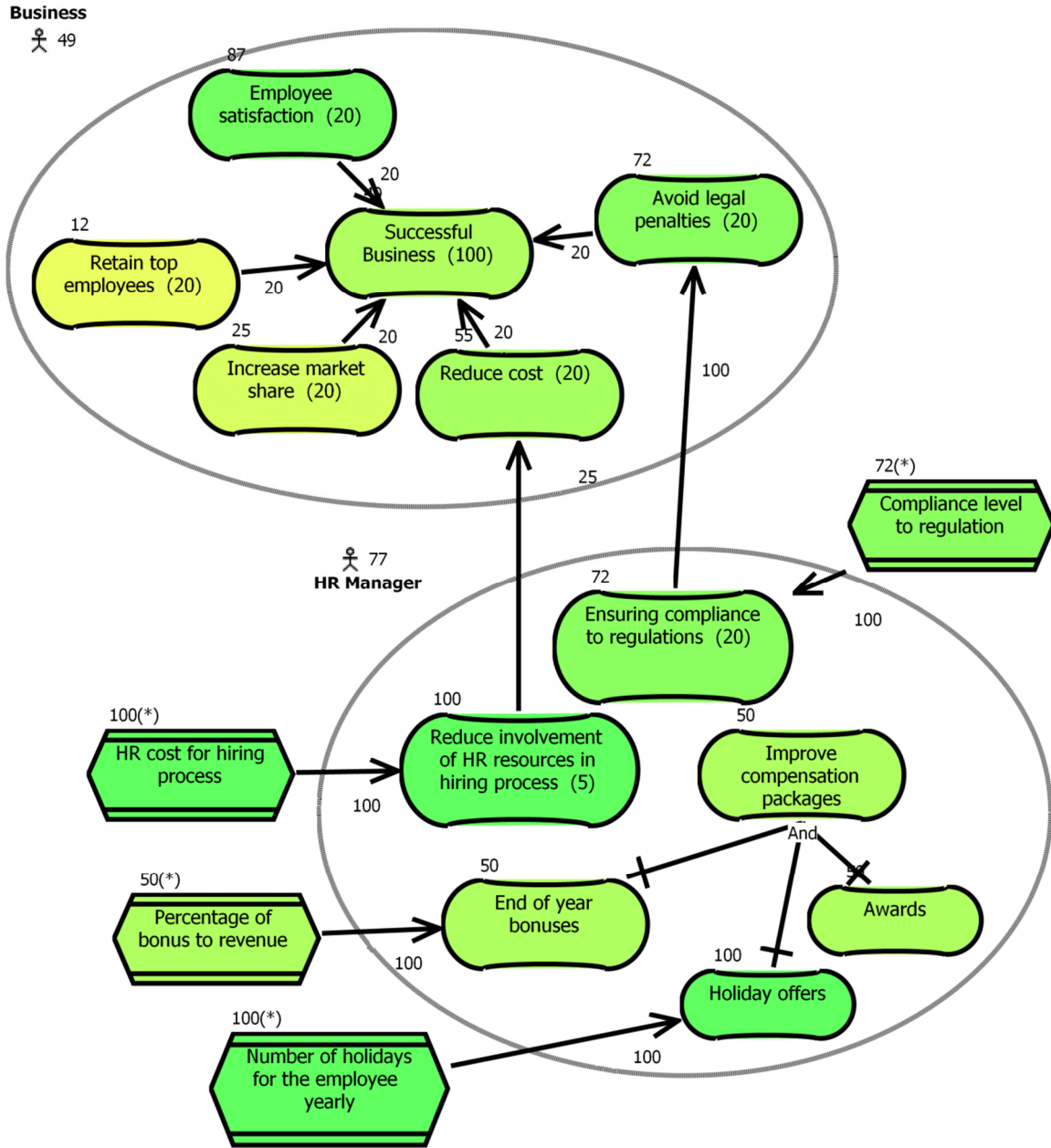


Figure 47, HR Manager's Satisfaction Level before Process Modification

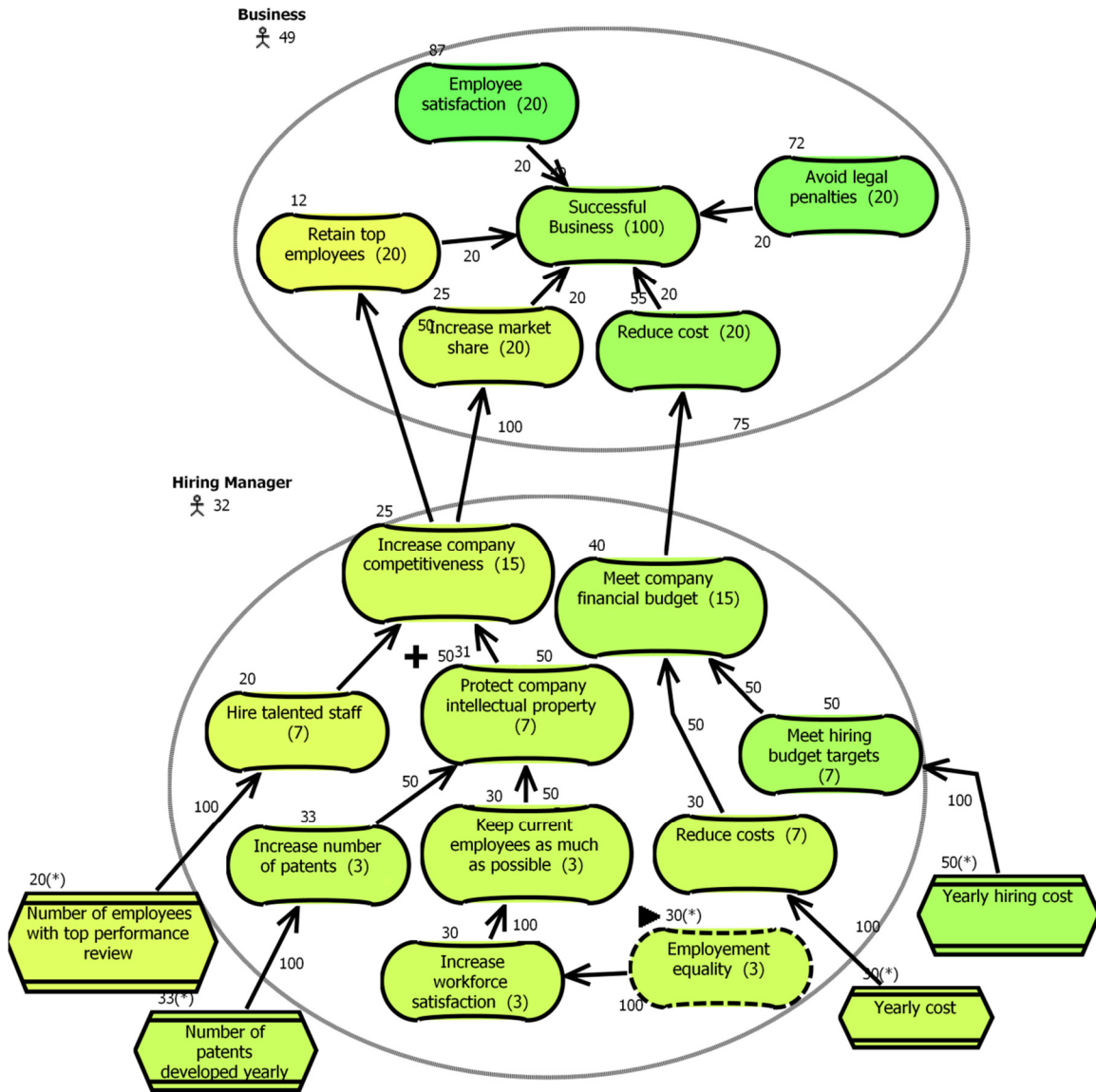


Figure 48, Hiring Manager’s Satisfaction Level before Process Modification

Actors	Satisfaction level
	Before Process Modification
Employees	87
HR Manager	77
Hiring Manager	32
Business	49

Table 18, Satisfaction Level of Actors before Process Modification

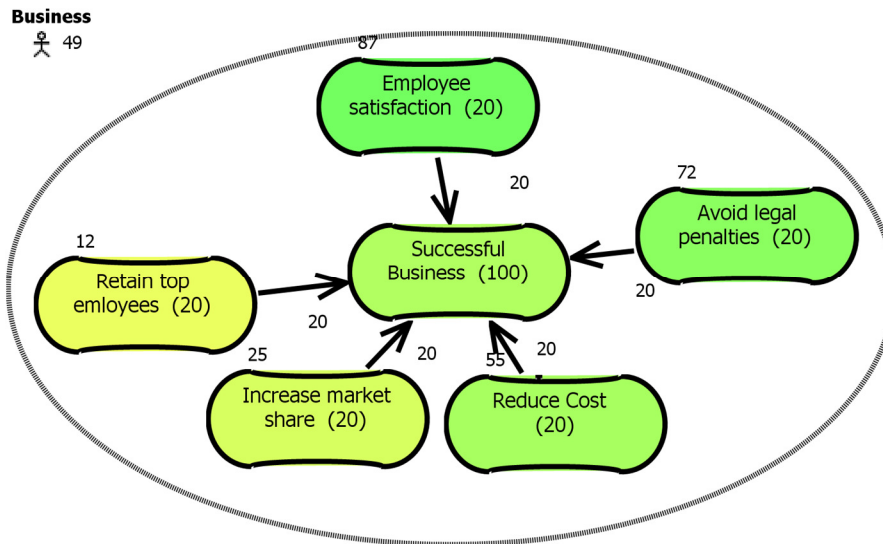


Figure 49, Business' Satisfaction Level before Process Modification

Actor	Key Performance Indicator	Target	Threshold	Worst	Evaluation
Employees	Number of new managers an employee works for within a year	1	0	0	1
	Number of employees with long term care insurance plan	50	40	0	48
	Number of employees with medical and dental insurance plan	50	40	0	48
	Number of project involved in last 2 years	4	2	0	3
	Number of employees that have life insurance plans	50	40	0	48
HR Manager	Number of awards announced yearly	20	10	5	15
	Number of holidays for the employee yearly	15	20	25	15
	Percentage of bonus to revenue	50	40	0	45
	HR cost for hiring process	2500	3000	5000	500
	Compliance level to regulation	100	50	20	86
Hiring Manager	Yearly hiring cost	5000	3000	0	4000
	Yearly cost	30000	20000	0	23000
	Number of patents developed yearly	15	9	0	11
	Number of employees with top performance review	40	30	0	32

Table 19, KPIs Values for Employees, HR Manager and Hiring Manager before Process Modification

5.3. Step C: Improvement

In this step, the organization attempts to improve its business processes based on the results highlighted in the quadrant diagram.

5.3.1 Rule Prioritization

As illustrated in Figure 45, rule R2 has the highest level of non-compliance whereas rule R4, also partially compliant, has the highest level of importance. Selecting one to deal with first is an issue. A mathematical formula can be used to choose between different rules. One such formula is based on the underlying rectangle area, where the position of the rule on the quadrant is one extremity of the rectangle's diagonal and the other extremity is the point where the importance is 0 and the compliance is 100. Hence, the importance level is multiplied by the difference between 100 and the compliance level, and the rule that has the highest value will take priority. Therefore, rule R2 takes priority over rule R4 in this example. Table 20 illustrates the results.

Rule	Compliance	Importance	Importance $\times$ (100 – Compliance)
R1	25	3	225
R2	-70	3	510
R3	50	1	50
R4	33	7	469
R5	58	1	42
R6	25	1	75
R7	66	1	34
R8	100	1	0

Table 20, Priority between Rules

By observing the results in Table 20, R8 is discarded immediately from the prioritization list since this rule is fully compliant (which is reflected by the metrics, whose value is 0 for this rule). The list of priorities based on compliance level and importance level for the other rules is shown in Table 21.

Priority	Rule
1	R2
2	R4
3	R1
4	R6
5	R3
6	R5
7	R7

Table 21, Prioritization List

5.3.2 Business Process Improvement

Since R2 has priority over other rules, the process associated to R2 should be improved in order to get the highest impact on the global compliance level. As Table 17 illustrates, out of ten internal applicants in a year, seven were employed without being interviewed first. In order to enforce rule R2 and increase the compliance level, two modifications to the business process related to R2 are suggested.

- Human Resources shall be involved in performing candidate interviews; and
- Interviewers shall fill out the job candidate evaluation form.

Figure 50 illustrates the modification to the interview business process. By comparing the new process with the previous one (Figure 31), a candidate will be interviewed not only by the hiring manager but also by human resource personnel. In addition, the interviewer team shall fill a job candidate evaluation form for each candidate. By adding these two steps, the number of candidates hired without interviews will be reduced.

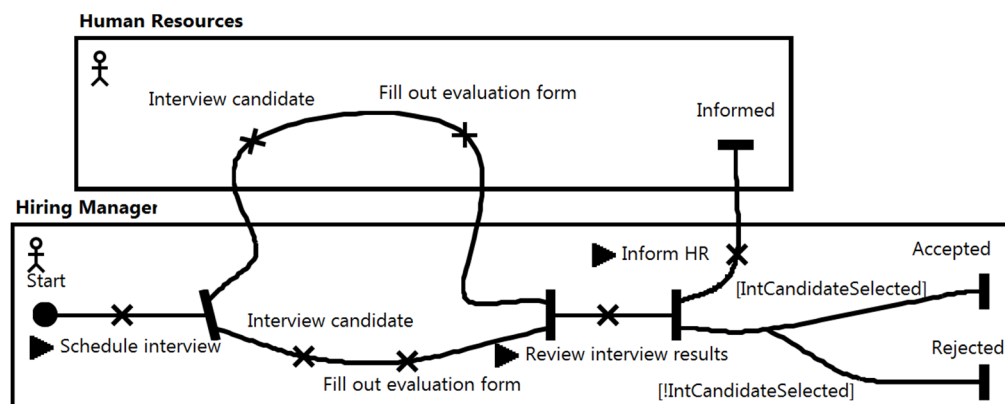


Figure 50, Interview Internal Candidates Sub-process after Process Modification

5.3.3 Handling of Goal and Rule Conflicts

In the monitoring step, the modified process will be monitored to observe improvement to the overall compliance level and also to detect potential side-effects introduced by this process modification on organization goals, including conflicting goals between stakeholders and conflicting rules. Before moving on to the next step however, it is assumed that the business processes related to R2, R4, R1, R6, R3 and R5 have already improved. The next and last rule according to the prioritization table (Table 20) is rule R7. This rule is linked to the “Keep resume of unselected applicants” business process step. Before making any modification to its business process, it is noticed that this process is not only linked to this rule (R7) but also to another regulation (R9), described in section 5.1 and Figure 39. As illustrated in Table 22, these two rules have conflicts. R7, which is an internal policy of the organization, requires keeping resumes of unselected applicant for a year whereas R9, which is a retention guideline of the government of Canada, requires keeping resumes for 6 months. In order to avoid non-compliance side-effects, it is the policy officer’s responsibility to apply necessary modifications to this rule in order to make it compliant with the regulation. After resolving the conflict the analyst can continue improving the business processes related to this rule. Although currently the conflict resolution is mainly handled manually, the modeling approach discussed in this thesis can help detecting issues like the one mentioned above. As part of the future work, there is an opportunity to improve the conflict detection by defining and exploring OCL rules that find process models (i.e., UCM model elements) with URN links going to more than one legal rule (i.e., GRL model elements tagged with a <<rule>> stereotype).

Business Process (or Step)	Rule
Keep resume of unselected applicants	Applications and resumes of applicants that were not selected for employment shall be forwarded to HR to ensure the retention of information for <i>a year</i> (R7)
	Staffing process requests, applications, examination papers, test results, employment offers, etc., shall be retained <i>2 years</i> for solicited applicants and <i>6 months</i> for unsolicited applicants (R9)

Table 22, Conflicts between R7 and R9

In the monitoring step, the main concern is on monitoring the business process related to R2.

5.4. Step D: Monitoring

As explained in section 4.5, the monitoring step is not only about monitoring the modified process to observe whether expected changes are happening, but also about monitoring organization goals in order to detect potential undesirable side-effects that may not have been modeled.

In section 5.3, the satisfaction level of actors in the organization and of rules *before* process modifications through a GRL strategy named “BeforeModificationToHiringProcess” are computed. In this section, the satisfaction level of actors and rules *after* process modifications are illustrated by defining a new strategy “AfterModificationToHiringProcess”. Such a strategy can be defined at modification time as a prediction model in order to support decision making (as is done in this section), or it can result from actual monitoring of the organization sometime after the process modification. In this case study, it is expected to observe an improvement for R2 “Qualified applicants shall remain subject to the normal hiring processes, including interviews” after the modification, is done on this process. Indeed, as illustrated in Figure 51, the satisfaction level for R2 has significantly improved from -70 to 100.

Table 23 illustrates the KPI values that changed for different actors, after process modifications. By comparing the actor satisfaction values before and after modifying the Interview internal candidates sub-process (see Table 24), one can observe that this modification has no effect on the satisfaction level of Employees (see Figure 52). The modification has a negative effect on the HR Manager’s satisfaction level (see Figure 53). However, the process improvement leads to a positive effect on the Hiring Manager’s satisfaction level (see Figure 54) and on the overall satisfaction of the Business (See Figure 55).

The main modification to the Interview internal candidates sub-process is to involve Human Resources in performing interviews. Before, Human Resources were not part of the interview, therefore this modification affects the “HR cost for hiring process” KPI. According to Job Canada’s website [61], a human resource manager working in Canada earns an average salary of \$83,859. It is assumed that five one-hour interviews per position are needed; in addition, it is assumed that a human resource manager works 49 weeks in a year, 37.5 hours/week of work, plus 30% overhead (in addition to the sala-

ry). Therefore, the total cost of a human resource manager participating in 10 new postings would be about \$2966. The evaluation value of this KPI changes from 500 to 2966 and this has negative side-effect on the HR Manager's satisfaction level. On the other hand, this process modification can increase the chances of hiring a talented candidate by adding the suggested steps. Therefore, this has a positive impact on the Hiring Manager's goals. This process increases the satisfaction level of the Number of employees with top performance review KPI from 20 to 40 and of the Number of patents developed in a year from 33 to 66. Therefore, this improves the total satisfaction level of the Hiring Manager from 32 to 52. Finally, the overall satisfaction of the organization's Business improved from 49 to 53.

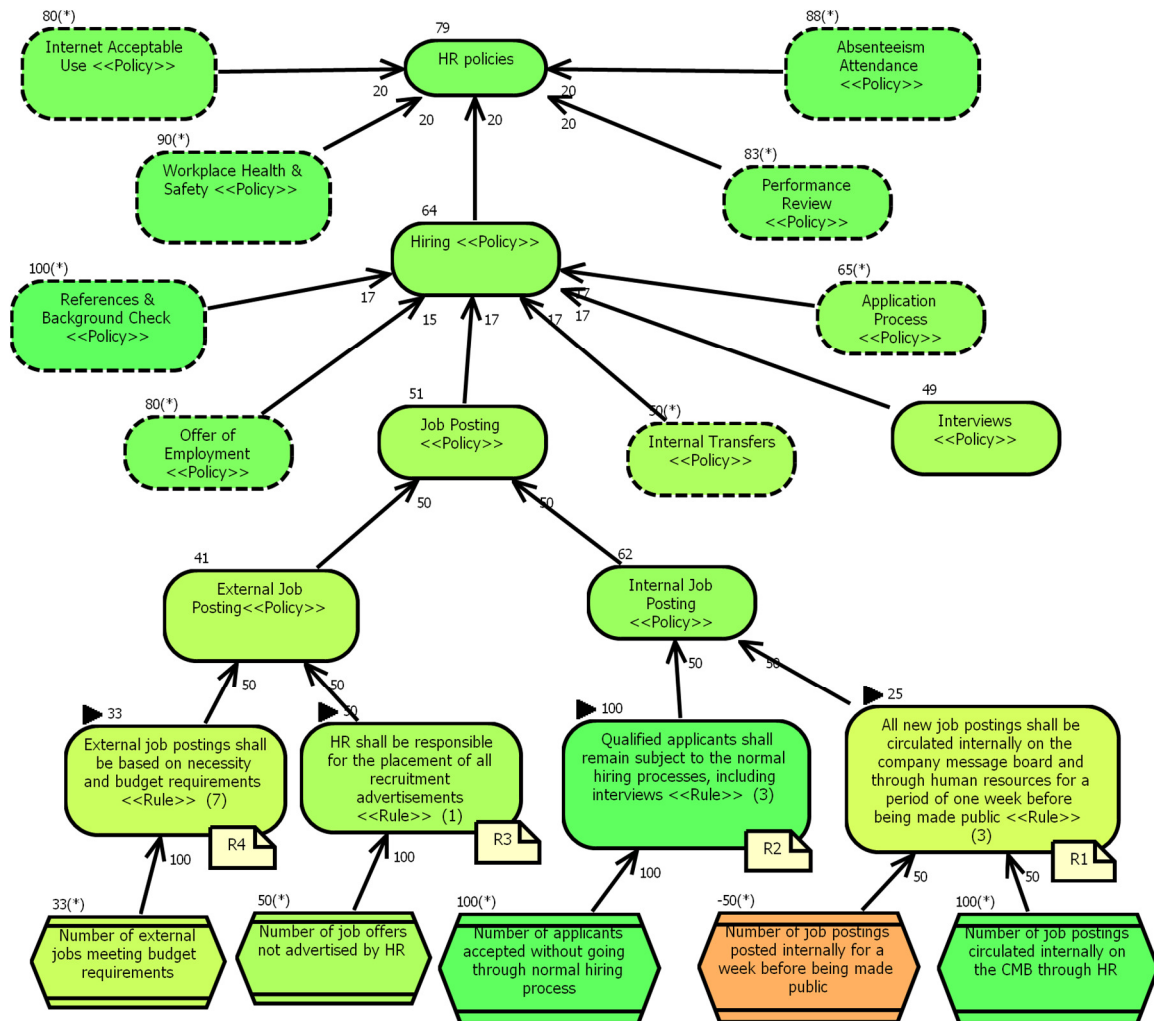


Figure 51, Job Posting Satisfaction Level after Process Modification

Key Performance Indicator	Target	Threshold	Worst	Evaluation
HR cost for hiring process	2500	3000	5000	2966
Number of patents developed in a year	15	9	0	13
Number of employees with top performance review	40	30	0	34

Table 23, KPIs Values for Employees, HR Manager and Hiring Manager after Process Modification

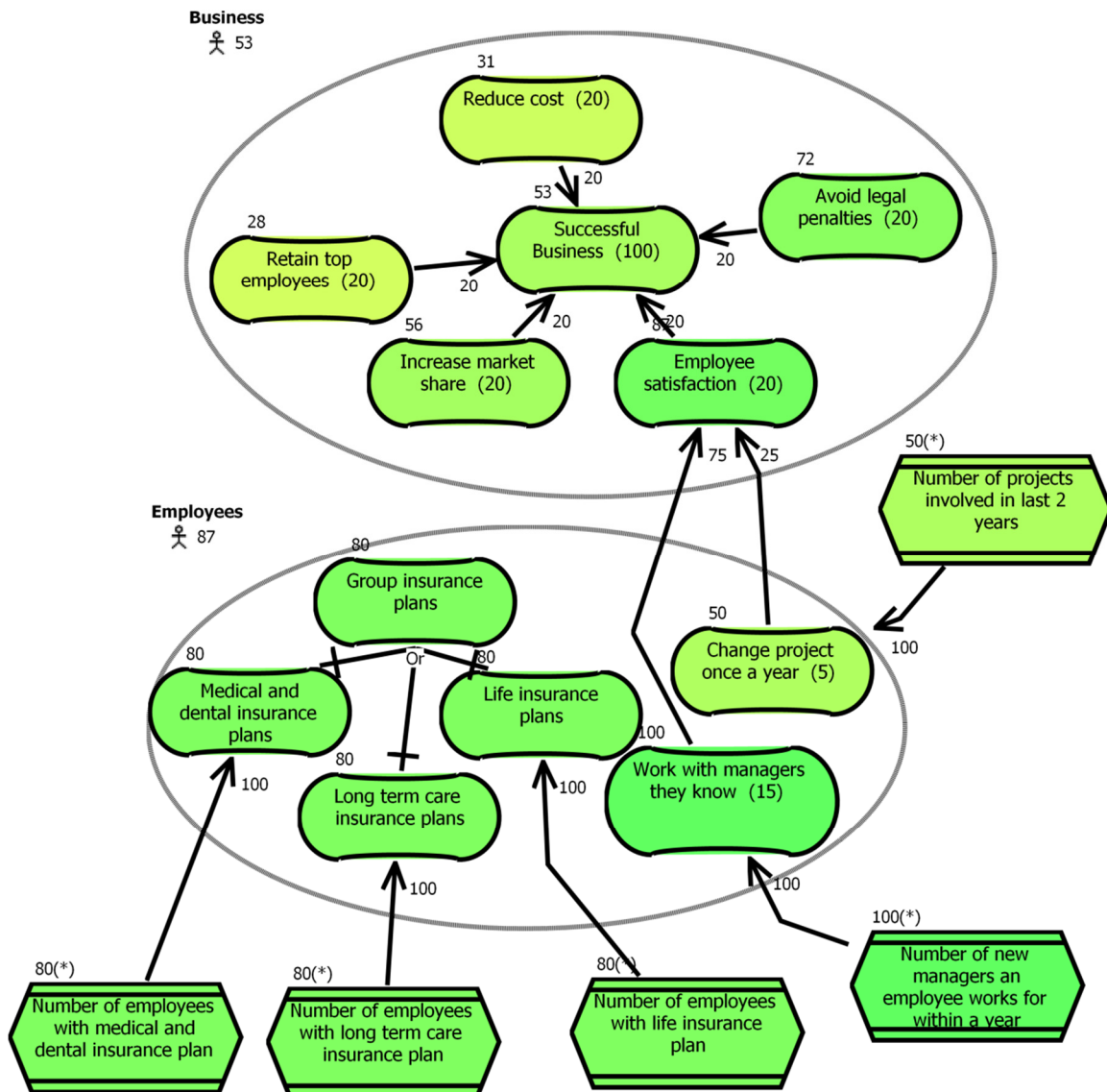


Figure 52, Employees' Satisfaction Level after Process Modification

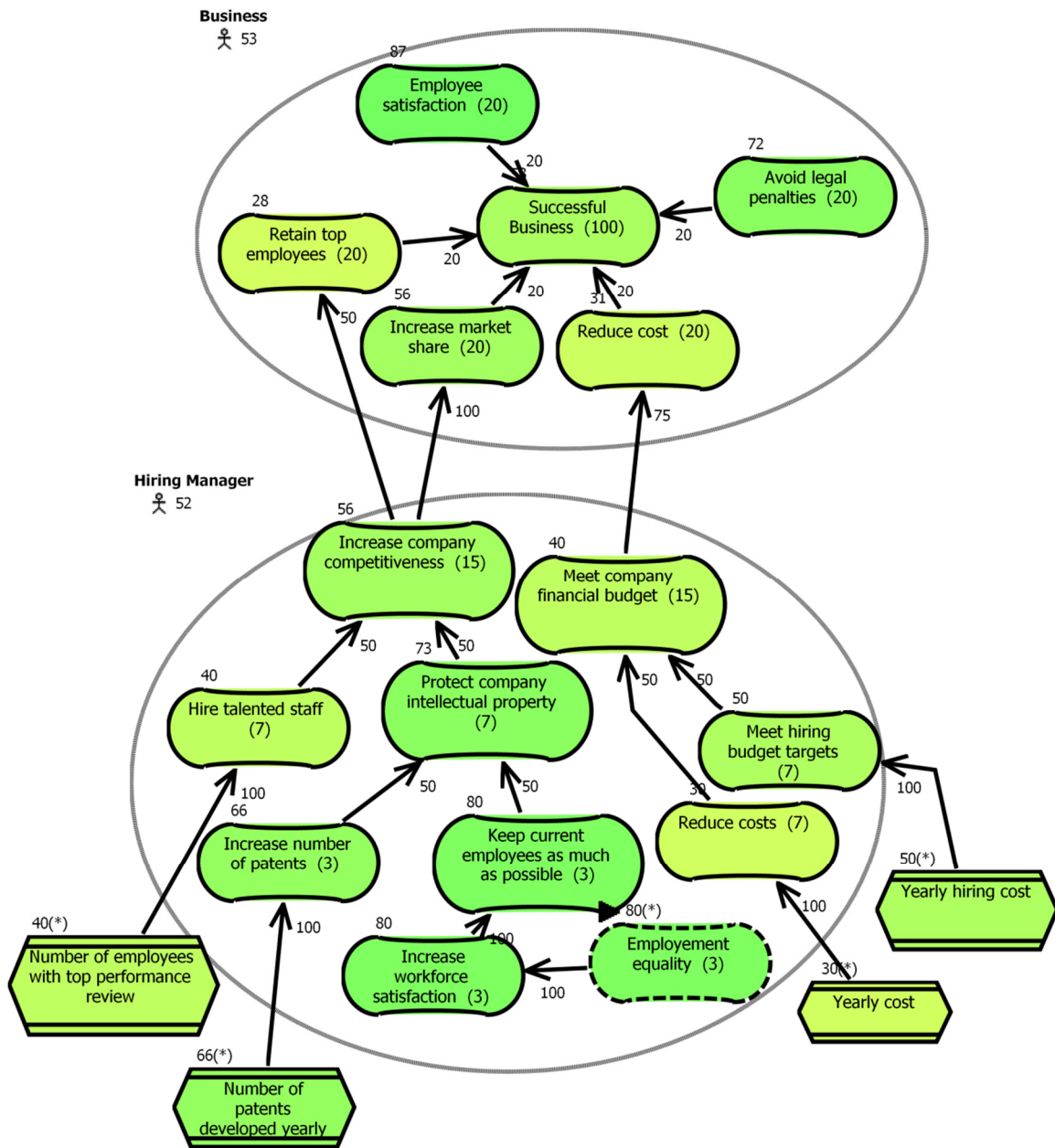


Figure 54, Hiring Manager's Satisfaction Level after Process Modification

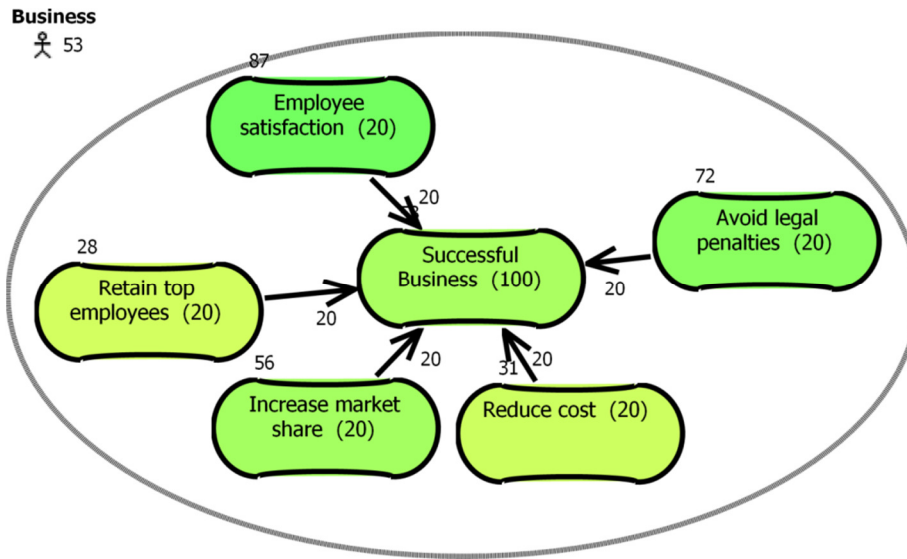


Figure 55, Business' Satisfaction Level after Process Modification

Actors	Satisfaction Level	
	Before Process Modification	After Process Modification
Employees	87	87
HR Manager	77	58
Hiring Manager	32	52
Business	49	53

Table 24, Comparison between Stakeholders' Satisfaction Levels

According to the model and the *before* and *after* strategies, the proposed modification will increase the organization cost but will also help improve the compliance level. Depending on the total cost incurred by such a modification to business processes, decision makers can assess whether to apply the modification or not. Since the cost in this case is not high, it is worthwhile to increase the chances of hiring a talented candidate by adding the extra steps to the interview business process. Although this modification has a negative effect on the satisfaction of the HR Manager (because of higher costs), it brings positive effects on other stakeholders and on the overall business.

5.5. Summary

In this chapter, all of the method steps were discussed using a human resource case study.

Business goals of the organization were modeled as well as its hiring business process and KPIs. Goals were linked to related business processes through URN links. Then the hiring policy, the job posting sub-policy, the internal and external job posting sub-policies, and finally the rules and their KPIs were modeled. In the evaluation step, two GRL strategies were identified, “BeforeModificationToHiringProcess” and “After-ModificationToHiringProcess”. These strategies were used to initialize KPIs and evaluate the satisfaction level (compliance level) of rules, policies and organization goals before and after modifications to a business process. In addition, the importance level of each policy/rule and intentional element contributing to the business was calculated through the algorithm proposed in section 4.3. Then, a quadrant diagram was used to display the situation of rules based on these compliance and importance values. Finally, in the improvement and monitoring steps, the most important, non-compliant business process were modified and described the effects of this modification on the satisfaction of rules and organization goals.

Chapter 6. Evaluation Example – Aerodrome Perimeter Security

In this chapter, a real-world example is used to evaluate the Indicator-based Policy Compliance Framework. This example, related to the aviation security regulator in Canada, is related to aerodrome perimeter security. The regulator would like to move away from prescriptive-based compliance towards outcome-based compliance, where goals and KPIs will play an important role. The benefit of having goal-oriented models is that as long as the combination of rules satisfies the high-level goals, the satisfaction of each rule individually has less significance whereas the outcome is important. Using KPIs also allows one to measure the compliance level of each individual rule as well as the compliance level of high-level goals. Therefore, if high-level goals are not satisfied, one can drill down to the low-level rules and find out the root cause of the problem. Finally, IBM Cognos is used both as an input to compute the indicators required by the URN model and as an output for reporting to stakeholders. The rest of this chapter is organized according to the framework steps. In each section of the chapter, the framework steps are applied to the example scenario.

6.1. Step A: Modeling

In this step, as discussed in 4.2, the organization business process and goal models are created and related business processes are associated with related goals through URN links. In addition, policies and their rules, together with links between rules and related business processes are modeled.

Normally, one of the major goals of an aerodrome is to have effective perimeter security. The regulator issues the required regulations to be implemented by the aerodromes. The regulations establish obligations on aerodrome operators and specify various security elements (e.g., signage, requirements for fencing, access control, etc.) that would comprise an appropriate system of perimeter security. Due to the sensitive nature of secu-

rity regulations, only security regulations that are public (such as signage) are demonstrated. An artificial, simplified, and obfuscated example is used instead of a real one, but the framework was applied to many real and complex aviation security regulations.

6.1.1 Organization Business Process Model

Among various business processes that are put into place to implement perimeter security by aerodromes, the focus of this chapter is mainly on modeling the sign inspection and installation business process. There are three different types of signs that exist in an aerodrome [24]. *Mandatory signs* are those signs that indicate an entrance into restricted and critical areas. They have a red background with white imprint. *Location signs* are used to indicate locations in an aerodrome. They are black with a yellow border and yellow imprint. Finally, *Direction signs* are used to indicate different directions at aerodromes. They have a yellow background with black imprint. Mandatory signs and particularly regulations related to restricted area signs are picked for this example.

A simplifying assumption in this example is that the aerodrome is divided into four sections, A, B, C, and D as illustrated in Figure 56. Each section consists of four restricted areas (there exact shape does not matter for this example). In each area, various restricted area signs should exist or be installed.

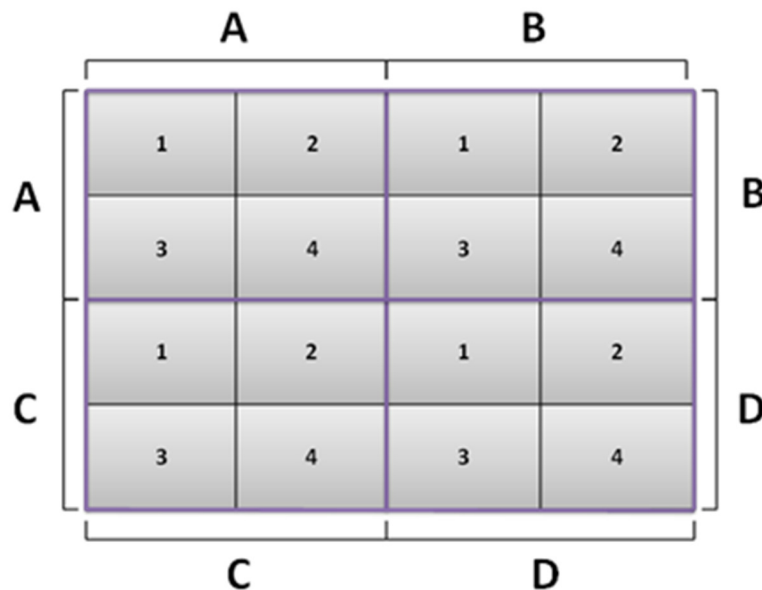


Figure 56, Restricted Area in Aerodromes

Various reports on the sign-related processes of different aerodromes were studied. One of the documents that help to understand such processes is from the Los Angeles International Airport [75]. The *sign inspection process* is modeled using the UCM notation. This process, illustrated in Figure 57, has three actors: Compliance Department, Compliance Officer, and Aerodromes Operator. It is also composed of two sub-processes modeled using UCM stubs with plug-ins: Report on non-compliance, and Improve non-compliance area (see Figure 58 and Figure 59).

The sign inspection process starts when a Compliance Officer selects areas for inspection and informs an Aerodromes Operator of those areas. The Aerodromes Operator inspects the selected areas and if no non-compliance issue is found, the Aerodromes Operator creates a compliance notice and submits it to the Compliance Department, which keeps records of inspected areas. If an area is found to be non-compliant, the Aerodromes Operator starts reporting on non-compliance areas (see Figure 58) by creating a non-compliance notice and informs the Compliance Officer with a written notice. The Compliance Officer reviews them and determines the required action based on the sign status, i.e., the sign is either removed or refurbished (see Figure 59). The Compliance Officer informs the Compliance Department of the required actions, and the latter keeps a record of inspected areas, reviews the actions required for compliance, and approves the recommended actions.

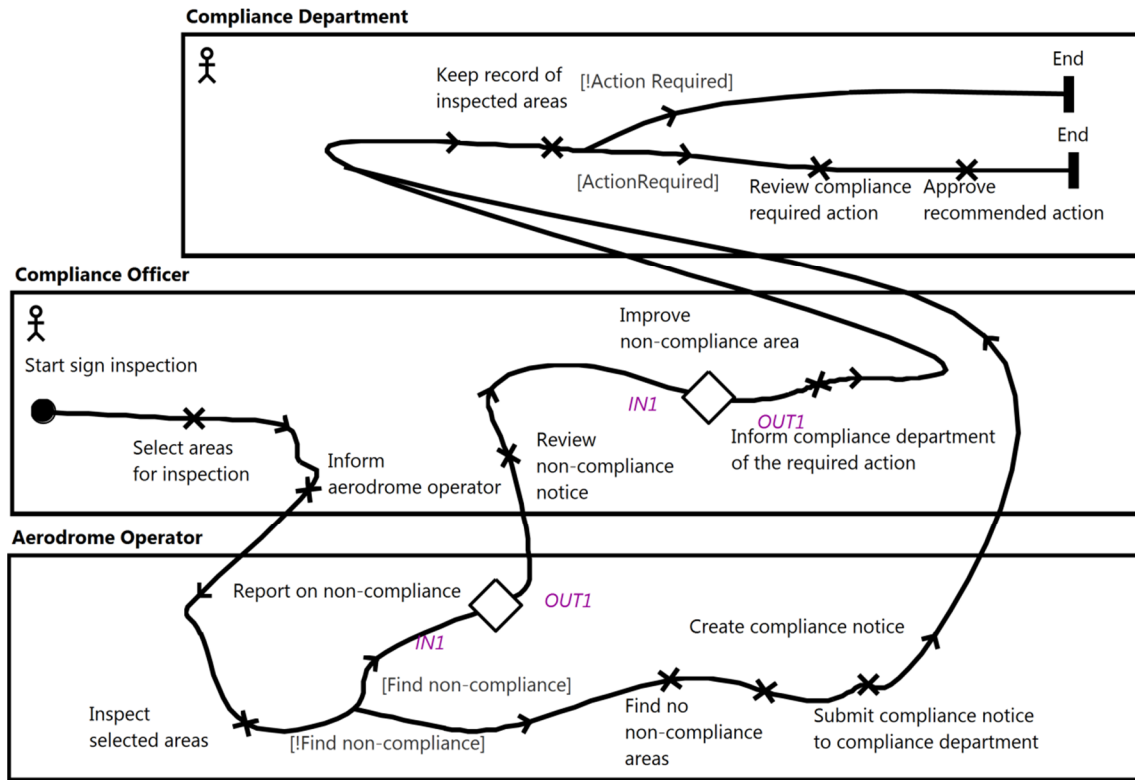


Figure 57, Sign Inspection Business Process (As-Is)

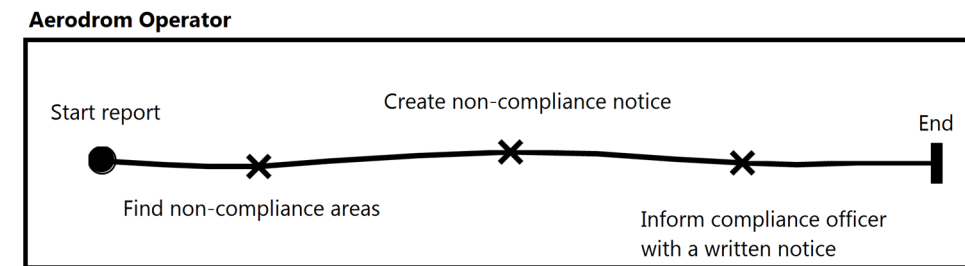


Figure 58, Report on Non-Compliance Areas Sub-Process (As-Is)

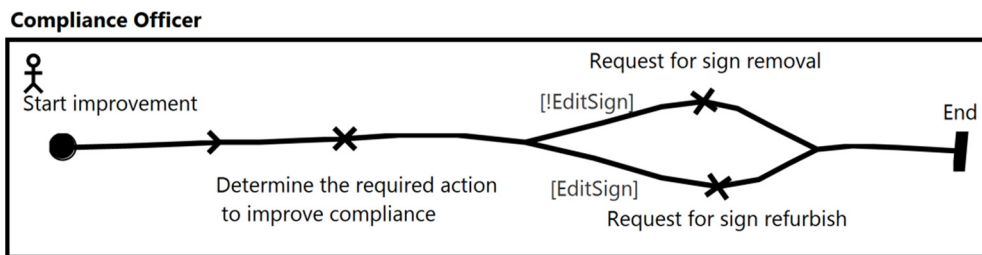


Figure 59, Improve Non-Compliance Areas Sub-Process (As-Is)

The *sign installation process* has also been modeled. This process, illustrated in Figure 60, has three actors: Assembly Department, Aerodrome Operator, and Engineering & Project Management Division (EPMD). It also contains two sub-processes modeled using

UCM stubs with plug-ins: Write Sign Proposal, and Sign Checklist (see Figure 61 and Figure 62).

An Aerodromes Operator starts the sign installation process by submitting a written sign proposal to EPMD. The proposal (see Figure 61) should include a description of the sign type, as well as a set of renderings or elevations to scale, and the drawing should be done on a sheet minimally of size 11"x17". Upon receiving the sign proposal, the EPMD reviews the proposal and informs the Aerodrome Operator of the decision taken. The sign proposal may be rejected by EPMD right away. However, if EPMD accepts the proposal, it is the Aerodrome Operator's responsibility to then submit the sign proposal to the Assembly Department for its creation. Upon receiving the created sign, the Aerodrome Operator goes through a checklist to insure the sign complies with all its requirements (see Figure 62). The Aerodrome Operator checks the sign's font and text color, whether the sign indicates the entry is restricted to unauthorized people, the sign material, whether the sign has a restricted area symbol, whether the text is written in all required languages, etc. If any of these checks fails, the Aerodrome Operator requests the Assembly Department to fix the sign, whereas if all checks pass then the sign is installed.

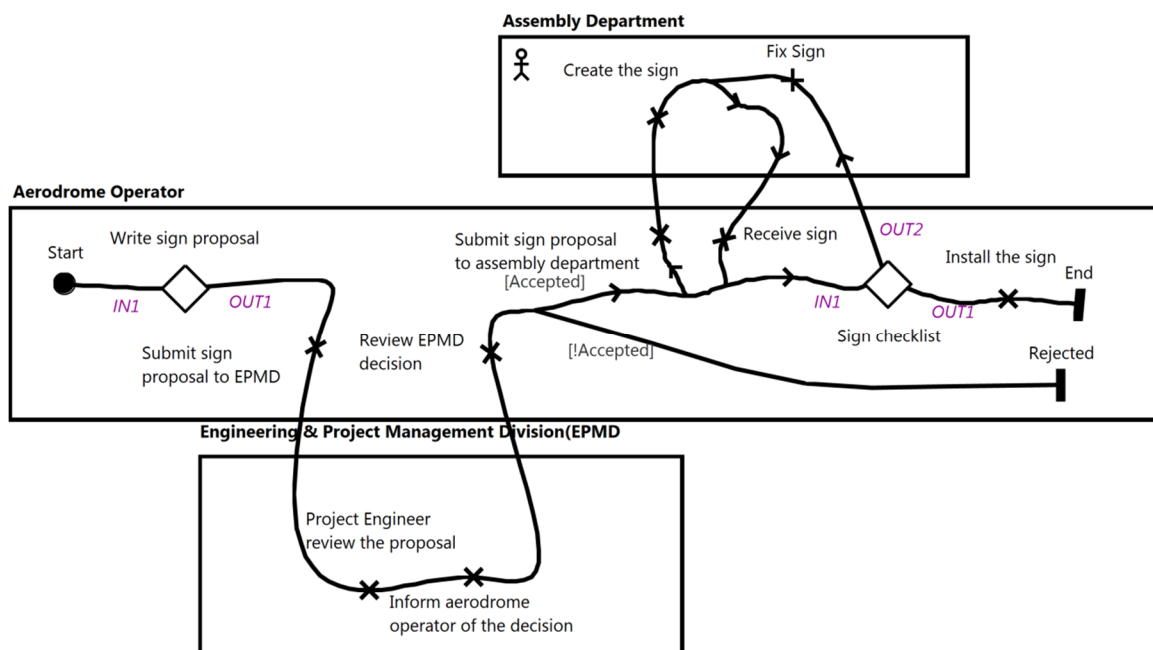


Figure 60, Sign Installation Business Process (As-Is)

Aerodrome Operator

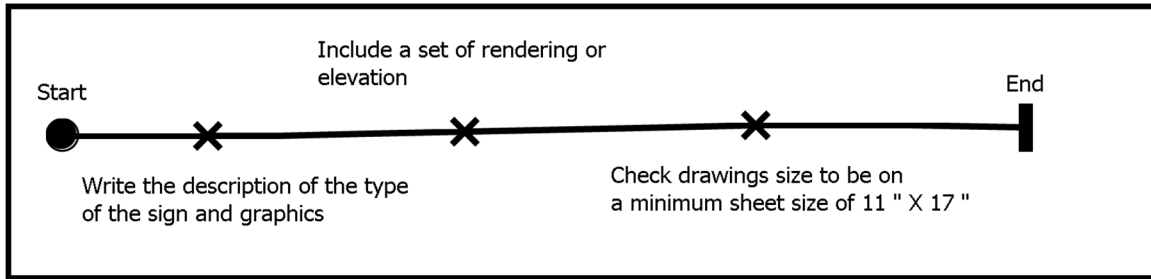


Figure 61, Write Sign Proposal Sub-Process (As-Is)

Aerodrome Operator

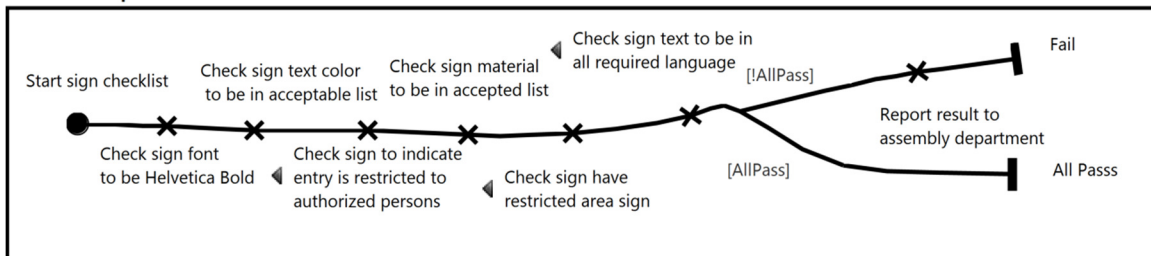


Figure 62, Sign Checklist Sub-Process

6.1.2 Organization Business Goal Model

The organization's high-level goals are modeled. There are different types of actors involved in aerodromes including [117]: Compliance department, aerodrome operator, finance department, parking operators, passengers, air carriers' employees, and service providers whom all have different goals. In this example the goals of the Compliance Department, Aerodrome Operator, and Finance Department are modeled. In addition, as discussed in section 4.3, an extra Business actor is added as part of the method for calculating the importance level of different GRL intentional elements.

The various intentional elements contributing to a successful business are modeled. Six softgoals that affect the Successful Business main objective are identified in Figure 63. All these softgoals are assumed to be more or less equally important and required for complete satisfaction. Therefore, they are all connected to Successful Business with quantitative contributions of 17 (except for one with a contribution of 15, in order to get a contribution sum of 100). Numbers between parentheses inside each softgoal represent their importance level, which will be discussed in section 6.2.2.

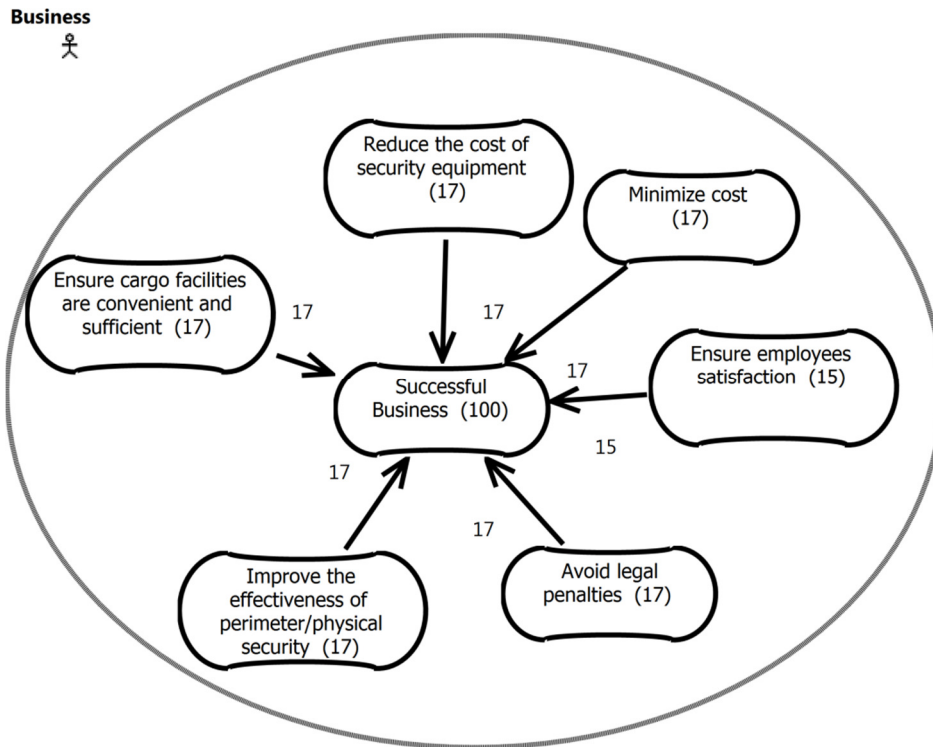


Figure 63, Business High-level Goal Model for Aerodrome Security

Next, the goals of various stakeholders (actors) involved in the organization and their impact on the goals of the Business actor are modeled. Figure 64, Figure 65, and Figure 66 show the goals of the actors Compliance Department, Aerodrome Operator and Finance Department respectively, together with their contributions to a Successful Business. As Figure 64 illustrates, one of the goals of the Compliance Department is to improve perimeter security. This goal can be achieved through three sub-goals: identification of perimeter security (for instance, by having appropriate signs and appropriate lines on the ground for restricted areas), improve the delineation of perimeter security (e.g., by using security barriers such as fences), and finally improve the detection of perimeter security breaches (e.g., through Closed Circuit Television and guards). These three soft-goals are assumed to contribute respectively with weights of 36, 32, and 32 to the satisfaction of Improve perimeter security, which itself has a contribution level of 100 on Improve the effectiveness of perimeter/physical security, which in turn has a contribution level of 16 on Successful Business. Another goal of the Compliance Department is to ensure compliance to regulations that can cause financial penalties. This has been illus-

trated by showing a contribution level of 100 from these regulations to the Avoid financial penalties goal, which itself has a contribution level of 17 on Successful Business.

Then, several KPIs are defined to help analyzing the impact of the changes made to business processes for improving the compliance level on the organization goals. For instance, in order to measure the softgoal Ensuring compliance to regulations, the indicator Compliance level of regulations is used, where the target value (the number of regulations to be compliant with) is equal to 40, and the worst value is 0. Furthermore, to measure the satisfaction level of the softgoal Identification, the indicator Sign regulation compliance is used, where the value is propagated from the sign regulation model (see Figure 67) to this KPI. In general, KPI satisfaction values can either be propagated from another intentional element as shown in Figure 67 or be calculated through target, threshold, evaluation and worst values.

URN links between the UCM diagrams and the GRL graphs are indicated by triangles next to labels on the graphical models (see Figure 64). For instance, there is a traceability link from the Identification softgoal in the Compliance Department (Figure 64) to the Sign Installation UCM Map (Figure 60).

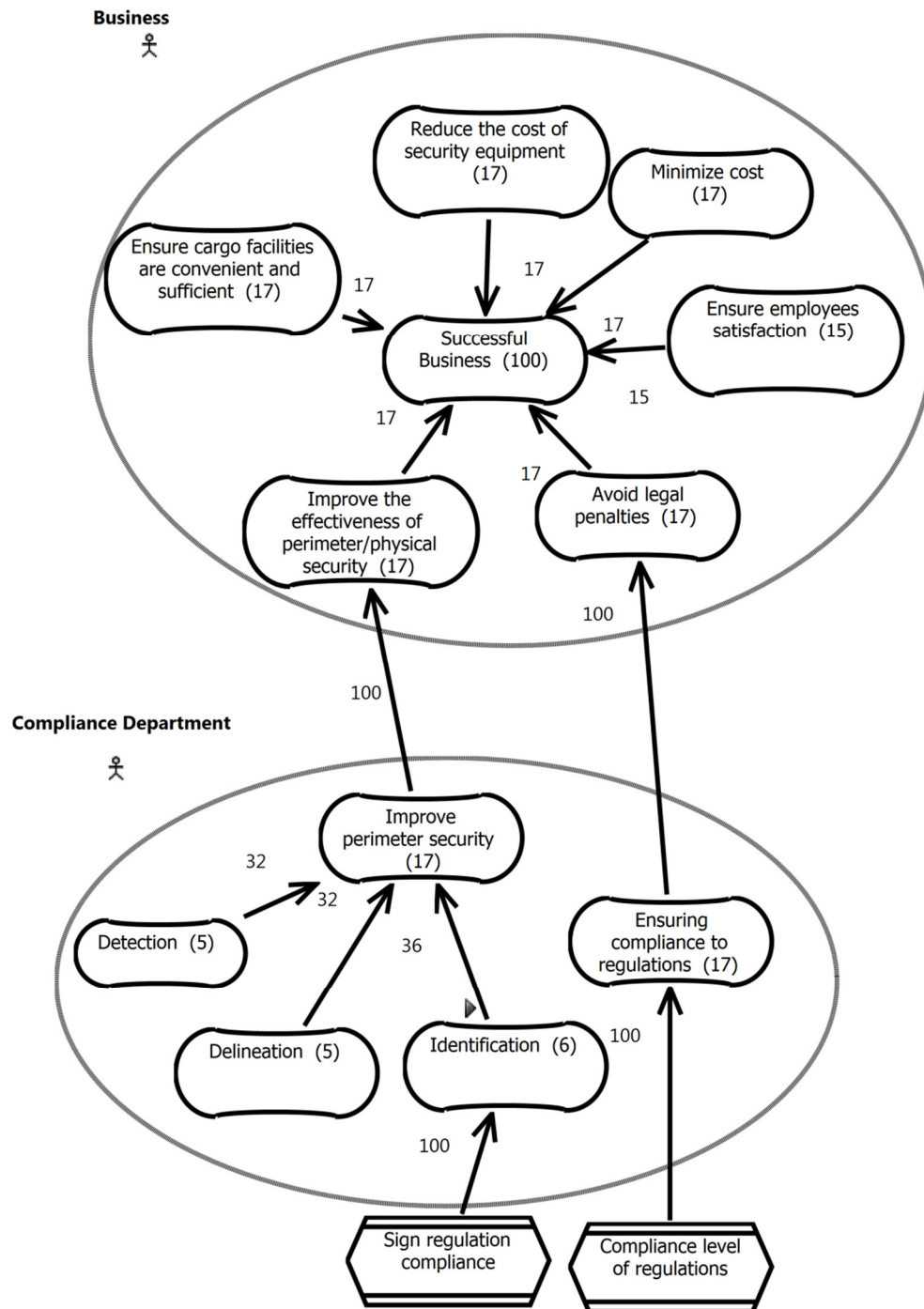


Figure 64, Compliance Department’s Business Goal Model, with Impact on Business Goals

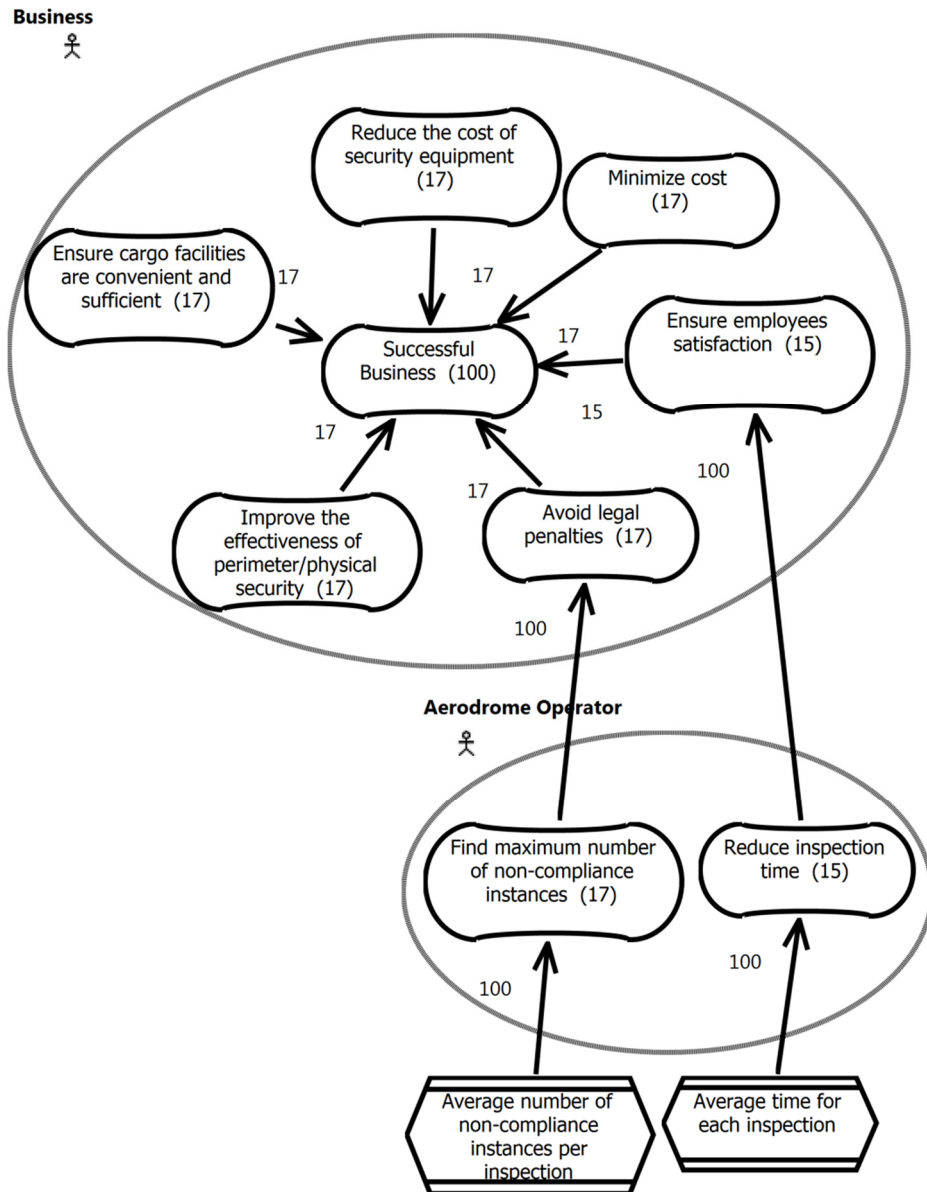


Figure 65, Aerodrome Operator's Business Goal Model, with Impact on Business Goals

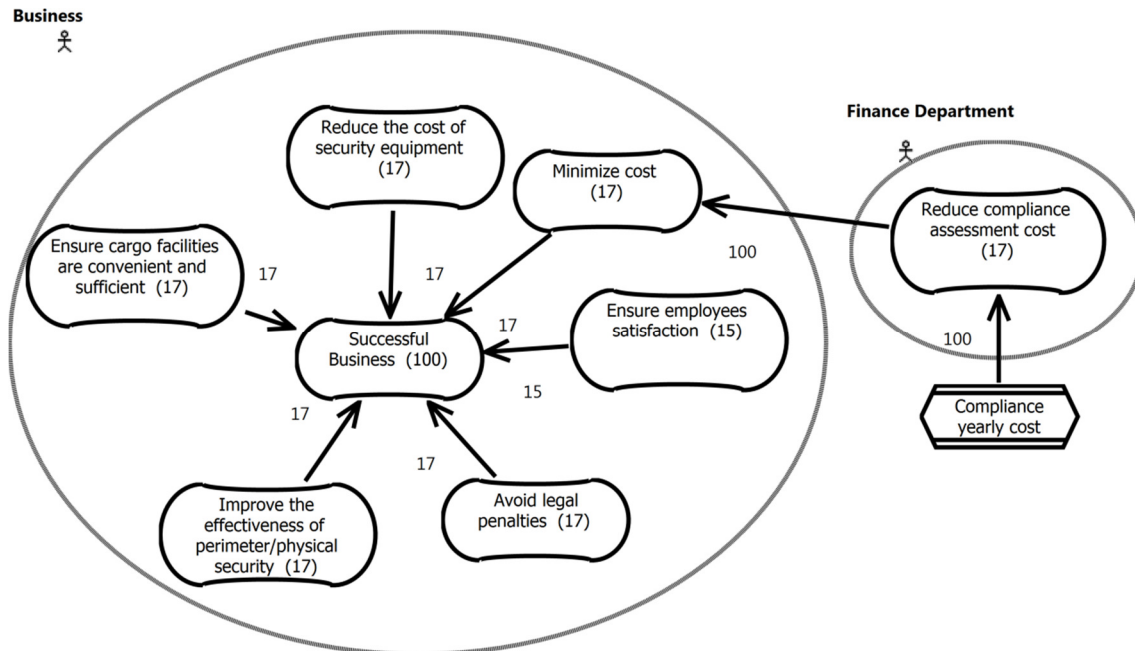


Figure 66, Finance Department’s Business Goal Model, with Impact on Business Goals

6.1.3 Regulation Model

Next, the regulations are modeled using GRL. Only the parts of the regulation that are public and have been published on the Canada Gazette website [25] are illustrated here. According to this source, regulations that apply to signs for restricted areas are:

“(1) The operator of an aerodrome listed in Schedule A, B or C must post signs on the outside of each restricted area access point and each security barrier. Each sign must

- (a) be in at least both official languages;
- (b) identify the restricted area as a restricted area; and
- (c) state that access to the area is restricted to authorized persons.

(2) The signs posted on a security barrier must be no more than 150 m apart.”

There are two sub-regulations/rules that apply to a sign as illustrated in Figure 67. As explained in the guideline for extracting GRL models from regulations (section 4.2.2) all sub-terms have by default an equal impact on the parent node (sign). Hence, the contribution links’ total weight (100) is divided equally between two sub-regulations. Therefore, each sub-term has a contribution level of 50. Obviously, such default values can be overridden by a domain expert where required.

For the first sub-term (1), there are three rules (a, b, and c) identifiable. Since all of them are required, AND-decomposition links connect them to the parent sub-regulation. The model in Figure 67 shows this relationship. Finally, relevant KPIs are defined for all leaf-level intentional elements. Table 25 gives the list of KPIs and rules. An identifier is assigned to each leaf-level intentional elements (R1 to R4, shown within comment boxes). These identifiers are used to reference the regulations in the rest of this chapter. In addition, as illustrated in Figure 67, Sign contributes with a weight of 100 to the Sign regulation compliance KPI, which is used to measure how well the Identification goal is doing for the Compliance Department actor. This particular KPI is hence computed from the satisfaction of other goals in the model.

Metadata is also added to intentional elements to specify the name and the value of the regulation, as well as the URL link of the regulations (Figure 68). In jUCMNav, by right-clicking on each intentional element with such metadata, the analyst can navigate automatically to the source document of the regulation.

Finally, URN traceability links between the regulations from the regulation model and processes from the organization business process model are created (Table 26).

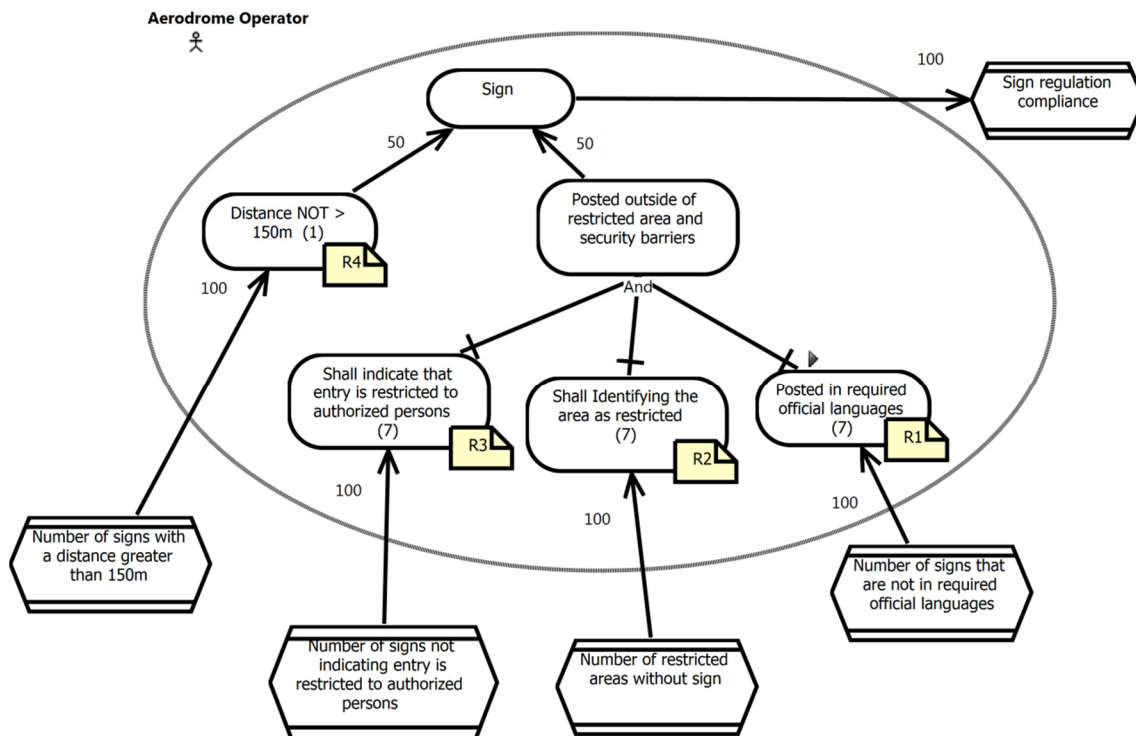


Figure 67, Sign Policy

METADATA:
 RegDocRef=AERONAUTICS ACT - Signs - Rule 1(a)
 hyperlink=<http://canadagazette.gc.ca/rp-pr/p1/2011/2011-12-10/html/notice-avis-eng.html#d101>

Figure 68, Sample Metadata Used to Navigate to Regulation Source Documents

Rule	Key Performance Indicator
R1	Number of signs that are not in required official languages
R2	Number of restricted areas without sign
R3	Number of signs not indicating entry is restricted to authorized persons
R4	Number of signs with a distance greater than 150m

Table 25, Sign Regulations and KPIs

Business Process (or Step)	Rule
Sign Installation UCM Map	R1
Check sign text to be in all required language	
Sign Installation UCM Map	R1
Check sign have restricted area sign	
Sign Installation UCM Map	R3
Check sign to indicate entry is restricted to authorized persons	
Sign Installation UCM Map	R4
No Particular Responsibility	

Table 26, Mapping between Business Processes and Sign Regulation

6.2. Step B: Evaluation

In this step, GRL strategies are defined to evaluate the current satisfaction level of the sign regulation. In addition, the importance levels of policies/rules are evaluated. The evaluation results are illustrated on a quadrant diagram based on satisfaction and importance levels.

6.2.1 Evaluation of Satisfaction Levels

GRL strategies, where KPI evaluation values are populated from data capturing the as-is (current) situation, are used to evaluate the satisfaction level of regulation model. This example assumes that there are 100 restricted area signs in the aerodrome under study. The Target, Threshold, Worst, and Evaluation values are defined for the KPIs in the sample strategy called “BeforeModificationtoSignInstallationProcess”, as shown in Figure 69 and Table 27. These values are entered manually to initialize the KPI value sets. As explained in section 5.2.2, each KPI evaluation value is mapped to a GRL evaluation level for each KPI. These values are used to evaluate the satisfaction level of the other intentional elements as illustrated in Figure 70, using the quantitative evaluation algorithm supported by GRL and jUCMNav [6]. For instance, out of 100 signs, no sign is expected not to be written in both required official languages. Therefore the Target value for the “Number of signs that are not in required official languages” KPI is 0 and its Worse value is set to 100, meaning that no sign shall exist without having both required official languages. However, if there are less than about 20 signs that do not have all required languages, then the aerodrome’s score is still positive regarding compliance to official languages (based discussions with domain experts), and hence the Threshold value is set to 20. A stricter interpretation of this compliance would rule would have a lower Threshold than this (and its value would be 0 in the strictest interpretation). As shown in Figure 70, the satisfaction level for Sign is 10, and among the four rules, R4 has the lowest satisfaction level (-42) and R1 has the highest satisfaction level (85).

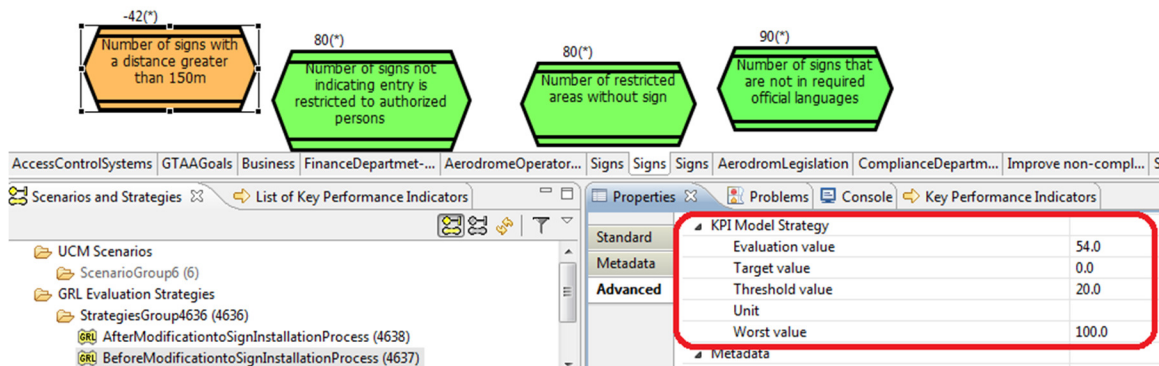


Figure 69, Initializing Signs KPIs in jUCMNav for Sign Example

Rule	Key Performance Indicator	Target	Threshold	Worst	Evaluation
R1	Number of signs that are not in required official languages	0	20	100	2
R2	Number of restricted areas without sign	0	20	100	4
R3	Number of signs not indicating entry is restricted to authorized persons	0	20	100	4
R4	Number of signs with a distance greater than 150m	0	20	100	54

Table 27, List of Sign's KPIs and Value Sets for Rules before Process Modification

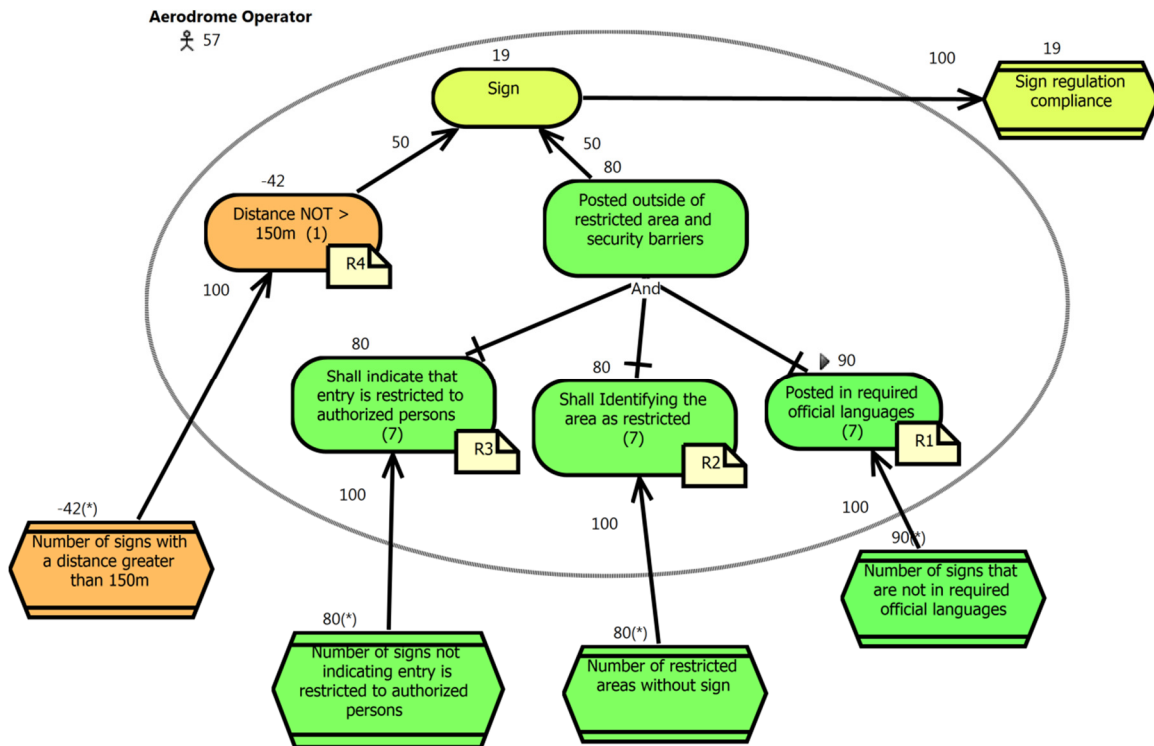


Figure 70, Sign Regulation Satisfaction Level (Before Modification)

6.2.2 Evaluation of Importance Values

In addition to satisfaction levels, the importance values of GRL intentional elements in the model are evaluated. The proposed importance algorithm (see section 4.3) is used to calculate the importance level of intentional goals, business processes and rules. For instance, the importance values of R1, R2, and R3 rules are all 7. These values are propagated all the way down from Successful Business which is the highest-level business goal (see Figure 63) and is initialized with an importance value of 100. The importance of

each source intentional element that contributes to a given target intentional element is proportional to both the importance level of the target and the weight of the element's contribution. For example, Improve the effectiveness of perimeter/physical security is one of the Successful Business goals with a contribution level of 17. Therefore the importance value of this goal becomes $100 \cdot 17 / (100 \cdot 1) = 17$. This goal is connected to Improve perimeter security through a contribution link with a contribution level of 100. Consequently, the importance value of this intentional element becomes $17 \cdot 100 / (100 \cdot 1) = 17$. This goal is connected to Identification, Delineation, and Detection with contribution levels of 36, 32, and 32 respectively. Hence, the importance value of these intentional elements becomes $36 \cdot 16 / (100 \cdot 1) = 7$ and $32 \cdot 16 / (100 \cdot 1) = 5$ respectively. Integer values are used here, and no importance value can be less than 1.

The importance value of Identification softgoal is propagated to the UCM Sign Checklist, and therefore the importance values of all the responsibilities in this map are set to 7. Therefore, the importance values of rules R1, R2, and R3, which are linked to a responsibility in this map, become 7. The importance value of rule R4, which is not connected to any responsibility, is set to 1 by default. Again, all these default and computed values can be overridden by domain experts.

6.2.3 Importance/Compliance Quadrant Diagram Representation

Satisfaction and importance values are used to lay out the rules on a quadrant diagram. This quadrant allows one to *identify what are the most important rules with the lowest level of compliance*. This will allow the people in charge to easily prioritize the improvement candidates.

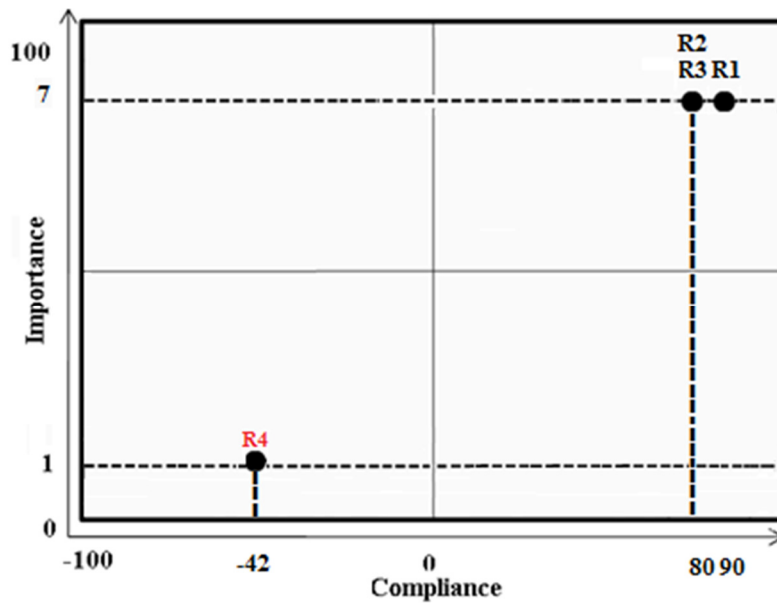


Figure 71, Importance and Compliance of Sign Rules on a Quadrant Diagram

Business processes are improved based on the results of the quadrant diagram in the Improvement step covered in next section. However, in order to be able to determine the impact of compliance-related process modifications on business goals of different stakeholders, first the satisfaction level of various stakeholder goals is recorded using KPIs. These KPIs are illustrated in Figure 72, Figure 73, and Figure 74. The KPIs Target, Threshold, Worst and Evaluation values, and the Evaluation level in the case of Sign regulation compliance, are detailed in Table 29. After defining a GRL strategy and initializing the KPIs with these values, the quantitative propagation algorithm is used to evaluate the satisfaction level of stakeholder goals. As a result, Compliance Department (Figure 72), Aerodrome Operator (Figure 73), Finance Department (Figure 74) and the extra Business actor (Figure 75) have satisfaction levels of 35, 57, 80 and 59 respectively (Table 28).

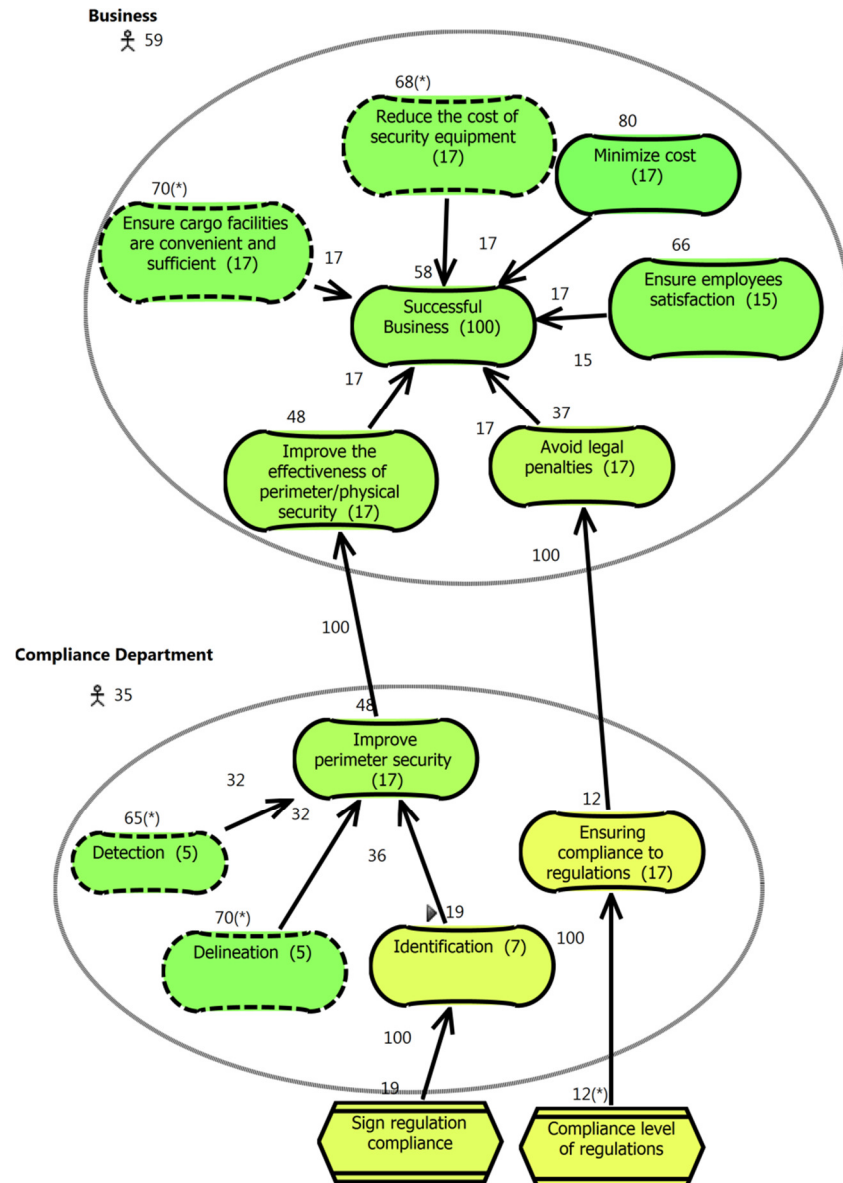


Figure 72, Compliance Department’s Satisfaction Level before Process Modification

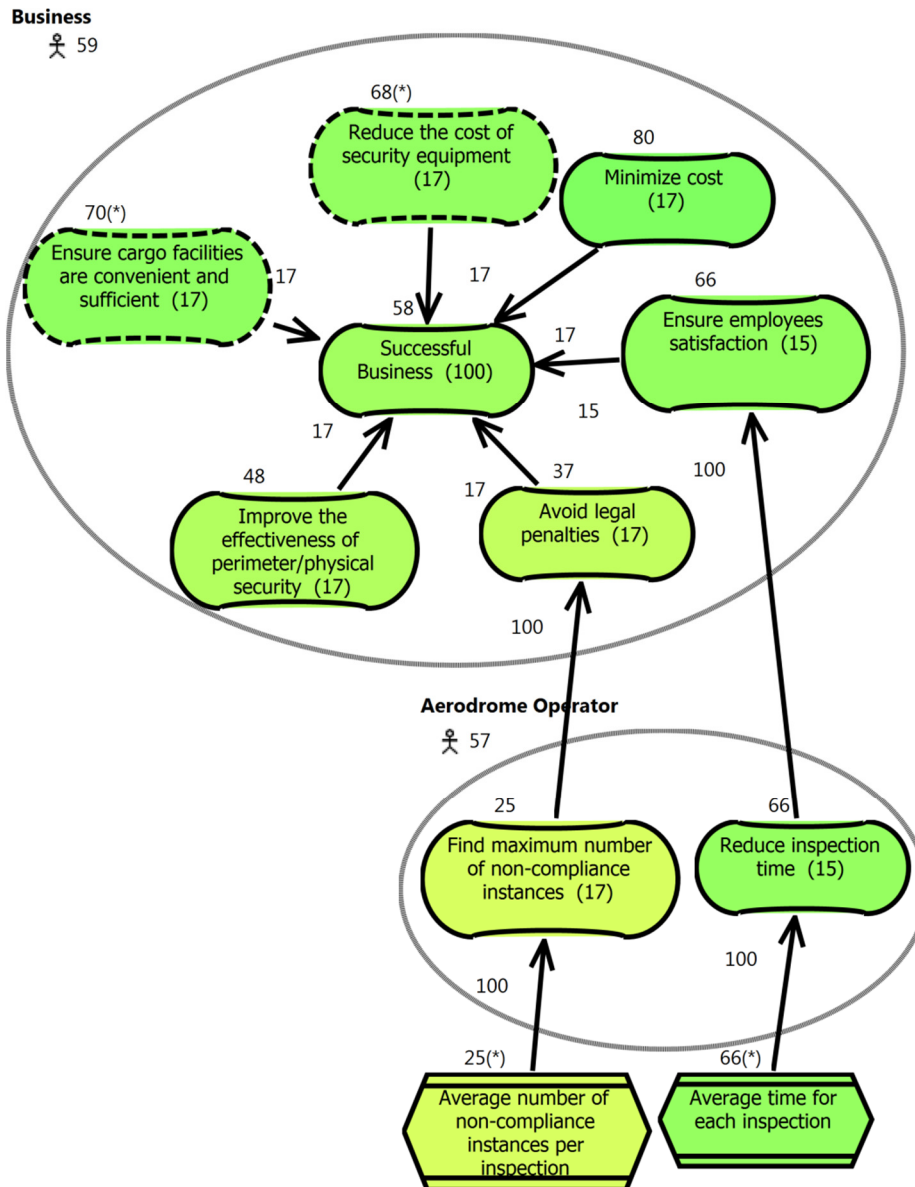


Figure 73, Aerodrome Operator’s Satisfaction Level before Process Modification

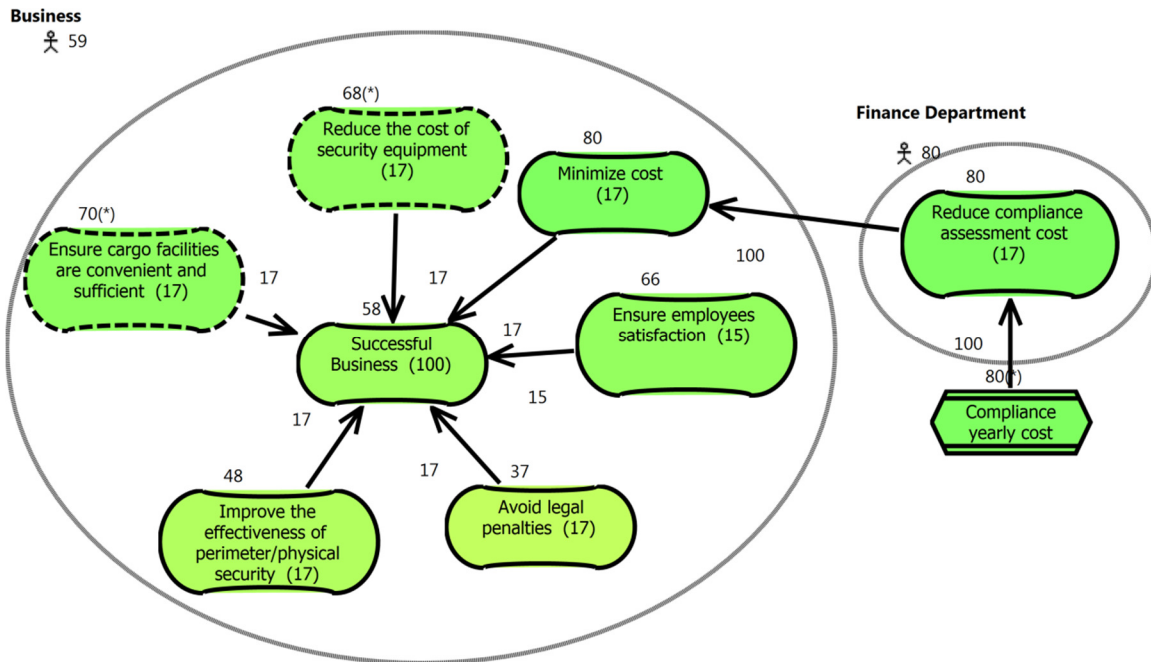


Figure 74, Finance Department's Satisfaction Level before Process Modification

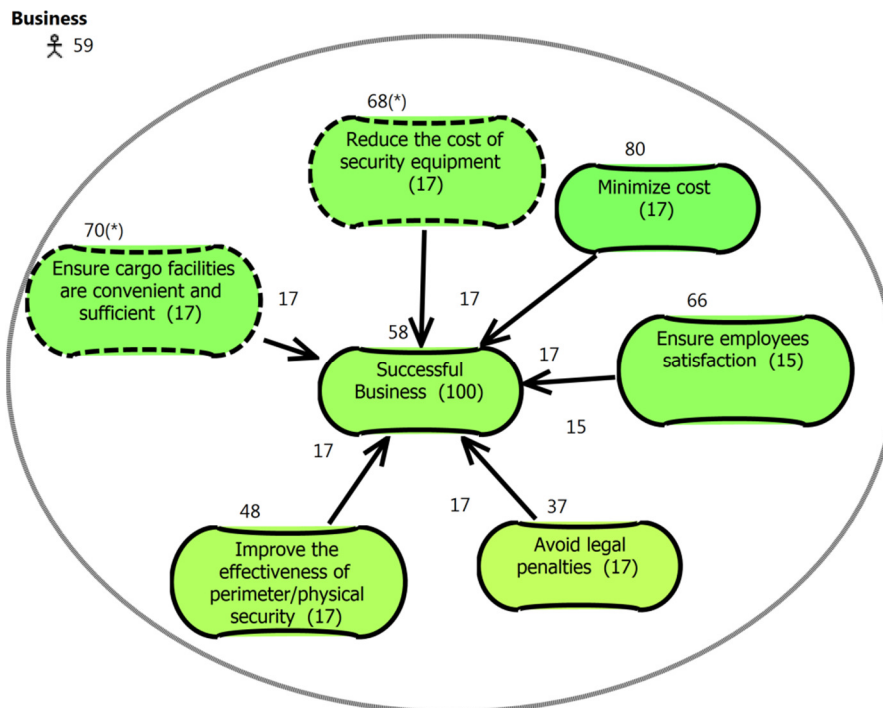


Figure 75, Business's Satisfaction Level before Process Modification

Actors	Satisfaction level
Before Process Modification	
Compliance Department	35
Aerodrome Operator	57
Finance Department	80
Business	59

Table 28, Satisfaction Level of Aerodrome Security Actors before Process Modification

Actor	Key Performance Indicator	Target	Threshold	Worst	Evaluation	Evaluation Level
Compliance Department	Sign regulation compliance	-	-	-	-	19
	Compliance level of regulations	40	32	0	33	12
Aerodrome Operator	Average time for each inspection	60	90	120	70	66
	Average number of non-compliance instances per inspection	6	2	0	3	25
Finance Department	Compliance yearly cost	50000	55000	60000	51000.0	80

Table 29, KPIs Values for Aerodrome Security Actors before Process Modification

6.3. Step C: Improvement

In this step, the business processes are improved based on the results highlighted in the quadrant diagram (Figure 71).

6.3.1 Rule Prioritization

As illustrated in Figure 71, rule R4 has the highest level of non-compliance whereas other rules are relatively compliant. The mathematical formula explained in section 5.3.1 is used to prioritize the rules. Table 30 illustrates the results.

Rule	Compliance	Importance	Importance $\times$ (100 – Compliance)
R1	90	7	70
R2	80	7	140
R3	80	7	140
R4	-42	1	142

Table 30, Priority between Sign Rules

The list of priorities based on compliance level and importance level for the other rules is shown in Table 31. Rule R4 has the highest priority, but closely followed by R2 and R3 (which would be impossible to understand by simply looking at the compliance level).

Priority	Rule
1	R4
2	R2,R3
3	R1

Table 31, Sign Rules Prioritization List

6.3.2 Business Process Improvement

Since R4 (Number of signs with a distance greater than 150m) takes priority among other rules, the business process (Sign Installation) associated with this rule should be improved. In this section, the modifications to do to this business process in order to improve the compliance level of R4 are explained.

Since one the objectives of IPCF is concerned with the use of a Business Intelligence tool (such as IBM Cognos) to compute the indicator evaluation values and generate compliance reports for stakeholders, the Sign Inspection business process is modified to take this concern into account. In the Sign Inspection (As-Is) process (see Figure 60), the Compliance Officer selects an area for inspection in a fairly random fashion, or based on instincts. This process can be improved in such a way that the Compliance Officer could view a relevant compliance dashboards and select an area that has not been inspected recently or an area recently inspected but where problems were detected that are now expected to be fixed (see Figure 78). It is the responsibility of Aerodrome Operators to

make the inspection data available as input to the BI system (see Figure 77). The Aerodrome Operators, in the as-is process, usually inspect an area and create a compliance notice that is usually paper-based and that includes the inspector's name, the date, and comments regarding the non-compliance issue. To enable the creation of reports and dashboards, a spreadsheet questionnaire is created for inspection (see Table 32). Once the questionnaire is filled by the inspectors, the values are published automatically to a database server (Figure 76).

#	Question
1	Inspector Name
2	Date of Inspection
3	Please indicate the sign location (A, B, C, D)
4	Please indicate the restricted area (1,2,3,4)
5	Does the restricted area have restricted sign? (Yes/No)
6	Please indicate sign Id
7	Please scale the sign distance (0,1,2,3,4)
8	Is the sign written in all required official languages (Yes/No)
9	Does the sign have a restricted symbol? (Yes/No)
10	Does the sign indicate that entry is restricted to authorized people? (Yes/No)

Table 32, Sign Inspection Questionnaire

SABT.signs - dbo.signreport			
	Column Name	Data Type	Allow Nulls
	recordid	numeric(18, 0)	☒
	location	nvarchar(50)	☒
	restrictedArea	nvarchar(50)	☒
	inspectionDate	date	☒
	inspectorName	nvarchar(50)	☒
	hasSign	nchar(10)	☒
	signId	nvarchar(50)	☒
	distanceScale	numeric(18, 0)	☒
	signLanguage	nchar(10)	☒
	signMentionsRestriction	nchar(10)	☒
	signMentionsRestrict...	nchar(10)	☒

Figure 76, Sign Inspection Table Design in Database Server (Microsoft SQL)

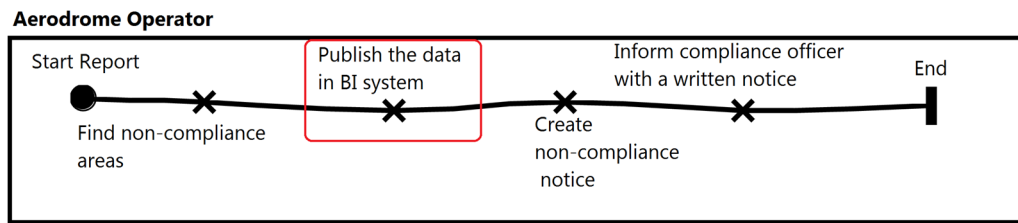


Figure 77, Report on Non-Compliance Areas Sub-Process (To-Be)

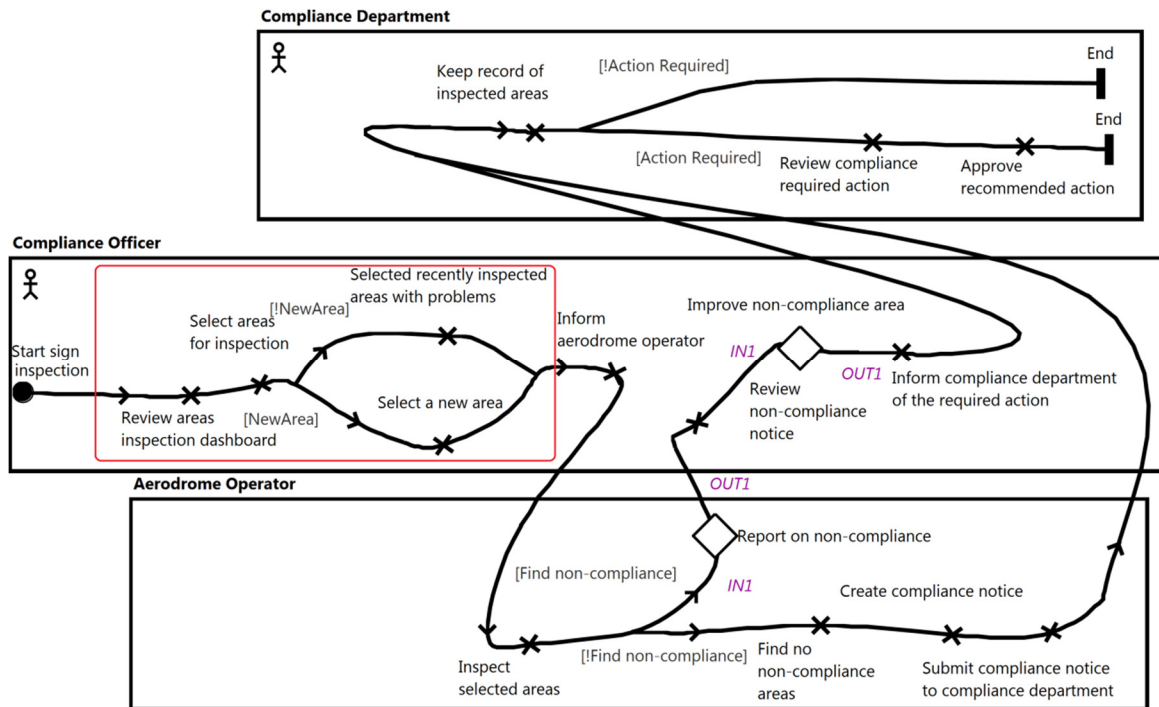


Figure 78, Sign Inspection Business Process (To-Be)

After having improved the Sign Inspection process, the IBM Cognos BI reports that return indicator evaluation values from compliance reports generated in IBM Cognos Report Studio can be produced and then used by different stakeholders. Before the Sign Inspection process modifications, KPI values for R1, R2, R3, and R4 needed to be computed manually from paper-based reports or natural language comments provided by inspectors. Therefore, extracting these values was a time-consuming and error-prone process. The use of more formal questionnaires and of BI tools makes this much easier. Figure 79, Figure 80, Figure 81, and Figure 82 are snapshots from such BI reports that indicate KPI evaluation values (overall counts) for R1, R2, R3, and R4 respectively. These reports indicate the same KPI value for the rules in section 6.2.1. However, getting these

values from Cognos IBM is much faster and easier than getting them from paper-based sources.

In addition, KPI evaluation values in jUCMNav strategies can be initialized automatically from the BI tool reports (using imported text files or through existing extension points) instead of being input manually.

Number of signs without Required Official Languages

recordid	location	restrictedArea	signId	signLanguage
4	A	1	abc127	No
5			abc129	No
		1 - Count	2	
A - Count			2	
Overall - Count			2	

Figure 79, R1 KPI Value (As-Is Process)

Number of Restricted Areas without Sign

recordid	location	restrictedArea	hasSign
26	B	2	No
B - Count			1
76	C	2	No
75		3	No
64		4	No
C - Count			3
Overall - Count			4

Figure 80, R2 KPI Value (As-Is Process)

Number of Signs without Restriction to Authorized Person

recordid	location	restrictedArea	signId	signMentionsRestrictedtoAuthorized
48	B	2	abc172	No
49			abc173	No
		2 - Count		2
B - Count			2	
72	C	3	abc196	No
		3 - Count		1
71		4	abc195	No
	4 - Count		1	
C - Count			2	
Overall - Count			4	

Figure 81, R3 KPI Value (As-Is Process)

Number of Signs with Distance <=2

recordid	location	restrictedArea	signId	distanceScale
1	A	1	abc123	0
2			abc125	2
3			abc126	2
4			abc127	2
5			abc129	2
		1 - Count		5
A - Count				5
35	B	1	abc159	0
36			abc160	1
37			abc161	2
38			abc162	2
39			abc163	2
40			abc164	2
53			abc177	2
54			abc178	2
55			abc179	2
			1 - Count	
47	2		abc171	2
48			abc172	2
49			abc173	1
51			abc175	0
52			abc176	2
			2 - Count	
34	3	abc158	0	
		3 - Count		1

Number of Signs with Distance <=2

recordid	location	restrictedArea	signId	distanceScale		
41	B	4	abc165	2		
42			abc166	2		
43			abc167	2		
45			abc169	2		
46			abc170	2		
			4 - Count		5	
B - Count				20		
56	C	1	abc180	2		
69			abc193	2		
85			abc209	0		
86			abc210	1		
87			abc211	2		
88			abc212	2		
89			abc213	2		
90			abc214	2		
			1 - Count		8	
58			2	abc182	2	
			2 - Count		1	
66	3		abc190	2		
67			abc191	2		
72			abc196	2		
73			abc197	0		
74			abc198	2		
84			abc208	0		
			3 - Count		6	

Number of Signs with Distance <=2

recordid	location	restrictedArea	signId	distanceScale		
60	C	4	abc184	2		
62			abc186	1		
63			abc187	2		
65			abc189	1		
70			abc194	2		
		4 - Count		5		
C - Count				20		
97	D	2	abc221	2		
98			abc222	2		
99			abc223	1		
			2 - Count		3	
91			4	abc215	2	
92	abc216	2				
93	abc217	2				
94	abc218	2				
95	abc219	2				
96	abc220	2				
		4 - Count		6		
D - Count				9		
Overall - Count				54		

Figure 82, R4 KPI Value (As-Is Process)

A tool such as IBM Cognos Business Insight can also be used to generate interactive dashboards for stakeholders. As an example, Figure 83 illustrates a sample *Sign dashboard* filtered (highlighted in red) by inspector name, location, distance scale. This figure shows the signs that are inspected by inspector John Howard, in locations B and D, and with distance between 0 and 2 (*Sign report* on left).



Figure 83, Sign Dashboard

Users of such a dashboard can change the value of existing filters on the fly and add new filters or reports to perform ad-hoc analysis on the data. In addition, the *Inspection report* on the right hand side shows the inspected area, inspection date and inspector name. By looking at this report, compliance officers can assess the status of restricted areas. For instance, the area highlighted in yellow (extreme right) has not been inspected at all by any inspector.

Next, the business process related to R4 (Number of signs with a distance greater than 150m) will be improved. In the as-is version of this process, the Aerodrome Operators never used to check the physical distance of the signs. In the to-be version of this process, a Check physical distance responsibility is added to the Sign Installation business process (Figure 84). In addition, when an Aerodrome Operator submits a proposal to EPMD, a new responsibility called Submit a location map is added (Figure 85), so that EPMD can also check the distance between the sign and all other signs in close proximity prior to sign approval. If the sign distance does not meet the minimal requirements, the EPMD informs the Aerodrome Operator of the proposal rejection.

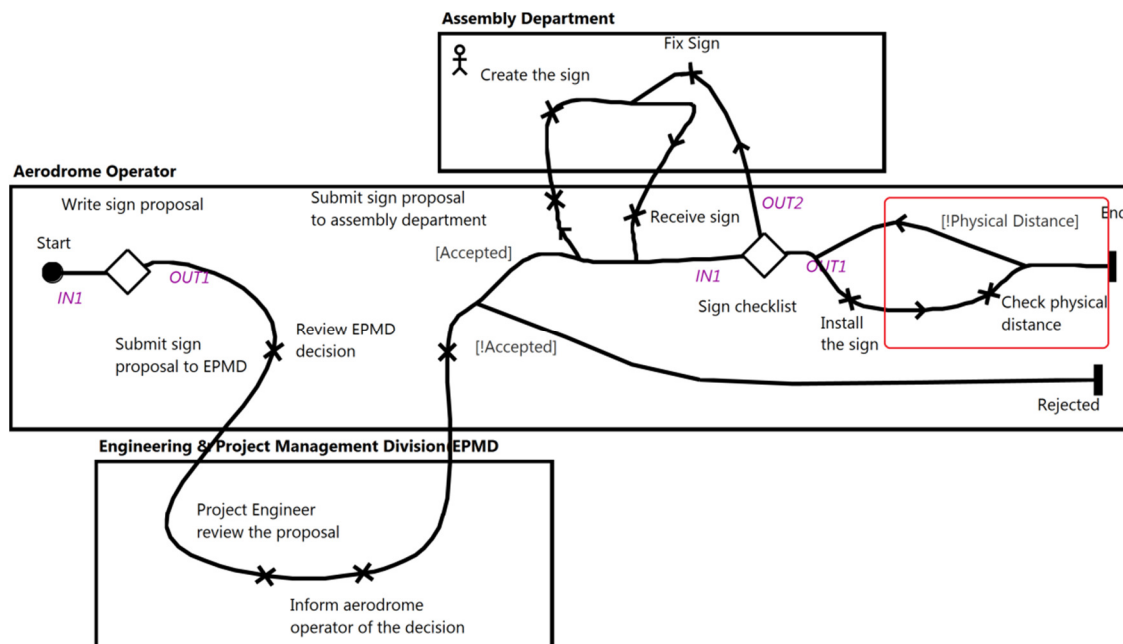


Figure 84, Sign Installation Business Process (To-Be)

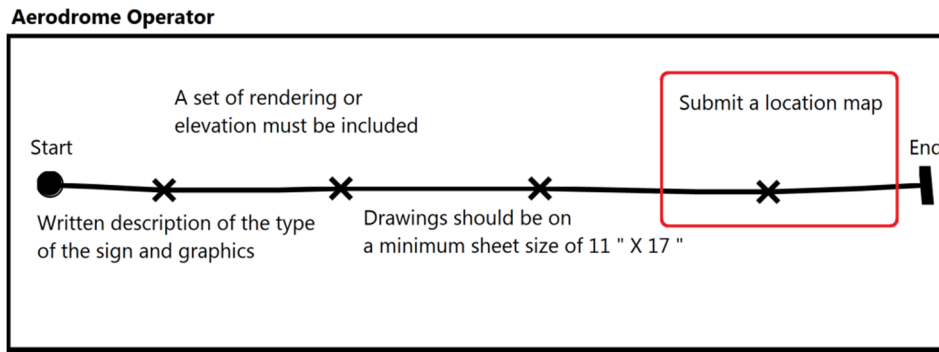


Figure 85, Write Sign Proposal Sub-Process (To-Be)

6.4. Step D: Monitoring

As explained in section 4.5, in the monitoring step, not only are the modified processes monitored to observe whether expected changes are happening, but also organization goals are monitored in order to detect potential undesirable side-effects.

6.4.1 Analysis of Three Strategies

In section 6.2, the satisfaction level of actors in the organization and of rules *before* process modifications using the “BeforeModificationToSignInstallationProcess” GRL strategy was computed. In this section, the satisfaction level of actors and rules *after* process modifications is illustrated by defining couple of new strategies “AfterModificationToSignInstallationProcess1”, “AfterModificationToSignInstallationProcess2”, and “AfterModificationToSignInstallationProcess3”. The process model is the same in all three strategies, whereas different KPI evaluation values are assumed in each strategy to showcase and explore various potential outcomes. Such strategies can be defined at modification time as a prediction model and what-if scenario analysis in order to support decision making [108] (as done in this section, because real monitoring data was unavailable), or it can result from actual monitoring of the organization sometime after the process modification. Since predictive strategies are used here, many can be defined easily to explore different scenarios. However, the prediction is not limited only to these strategies.

In this example, for strategy AfterModificationToSignInstallationProcess1, an improvement for R4 “Distance NOT > 150m” is expected after modifying this process. Indeed, as illustrated in Figure 86, this process modification is assumed to decreases R4’s

KPI, “Number of signs with a distance greater than 150m”, from 54 to 5 instances. Therefore, the satisfaction level for R4 has significantly improved from -42 to 75. Table 33, illustrates the KPI values that changed for different actors, after process modification for strategy 1. By comparing the actor satisfaction values before and after modifying the Sign Installation business process and Write Sign Proposal sub-process (see Table 34), one can see this modification has a slightly negative effect on the Finance Department’s satisfaction level (see Figure 89). However, the process improvement leads to a positive effect on the Compliance Department’s satisfaction level (see Figure 87), Aerodrome Operator’s satisfaction level (see Figure 88), and on the overall satisfaction of the Business (See Figure 90).

The main modification to the Sign Installation business process and Write Sign Proposal sub-process is to submit a location map that indicates the physical location of the sign by Aerodrome Operator to EPMD, as well as checking the physical distance of the sign after installing the sign. This modification has a negative impact on the Reduce inspection time goal of the Aerodrome Operator. However, it has a positive effect on the Find maximum number of non-compliance instances goal by improving the chance of finding signs that do not comply with the “Distance NOT > 150m” rule. Globally, the positive effects outweigh the negative effects, and the satisfaction level of this stakeholder improves from 57 to 65.

The improvements also have positive effects on the Identification goal of perimeter security, as illustrated in Figure 87. Improving the Sign Inspection process has a direct effect on the Sign regulation compliance KPI, which is the sole contributor to the Identification goal. In addition, the Ensuring compliance to regulations goal is improved for the Compliance Department actor.

However, the modification has a slightly negative effect on the Reduce compliance assessment cost goal of the Finance Department. According to the Simply Hired website [116], aerodrome operation crews working in Canada earn an average salary of \$32,000. It is assumed that two Aerodrome Operators are required to do the inspection twice in a year. In addition, it is assumed to take an Aerodrome Operator 80 minutes to do an inspection after the modifications, whereas this time was 70 minutes previously. It

is also assumed that an Aerodrome Operator works 49 weeks in a year, at 35 hours per week. Therefore, the total cost of two Aerodrome Operators participating in an inspection twice a year would be about \$741 more. The evaluation value of this KPI changes from 51000 to 51746, and this has a slightly negative side effect on the Financial Department's satisfaction level. On the other hand, this process modification has a positive impact on the Compliance Department's goals as well as on the Aerodrome Operator's goals.

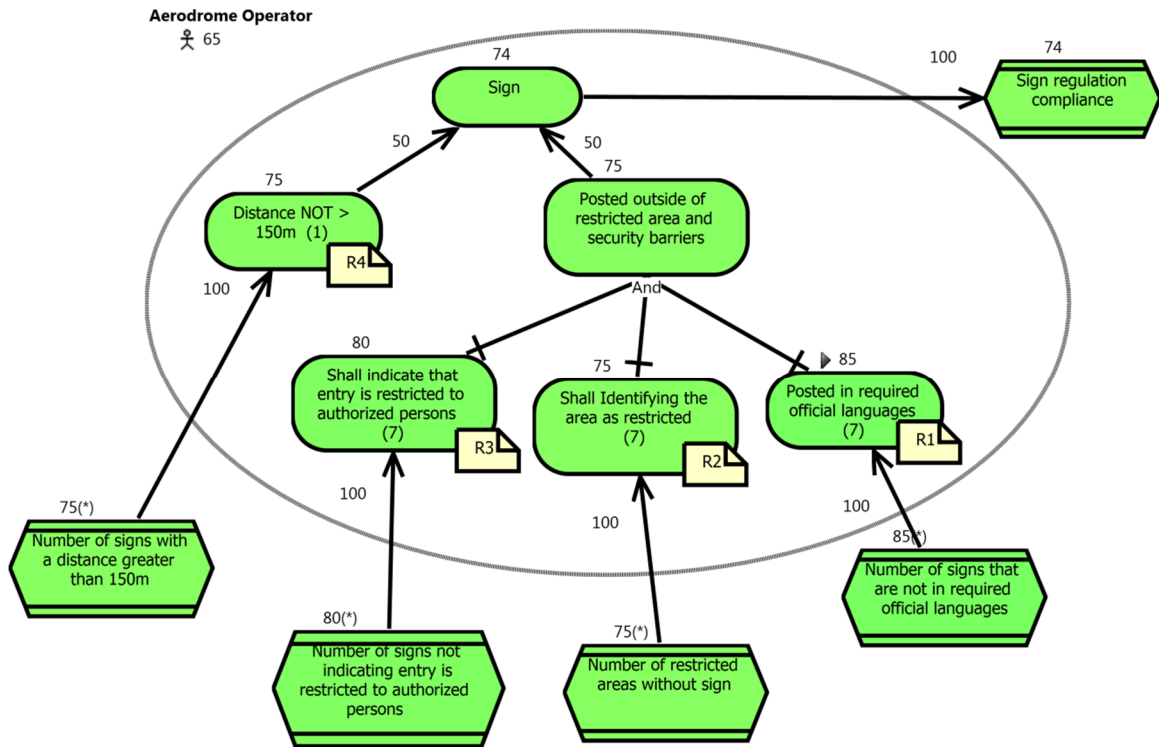


Figure 86, Sign Regulation Satisfaction Level (After Modification)

Actor	Key Performance Indicator	Target	Threshold	Worst	Evaluation	Evaluation Level
Compliance Department	Sign regulation compliance	-	-	-	-	74
	Compliance level of regulations	40	32	0	38	75
Aerodrome Operator	Average time for each inspection	60	90	120	80	33
	Average number of non-compliance instances per inspection	6	2	0	5	-75
Finance Department	Compliance yearly cost	50000	55000	60000	51746.0	65

Table 33, KPIs Values for Aerodrome Security Actors after Process Modification-Strategy 1

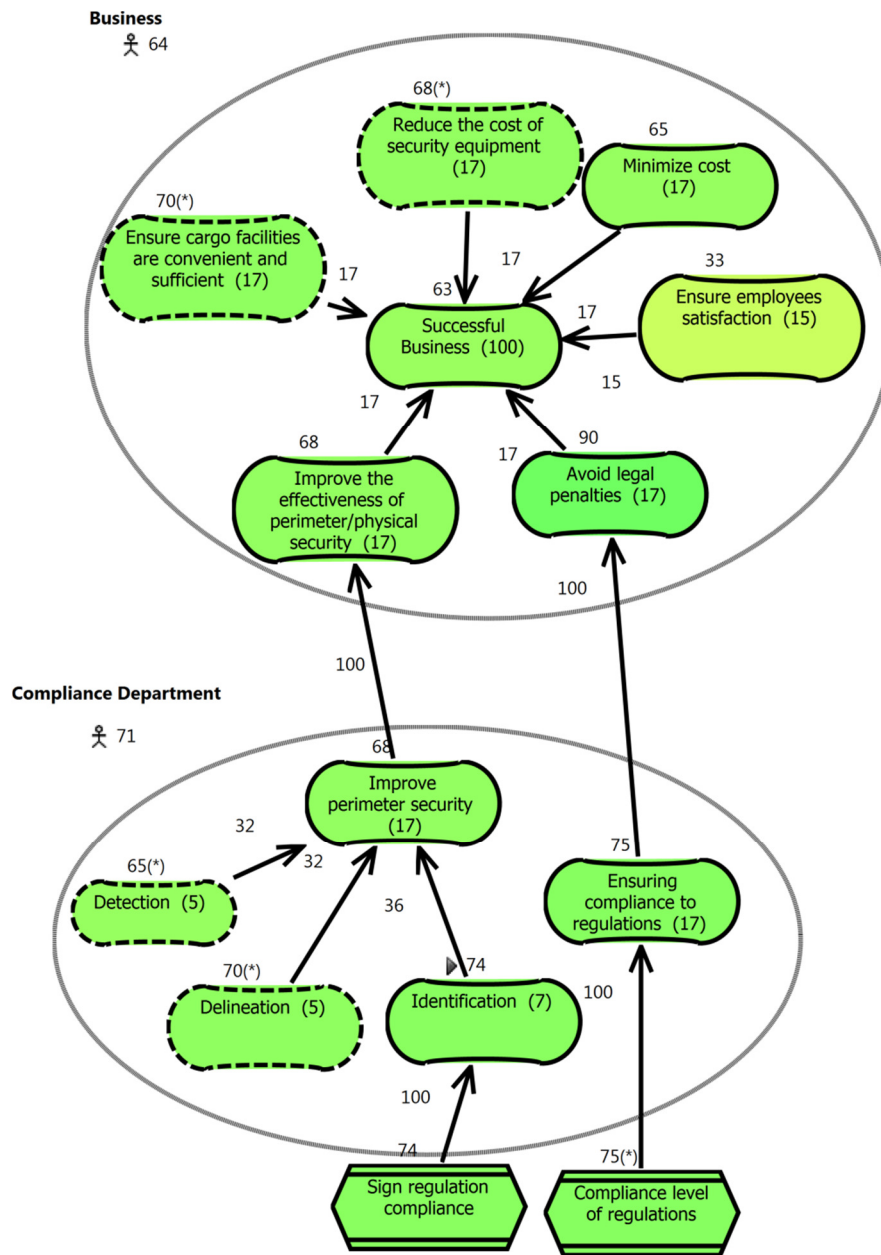


Figure 87, Compliance Department’s Satisfaction Level after Process Modification-
 Strategy 1

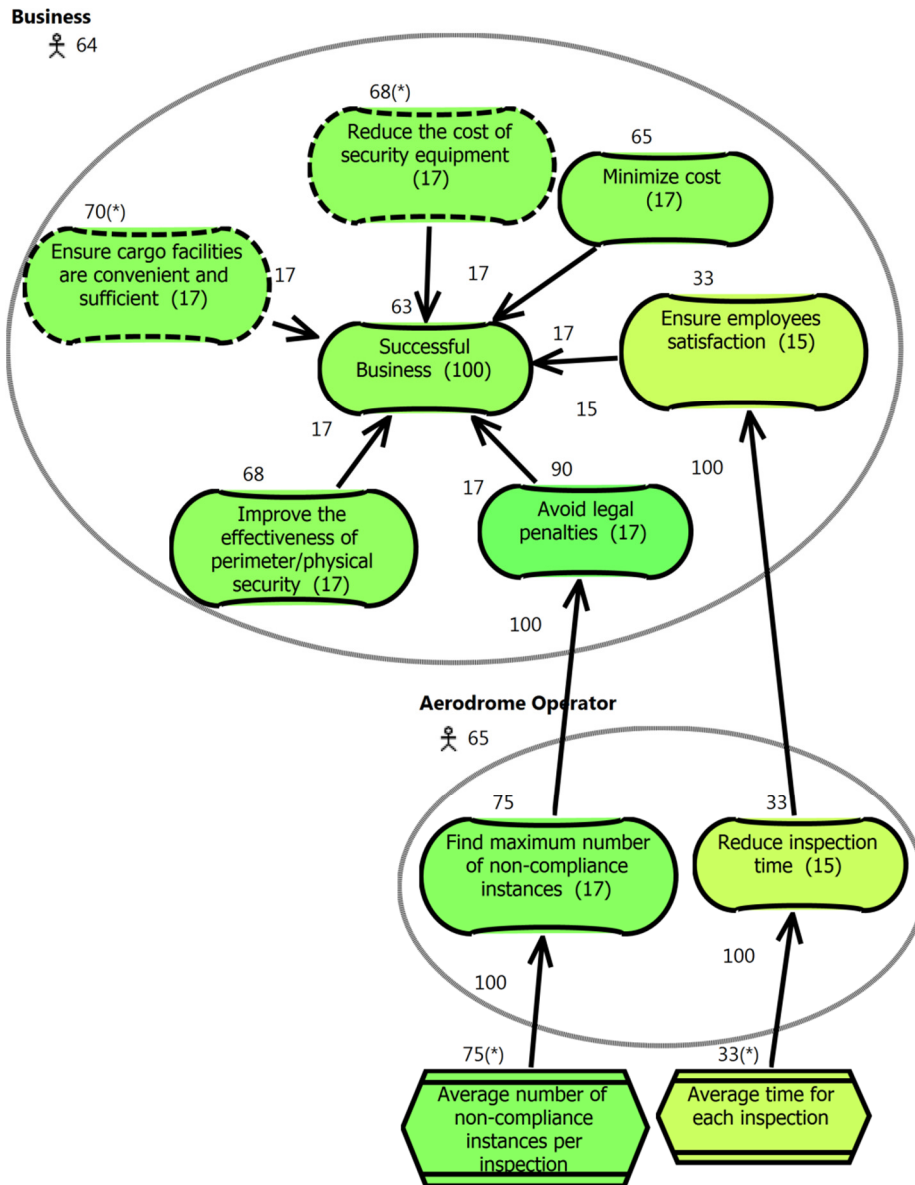


Figure 88, Aerodrome Operator’s Satisfaction Level after Process Modification-
 Strategy 1

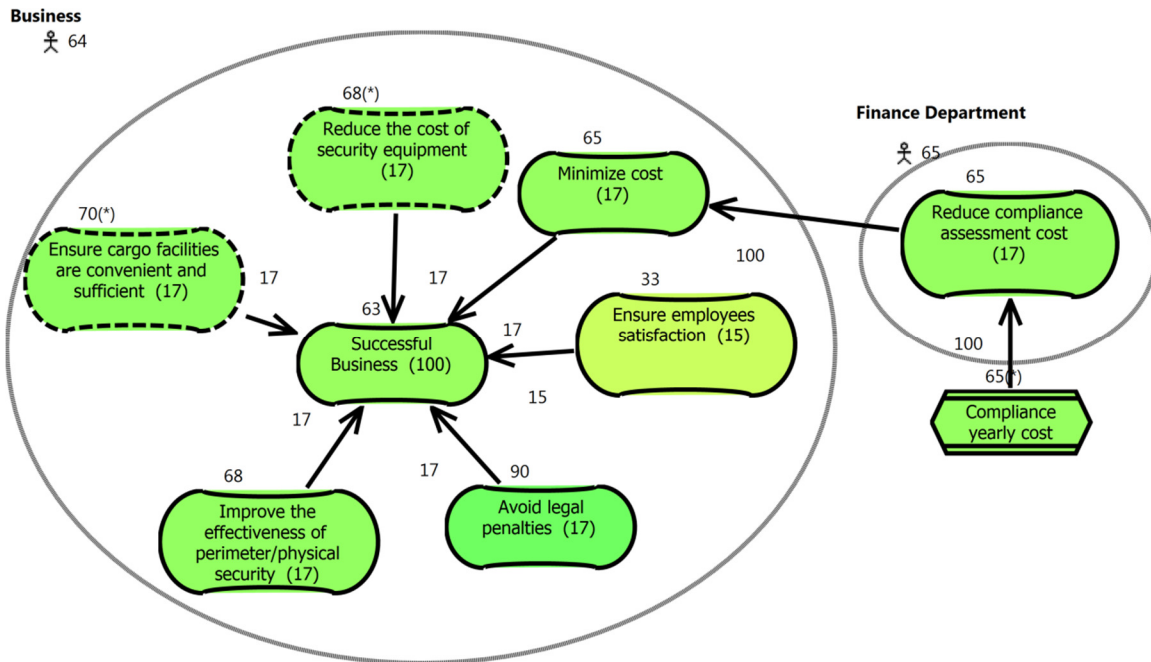


Figure 89, Finance Department's Satisfaction Level after Process Modification- Strategy 1

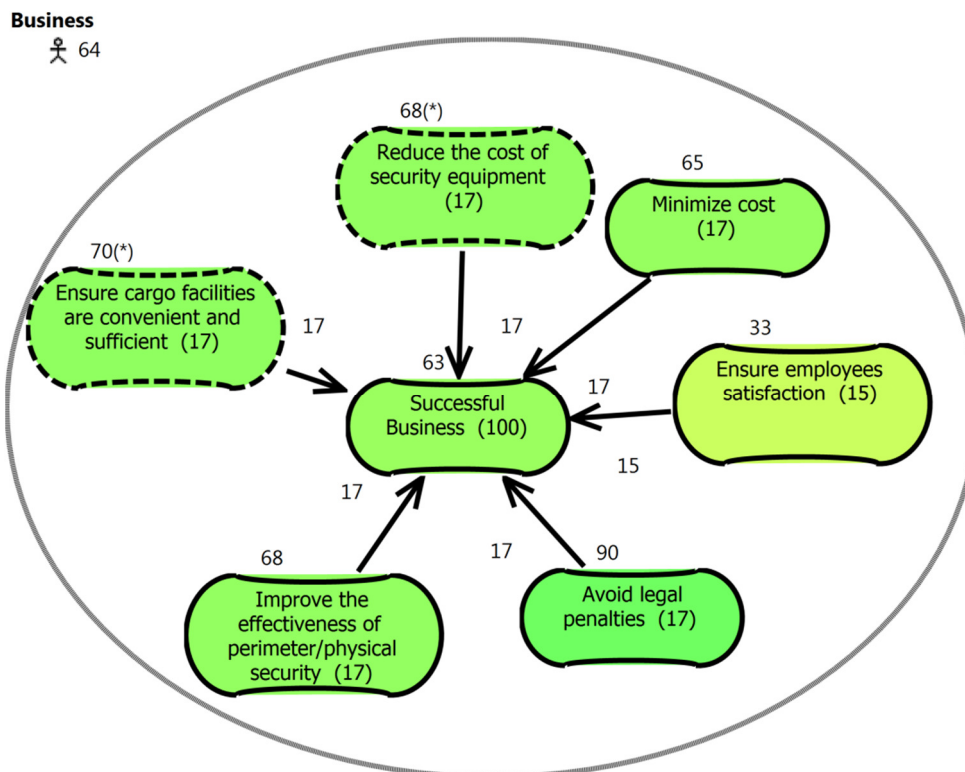


Figure 90, Business's Satisfaction Level after Process Modification- Strategy 1

Actors	Satisfaction level	Satisfaction level
	Before Process Modification	After Process Modification Strategy1
Compliance Department	35	71
Aerodrome Operator	57	65
Finance Department	80	65
Business	59	64

Table 34, Comparison between Satisfaction Level of Aerodrome Security Actors before and after Process Modification- Strategy 1

For strategy 2 (i.e., AfterModificationToSignInstallationProcess2) , it is assumed, after process modification, that 110 minutes will be required by an Aerodrome Operator to do inspections instead of the 70 minutes before process modifications and of the 80 minutes explored in strategy 1.

Table 35, illustrates the KPIs values that changed for different actors, after process modification for strategy 2. By comparing the actor satisfaction values before and after modifying the Sign Installation business process and Write Sign Proposal sub-process (see Table 46), one can observe that this has a dramatic negative effect on the Finance Department's satisfaction level and on the Aerodrome Operator's satisfaction level, as well as on the overall satisfaction of the Business. However, the process improvement leads to a positive effect on the Compliance Department's satisfaction level, (see Table 36, Table 37).

Actor	Key Performance Indicator	Target	Threshold	Worst	Evaluation	Evaluation Level
Compliance Department	Sign regulation compliance	-	-	-	-	74
	Compliance level of regulations	40	32	0	38	75
Aerodrome Operator	Average time for each inspection	60	90	120	110	-66
	Average number of non-compliance instances per inspection	6	2	0	5	75
Finance Department	Compliance yearly cost	50000	55000	60000	53984	20

**Table 35, KPIs Values for Aerodrome Security Actors after Process Modification-
Strategy 2**

Intentional Element	Satisfaction Level			
	As-Is	Strategy 1	Strategy 2	Strategy 3
Successful Business	58	63	42	60
Reduce the cost of security equipment	68	68	68	68
Ensure cargo facilities are convenient and sufficient	70	70	70	70
Improve the effectiveness of perimeter/physical security	48	68	68	57
Avoid legal penalties	17	90	90	87
Ensure employees satisfaction	15	33	-66	33
Minimize cost	80	65	20	65
Improve perimeter security	48	68	68	57
Detection	65	65	65	65
Delineation	70	70	70	70
Identification	19	74	74	42
Ensuring compliance to regulations	12	75	75	37
Find maximum number of non-compliance instances	25	75	75	50
Reduce inspection time	66	33	-66	33
Reduce compliance assessment cost	80	65	20	65
Sign	19	74	74	42
Distance NOT > 150m	-42	75	75	10

Table 36, Satisfaction Level of Intentional Elements for Strategies 1, 2, and 3

Actors	Satisfaction level	Satisfaction level
	Before Process Modification	After Process Modification- Strategy 2
Compliance Department	35	71
Aerodrome Operator	57	37
Finance Department	80	20
Business	59	42

**Table 37, Comparison between Satisfaction Level of Aerodrome Security Actors before
and after Process Modification- Strategy 2**

Table 38 illustrates the KPI values that changed for different actors, after process modification for strategy 3. By comparing the actor satisfaction values before and after modifying the Sign Installation business process and Write Sign Proposal sub-process (see Table 46 and Table 39), it is observed that this leads to negative effects on the Finance Department's satisfaction level and on the Aerodrome Operator's satisfaction level. However,

the process improvement leads to a positive effect on the Compliance Department's satisfaction level, and on the overall satisfaction of the Business (see Table 36 and Table 39).

For strategy 3 (AfterModificationToSignInstallationProcess3), it is assumed after process modification that R4 "Distance NOT > 150m" will be improved. In strategies 1 and 2, the number of non-compliance instances has decreased from 54 to 5. However, in strategy 3, the number of instance decreases from 54 to 18 only. The inspection time is set to 80 minutes, as in strategy 1. As illustrated in Table 36, the satisfaction level for R4 (Distance NOT > 150m) has significantly improved from -42 (before modification) to 10 (after modification). This has obviously a positive effect on the Compliance Department's satisfaction level. However, this leads to a negative effect on the Finance Department's satisfaction level.

Actor	Key Performance Indicator	Target	Threshold	Worst	Evaluation	Evaluation Level
Compliance Department	Sign regulation compliance	-	-	-	-	42
	Compliance level of regulations	40	32	0	35	37
Aerodrome Operator	Average time for each inspection	60	90	120	80	33
	Average number of non-compliance instances per inspection	6	2	0	4	50
Finance Department	Compliance yearly cost	50000	55000	60000	51746.0	65

Table 38, KPIs Values for Aerodrome Security Actors after Process Modification- Strategy 3

Actors	Satisfaction level	Satisfaction level
	Before Process Modification	After Process Modification Strategy3
Compliance Department	35	50
Aerodrome Operator	57	56
Finance Department	80	65
Business	59	61

Table 39, Comparison between Satisfaction Level of Aerodrome Security Actors before and after Process Modification- Strategy 3

6.4.2 Improved Visualization of Strategy Differences with jUCMNav

The study of these three what-if scenarios captured as strategies has led to much information that needs to be consumed by the analyst. A tool such as jUCMNav enables the analyst to switch easily between strategies, or to export their results as reports or as Excel spreadsheets for further analysis. However, it is still difficult to compare the results of two given strategies visually.

Figure 91, Figure 92, Figure 93, and Figure 94 illustrates a new jUCMNav feature that highlights strategy differences visually in terms of evaluations of intentional elements and actors [8]. The difference is computed between a base strategy (e.g., Figure 91) and a current strategy (e.g., Figure 92, Figure 93, Figure 94) on a per element basis (including actors). As the standard GRL scale for quantitative evaluations is $[-100..100]$, the difference scale is $[-200..200]$ because one evaluation can go from +100 down to -100, or from -100 up to +100. Differences are displayed between angle brackets, again with color feedback ($<-200>$ in red, $<0>$ in yellow, and $<+200>$ in green), so the trade-offs can be understood at a glance. In addition, Table 40 also indicates the actors' satisfaction values before and after process modification for all strategies. As illustrated in this table strategy 1 (Figure 92) and strategy 3 (see Figure 94) improve business objectives, whereas strategy 2 (see Figure 93) has a negative effect on business objectives, particularly on the Finance Department's satisfaction level.

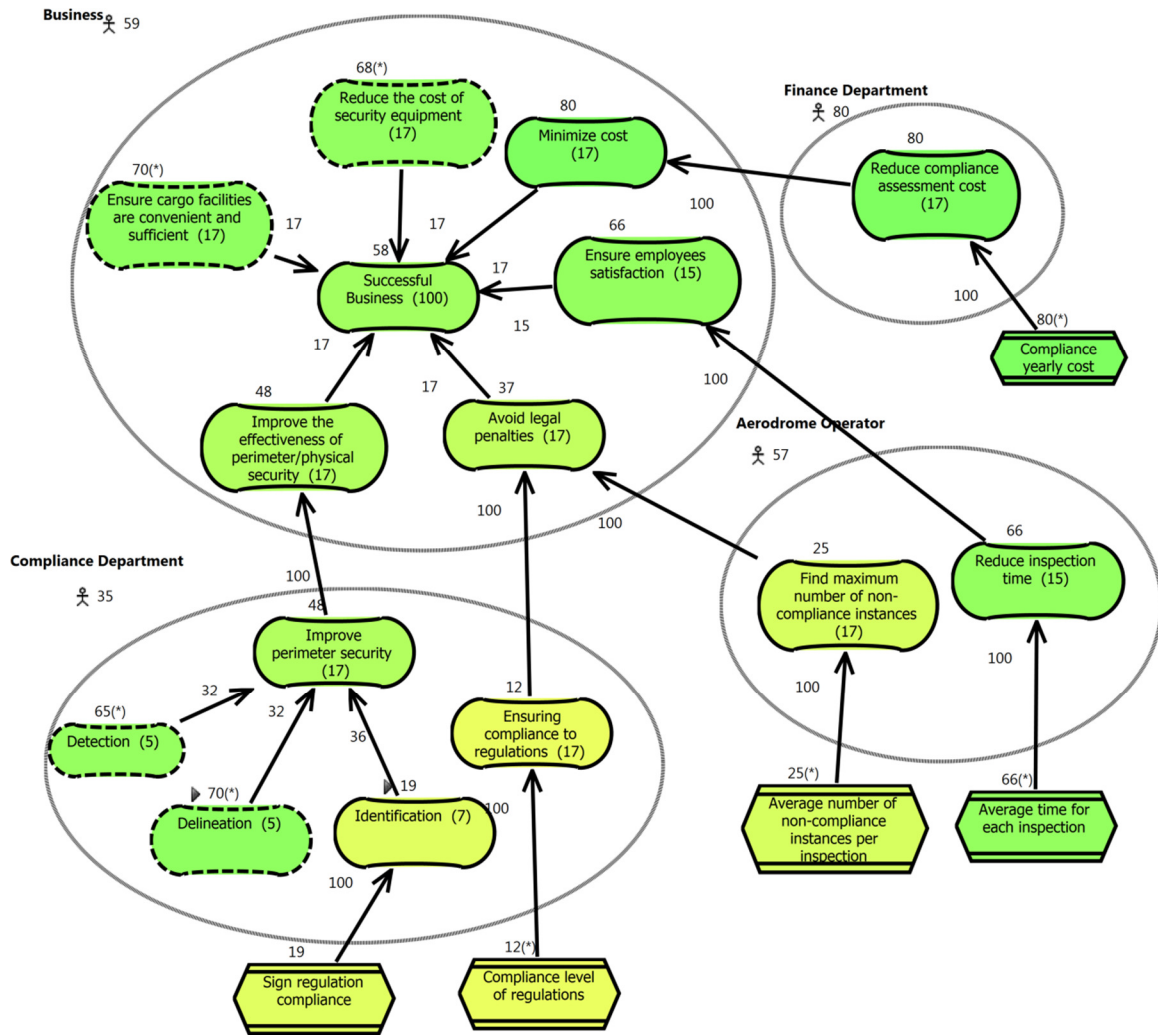


Figure 91, Base Strategy

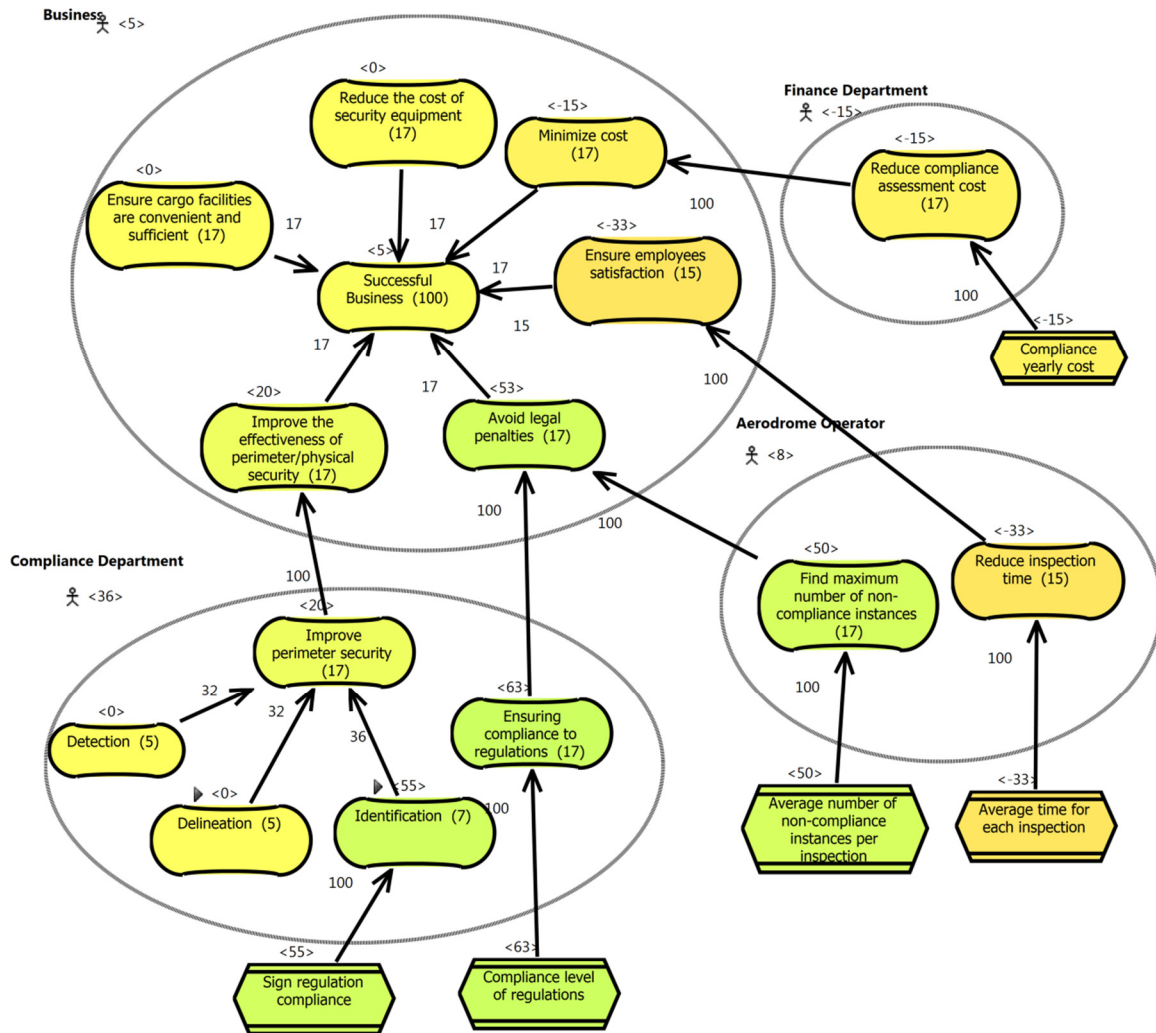


Figure 92, Difference: Base Strategy- After Process Modification Strategy 1

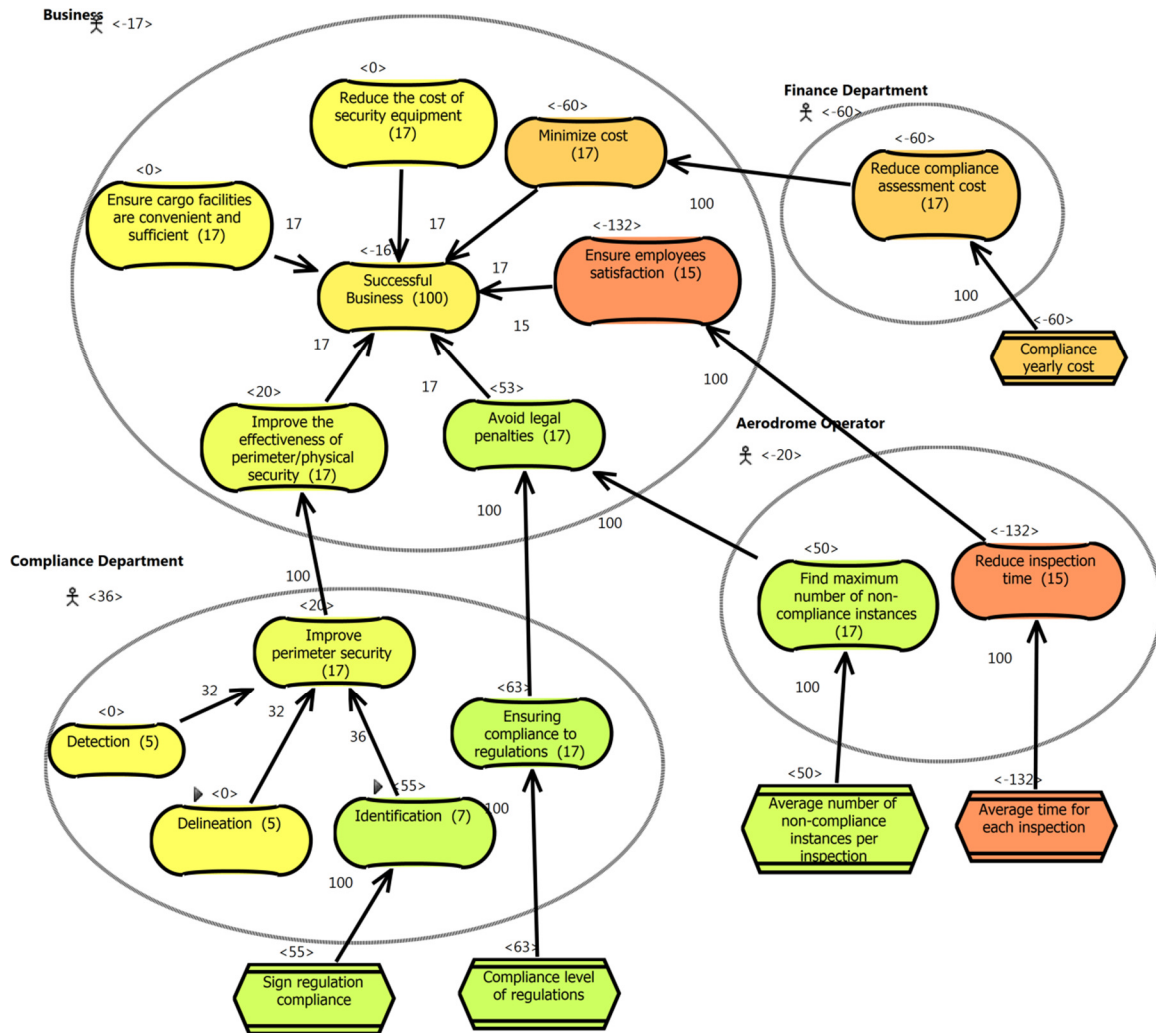


Figure 93, Difference: Base Strategy- After Process Modification Strategy 2

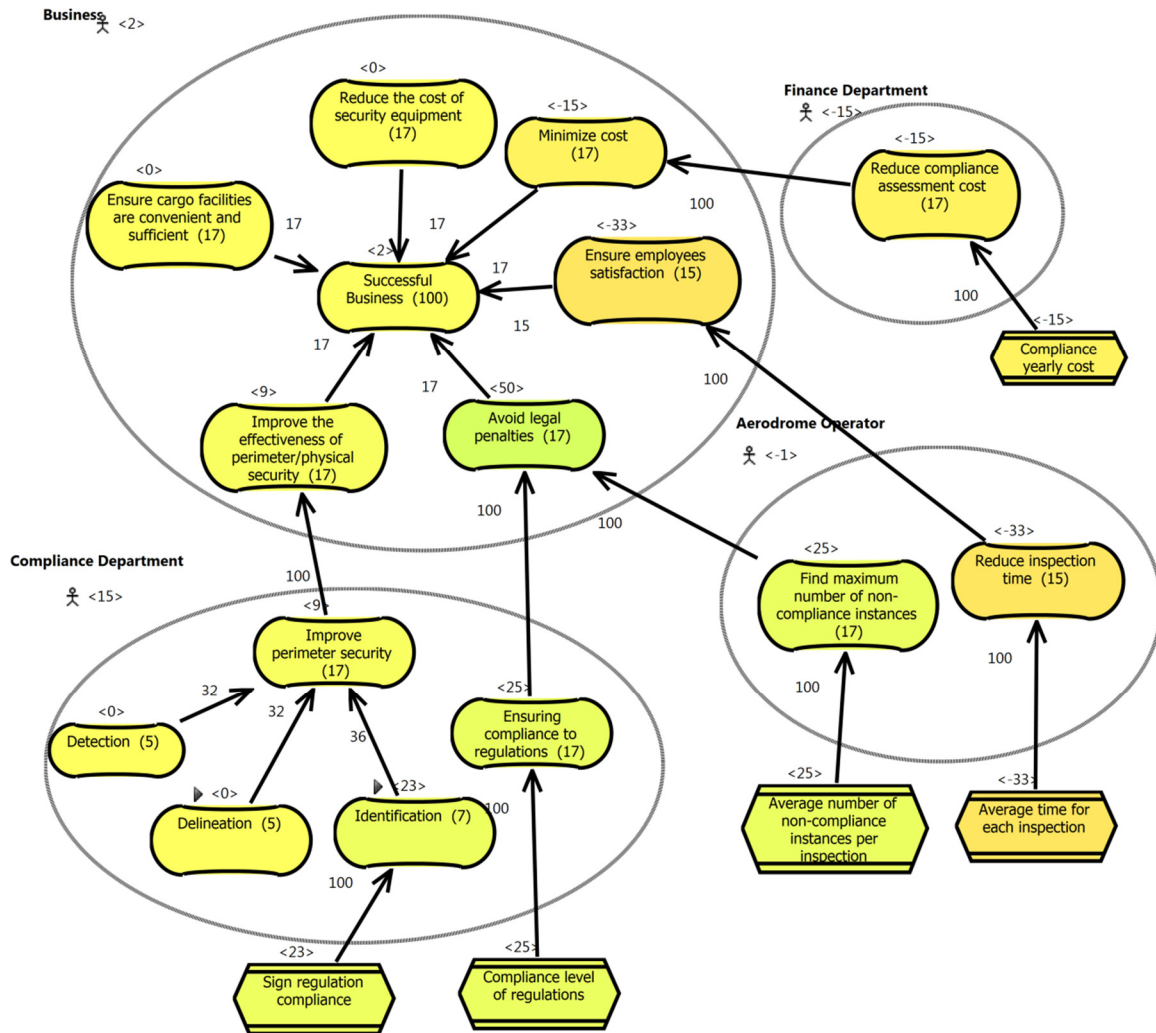


Figure 94, Difference: Base Strategy- After Process Modification Strategy 3

Actors	Satisfaction level	Satisfaction level		
	Before Process Modification	After Process Modification- Strategy1	Strategy2	Strategy3
Compliance Department	35	71	71	50
Aerodrome Operator	57	65	37	56
Finance Department	80	65	20	65
Business	59	64	42	61

Table 40, Comparison between Satisfaction Level of Aerodrome Security Actors before and after Process Modification- All Strategies

6.5. Summary

In this chapter, all steps of the Indicator Policy-based Compliance Framework method were illustrated using a realistic aerodrome security example.

The business goals of the organization were modeled, together with sign inspection and sign installation business processes and KPIs. Goals were linked to related business processes through URN links. Then the sign policy, its rules and finally their KPIs were modeled. In the evaluation step, four GRL strategies were identified to initialize KPIs and evaluate the organization satisfaction level and policy compliance level, before (with `BeforeModificationToHiringProcess`) and after modifications to a business process (with `AfterModificationToHiringProcess1`, `AfterModificationToHiringProcess2`, and `AfterModificationToHiringProcess3`, also referred to as strategies 1, 2, and 3). In addition, the importance level of each policy/rule and intentional element contributing to the business was calculated through the algorithm proposed in section 4.3. Then, a quadrant diagram was used to display the situation of rules based on these compliance and importance values.

In the improvement, the most important, non-compliant business process was modified by adding new BI-related responsibilities. IBM Cognos was used as an input, to compute the indicators required by the sign policy model in jUCMNav, and as an output, as a sample compliance dashboard and several reports targeting stakeholders were created. The example illustrated that using a combination of BI reports and URN compliance models provides a powerful toolkit for compliance measurement and analysis. While BI reports are useful for reporting on data and ad-hoc filtering and analysis, URN models help with goal-oriented and visual analysis of the compliance model, as well as of the impact of modifications (predicted or real) on business goals, stakeholders, and business processes. The latter capabilities were also exploited in the monitoring steps, where a new jUCMNav feature was developed to compare the results of two strategies, visually.

The next chapter will formalize a measured compliance profile for GRL, with suitable stereotypes, well-formedness constraints, a modified analysis algorithm for GRL model families, as well as an extension of the current jUCMNav tool to support the above profile, with appropriate visualizations.

Chapter 7. Specifying and Analyzing Goal Model Families with GRL

The focus of this chapter is on the particular problem of modeling complex regulations that apply to multiple types of organizations, based on a number of criteria. There are many regulations to be modeled, and these models can be used for compliance assessment by regulators. For example, Transport Canada regulations apply differently depending on the aerodrome type targeted. To have one goal model per type of organization would require significant maintenance effort if/when the legal context evolved, with the additional risk of introducing inconsistencies and other types of errors in the model. In this context, what is needed is a way to capture a family of goal models, whose individual members can be extracted for compliance analysis.

As suggested in the literature review (section 2.8), a goal modeling language can be tailored to support the concept of a model family, and hence mitigate the risks of inconsistencies while minimizing maintenance effort. This chapter formalizes the profile and algorithms needed to support the guidelines #7 (about Conditions) and #10 (about Regulated Types) in section 4.2.2, but the family concept and tools developed here are applicable in a more generic context to support variability in goal models. An example related to aerodrome regulations is described in section 7.1, followed by requirements for the support of families of goal models. In section 7.2, the experiment with modeling regulation families using conditional nodes and dependency links in GRL are reported and elaborated on current limitations of GRL. In order to solve these limitations, section 7.3 introduces a GRL profile as well as a new propagation algorithm, which are illustrated on the aerodrome regulations example. The stereotypes used in this new profile (and formalized in section 7.3.3) are concerned with conditions and types of organizations; they are independent from potential regulation structure stereotypes (*«part»*, *«sub-part»*, etc.) covered in guideline #2 of section 4.2.2 and mainly used for traceability to source regulations and for helping understand the resulting GRL models. Although other

researchers have explored the concept of variability (or family) in other goal modeling languages, as discussed in section 2.8, what exists in the literature is insufficient in a compliance context and does not exploit the full potential of GRL. The concepts required to address the specific needs for this research are hence formalized as a GRL profile in this part of the thesis.

7.1. Example Illustrating the Issues

The following example illustrates why modeling and analyzing of regulations that apply to multiple types of organizations, is challenging and why a family of goal models to address this issue is needed. This example is inspired from realistic aerodrome security regulations, with a focus on perimeter signage and access control.

7.1.1 Example of Regulation - Perimeter Security

Due to the sensitive nature of security regulations, a simplified and obfuscated example (illustrated in Figure 95) is used instead of a real one. Its structure however is illustrative and representative of the kind of issues faced while modeling real regulations.

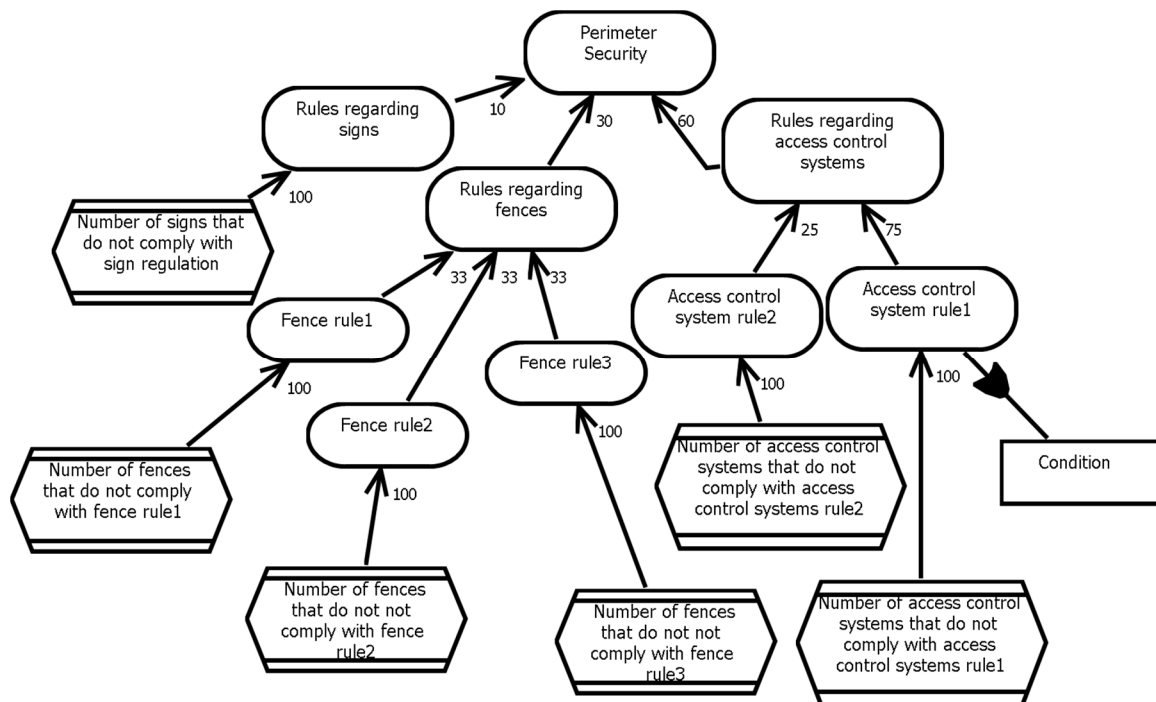


Figure 95, Goal Model of a Perimeter Security Regulation

GRL goals, KPIs, and contribution links are used to model regulations as explained in 4.2. In addition, *Dependency links* ($\neg$ —) are used in the example to show that an intentional element depends on another one to satisfy a goal. GRL *resources* ($\square$) are used to capture conditions that goals depend on (e.g., in Figure 95, Access control system rule 1 depends on Condition).

As an example of condition, one of the rules publicly available regarding plans for construction [25] is: “The operator of an aerodrome must notify the Minister of all plans to begin new construction to the physical security of the aerodrome if the construction relates to regulatory requirements respecting aircraft, passengers, baggage, cargo or mail”. The model in Figure 96 breaks down this rule and extracts out the condition. Therefore, when construction is not related to the items specified by the rule condition, the rule is ignored in the model and not used during the compliance evaluation.

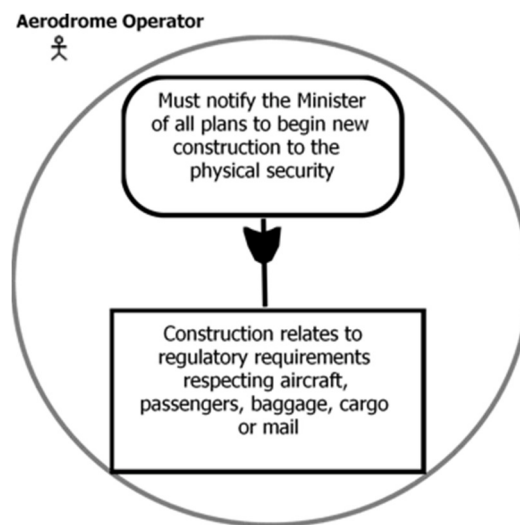


Figure 96, Sample of Condition on a Rule

7.1.2 Requirement for Families of Goal Models

Aerodromes are normally divided into various categories (or types). These types will be referred to as TYPE1, TYPE2, and TYPE3 aerodromes. Some elements of the regulation are only applicable to specific types. Table 41 shows the mapping between rules and aerodrome types for Figure 95.

A regulator requires a generic model for each regulation rather than having separate models based on the aerodrome type. The generic model gives a holistic view of the

regulation as opposed to a specific model for each type of aerodrome. For instance, out of 15 model elements related to fences, only 3 are specific to TYPE1 aerodromes. Therefore, if a model is created for TYPE1 aerodromes, the model will not show the complete picture of the regulation. Furthermore, having separate models for each type increases maintenance costs and the risk of errors in the models as different versions evolve. Therefore, a technique is required to create a *family* of goal models from a generic model, here based on aerodrome types, allowing some of the rules to be ignored in the generic model when a specific type of aerodrome is being evaluated.

Rules	Aerodrome Types
Fence rule1	TYPE3
Fence rule2	TYPE2
Fence rule3	TYPE1
Sign	ALL
Access Control system rule1	TYPE1, TYPE2
Access Control system rule2	ALL

Table 41, Mapping between Aerodrome Categories and Regulations

7.2. First Attempt: Modeling Families with Standard GRL

7.2.1 Modeling Goal Model Families with Dependency Links

To meet the requirement for goal model families, the existing GRL capabilities were used, including dependency links. In GRL, when an intentional element in a depender actor has a dependency link to another intentional element in a dependee actor, the satisfaction value of the depender element cannot be higher than the satisfaction value of the dependee element. First, it was attempted to model the aerodrome categories as GRL *resource* elements with *dependency links* to the rules. Some regulations can apply to more than one type. In order to have an OR condition among various categories, *condition* resource elements with dependency links can be used (as discussed in 7.1.1). In Figure 97, Access control system rule1 is restricted to aerodromes of types TYPE1 or TYPE2. These two types are combined by OR-decomposing Condition1.

In addition, some rules are applicable only under certain conditions (independent of the type, and more dynamic by nature). If the conditions are true, then the rule should

be imposed. As illustrated in Figure 97, such a condition also applies to Access control system rule1 for aerodromes of type TYPE1. Yet again, an intermediate node (Condition2) is needed to handle the Condition, this time with an AND-decomposition.

After modeling the regulation, GRL strategies are defined, each representing a global situation that indicates the rules that apply to each of the categories mentioned in Table 26. Depending on the strategy, either 0 (not selected) or 100 (selected) is used as an initial satisfaction value for the type categories. Figure 97 illustrates the results of a strategy where the value of the TYPE1 resource element is set to 100 and the other resource elements (TYPE2 and TYPE3) values are set to 0. Therefore, all the intentional elements that are dependent on TYPE2 or TYPE3 will be evaluated to a maximum value of 0 and will not affect the evaluation of the model. Hence, Fence rule1 and Fence rule2 are evaluated to 0, whatever the values of their corresponding KPIs, since they are not applied to TYPE1 aerodromes. In addition, Access control system rule1 is used in TYPE1 or TYPE2 aerodromes. Since TYPE1 has a satisfaction level of 100, and since the strategy explored here has the value of Condition set to 100 the satisfaction levels of Condition2 becomes 100, so Condition2 also becomes 100, and hence Condition1 is also evaluated to 100, which means that Access control system rule1 will not be ignored. The rules that are not dependent on any type represent *all* categories and are not ignored in any of the strategies.

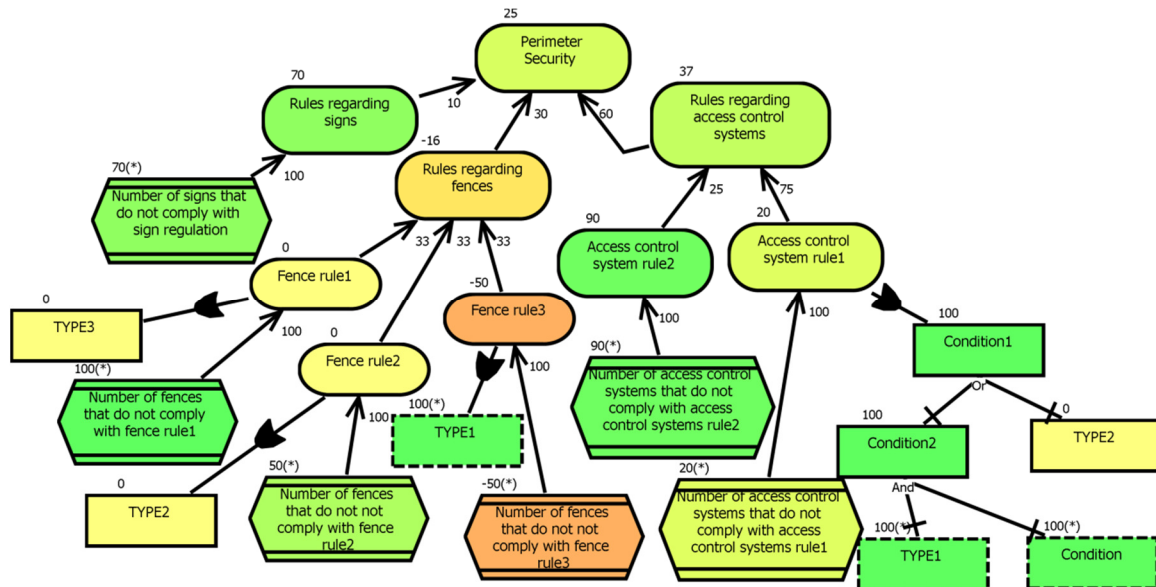


Figure 97, Generic Model from Scenario TYPE1 (Artificial Example)

Using the above method, creating a family of goal models from a generic goal model is possible but not optimal. Although this tentative approach based on standard GRL is addressing the specified requirements to some extent for simple examples, it is not a good solution for more complex real-life examples. In the next section, the problems of the approach are elaborated, with a justification of why a new GRL profile is required to address them.

7.2.2 Problem Definition

There are four main problems related to the approach described in the previous section: 1) noise in the models, 2) scalability and maintenance, 3) ambiguity between the two types of conditions, and 4) evaluation and analysis.

First, an additional model element with a dependency link is connected to each rule to specify the category of the rules. In cases where a rule is valid for more than one type, more intentional elements, dependency links as well as condition nodes are required. For instance, in the simple case where one rule is applicable to two types of aerodromes, three additional intentional elements are needed to show this condition. As illustrated in Figure 97, Access control system rule1 is applicable to TYPE1 and TYPE2. When the number of rules increases, there is much additional *noise* that is not really core to the model but only used to define the conditions and categories. This problem can be somewhat mitigated by moving the conditions and categories to separate diagrams of a same model. For instance, one additional diagram per type can be defined to show the relationship of the category with the rules. Therefore, although the model still includes the additional elements and links, the diagrams used by the end user for evaluation and analysis purposes are much cleaner and manageable.

Since some of the rules can apply to more than one aerodrome type, the rules will be repeated in multiple diagrams that capture the categories dependencies. Therefore, these diagrams again can become very large. In addition, creating a separate diagram and repeating the same elements with same links can be a tedious job and will increase the maintenance complexity.

Furthermore, there are often conditions other than about categories (as illustrated in Figure 96 and Figure 97) that need to be considered more dynamically when the applicability of the rules is being assessed. If resources and dependencies are used for showing yet another type of conditions, the models with two types of condition nodes become ambiguous and too complex to be used by targeted users of this method (i.e., compliance officers).

Finally, the evaluation of these models using the existing GRL evaluation algorithms can be misleading. For example, if the contribution levels of the eliminated rules and applied rules are kept the same as in the generic model, even with a satisfaction value of 100 for an applicable rule, the target intentional element will have a satisfaction value lower than 100, which in this application can be interpreted as non-compliance. This is due to the fact that the existing evaluation algorithms consider all the nodes and contribution links connected to a target intentional element while calculating its satisfaction level. Hence, there is an implicit requirement to redistribute the weight of removed contributions onto the weight of the contributions that remain.

7.3. Solution: Measured Compliance Profile for GRL

The URN standard, which includes GRL, offers lightweight mechanisms to extend the language. A GRL profile takes advantage of two important extensibility concepts:

- *Metadata*, which are name-value pairs used to annotate any model element (e.g., for stereotyping); and
- *URN links*, used to define typed links between any pair of model elements, even across GRL and UCM elements.

In addition, analysis and goal evaluation *algorithms* can also take advantage of profile information. *Constraints*, expressed in OCL, can also be used to enforce additional well-formedness rules for GRL models with metadata. For example, a URN profile for *i** modeling is described in [5]. In this section, stereotypes (metadata), OCL well-formedness rules and a propagation algorithm defined for GRL model families are intro-

duced, with a particular focus on compliance. The profile is called *measured compliance* profile.

The profile is called lightweight because it uses simple extensibility mechanisms and it does not require the extension of the URN metamodel (see Appendix D) or the use of heavyweight profiling mechanisms like UML. It instead uses the metadata (see Figure 115) associated to the GRL model elements to add the information required to the model elements for handling the aspect of the profile that are not supported by the standard GRL.

7.3.1 Specifying Goal Model Families with New GRL-Based Concepts

In order to solve the noise, maintenance and ambiguity issues of the models discussed in section 7.2.2, a new profile was created to manage goal model families within GRL, in a compliance context. Figure 98 introduces the concepts that used for capturing families with GRL. In essence, a *family* (a GRL model) is composed of *model elements* (GRL intentional elements are focused here, but obviously actors and links are included as well). Some of these elements can be *tagged* with metadata describing categories. These tagged model elements are part of *family members*, where a member is a subset of the family regrouping the elements for a given category. A model element can be tagged with multiple categories and hence can be part of many family members.

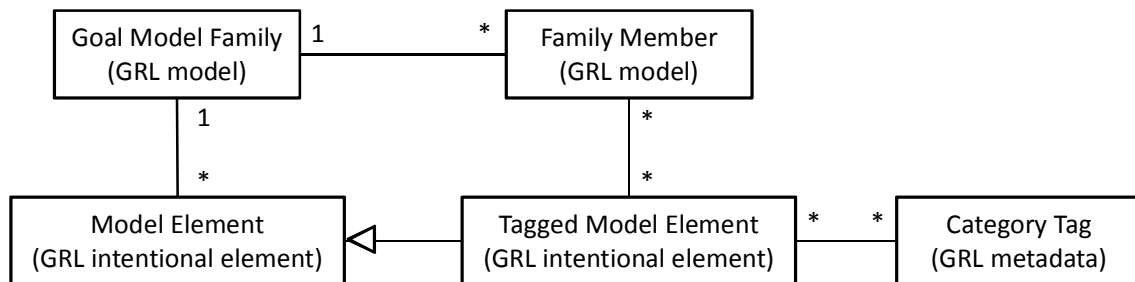


Figure 98, Conceptual Model for the GRL Profile for Goal Model Families

In the given aerodrome context, intentional elements are tagged with metadata (where the name is “ST_CLASSTYPE” and the value is “TYPE1”, “TYPE2”, or “TYPE3”) dis-

played by jUCMNav as stereotypes. An intentional element without a tag means the related rule applies to all aerodrome types. Using this approach, all the elements and dependency links used to define the categories are eliminated, which reduces the noise and ambiguities while improving the maintainability of the model.

Resources and dependency links are still used to model conditions that apply to an intentional element. The conditions are also tagged (metadata with name “ST_CONDITIONTYPE” and a user-defined enumeration value like “TYPE1”, “TYPE2”, or “TYPE3”) to specify which aerodrome categories the conditions apply to.

Furthermore, the GRL strategies are also tagged (metadata with name “acceptStereotype” and a user-defined value like “TYPE1”, “TYPE2”, or “TYPE3”) themselves to specify the model elements that will be evaluated by the strategies. For instance, when users run a strategy that is stereotyped as TYPE1 and TYPE2, all the elements tagged with TYPE1 or TYPE2 (or both) will be evaluated and tagged elements without those tags will be ignored. The described evaluation method only works with the new proposed algorithm described in the next section. In addition, well-formedness constraints in UML’s Object Constraint Language (OCL) can be defined and checked against the model by jUCMNav.

7.3.2 New Analysis Algorithm: Overview

There are three main GRL evaluation algorithms (quantitative, qualitative, and hybrid) that are supported by the URN standard and by jUCMNav [6]. More recently, a formula-based quantitative algorithm that supports KPI aggregation has been proposed and implemented [108]. Whereas such algorithms are sufficient to handle the examples found in the previous two chapters, they cannot handle conditions and goal model families. The standard quantitative algorithm (with support for KPIs) is hence extended to take the measure compliance profile’s stereotypes on strategies and intentional elements into consideration during the evaluation process, in order to be able to eliminate the intentional elements that are not of a specific type (i.e., not part of the desired family member), and to distribute the weights of the contribution links of the ignored intentional elements among accepted intentional elements. For instance, assume that goal G gets contributions

from X, Y, Z and W with values 45, 30, 10, and 15 respectively. The conventional qualitative algorithm multiplies the intentional elements' satisfaction values by their contribution weights, sums them up, and then divides the total by 100 to calculate the satisfaction level of the target intentional element. Figure 99 illustrates this example of three contributions. The satisfaction value of goal G is computed from the four other goals through their contribution links:

$$((45*45) + (70*30) + (50*15) + (100*10))/100 = \mathbf{58}$$

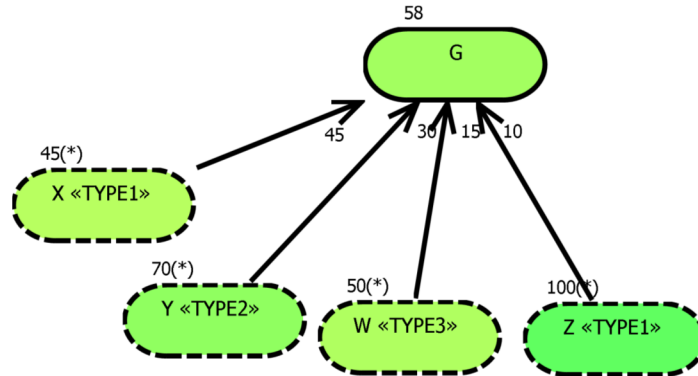


Figure 99, Example of Conventional GRL Quantitative Analysis

Now, assume this is a model family where X is tagged with «TYPE1», Y with «TYPE2», W with «TYPE3», and Z with «TYPE1». If a strategy that restricts the family to members of type TYPE1 is chosen, then the issue with the conventional algorithm is that the contributions to G sum up to 55, and hence G's satisfaction value cannot be higher than 55.

With the modified algorithm however, if the strategy is tagged with «TYPE1», then Y and W will be tagged dynamically (and only for the duration of the analysis of this strategy) with an “IgnoreNodeInEvaluation” stereotype. The contribution level of ignored elements will be divided proportionally between the contribution levels of remaining active intentional elements. It is assumed that the sum of contribution levels will not exceed 100; this particular style is checked through one of the framework's OCL rules (see Rule 1 in Appendix C). In this example, the total contribution value of Y and W computed at runtime, which is (30+15), will be divided proportionally between X and Z as follows (also illustrated in Figure 100):

$\text{IgnoredContributionLevel} = 30 + 15 = 45$ // Not TYPE1: Y + W
 $\text{SumConsideredContributionLinks} = 45 + 10 = 55$ // TYPE1: X + Z
 $\text{ContributionLevelX} = \text{ContributionLevelX} + (\text{ContributionLevelX} * \text{IgnoredContributionLevel} / \text{SumConsideredContributionLinks})$
 $= 45 + (45 * 45) / 55 = 81$
 $\text{ContributionLevelZ} = \text{ContributionLevelZ} + (\text{ContributionLevelZ} * \text{IgnoredContributionLevel} / \text{SumConsideredContributionLinks})$
 $= 10 + (10 * 45) / 55 = 18$

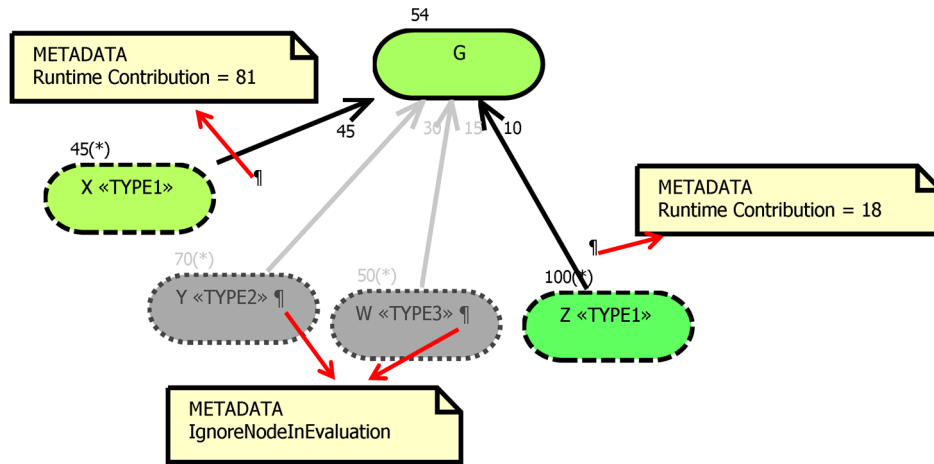


Figure 100, Example of Modified GRL Analysis Algorithm

Note: the ¶ symbol in jUCMNav shows that a model element is tagged with metadata.

jUCMNav now supports this analysis algorithm and will also grey out intentional elements (and their links) that are not part of the selected family member, as shown in Figure 100. This graying out feature allows the analyst to see the complete regulation while focusing on those elements that only concern the context specified in a given strategy.

In the aerodrome family example, Figure 101 illustrates a strategy-based analysis of perimeter security using the modified GRL algorithm. The strategy used for evaluating the model in this example has been tagged with a TYPE1 metadata, therefore only intentional elements and conditions tagged with a TYPE1 stereotype will be considered during the evaluation. As illustrated in this figure, Fence rule1 and Fence rule2 are applicable to TYPE3 and TYPE2 aerodromes, respectively. When the scenario is run, all these intentional elements are tagged with “IgnoreNodeInEvaluation”. The contribution values from

Fence rule1 and Fence rule2 are added to the contribution from Fence rule3, which become 99 at runtime (and the sole contributor to Rules regarding fences).

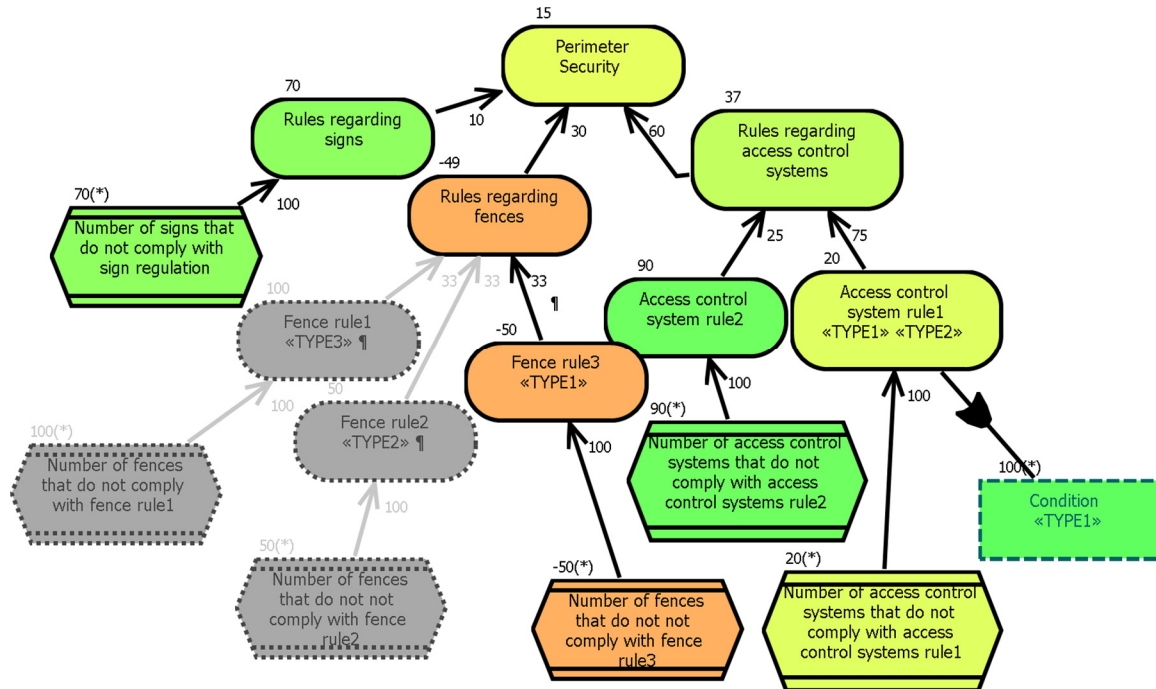


Figure 101, Example of TYPE1 Aerodrome with the Modified GRL Analysis Algorithm

This set of features is really important as it essentially enables the analyst to think of contributions more in terms of relative weights rather than absolute weights. Overall, the measure compliance profile, its adapted propagation algorithm, and the new jUCMNav visualization features help reduce noise in the models (through minimal usage of conditions and stereotypes), handle scalability and maintenance (with proper visualization and a reduced number of symbols for handling multiple models in one family model), resolve the ambiguity between the two types of conditions discussed earlier, and solved evaluation and analysis issues related to the redistribution of contribution weights.

7.3.3 Measured Compliance Profile: Summary of Stereotypes

Table 42 gives a complete summary of the stereotypes (URN metadata) related to IPCF' measured compliance profile, which was highlighted in the previous sections. This table can be used as a reference by modelers when using IPCF.

Three of the stereotypes (i.e., ST_CLASSTYPE, ST_CONDITIONTYPE, and acceptStereotype) are used to deal with RegulatedTypes (see Figure 17) and goal model families. Their values are defined by the modeler and correspond to the types of organizations targeted by the model (e.g., TYPE1, TYPE2, TYPE3, etc.). ST_NO can be used for optimization and for dropping a model element from the analysis when it is not measurable. These four stereotypes are inserted manually in the goal model.

Furthermore, ignoreNodeInEvaluation (where the value is ignored) and Runtime Contribution are two kinds of metadata that are added to the model dynamically by the algorithm during the evaluation process. While the former specifies the elements that are dropped from the evaluation due to unsatisfied conditions or unapplicable goals (this information is used to grey-out portions of the diagram), the latter is used to show the dynamically calculated contribution values to the analyst (see Figure 100).

ST_Term can be used by modelers to specify the SectionName attribute of the legal document's term. The value is a user-defined string that corresponds to one of the many type of sections that reflects the structure of a regulation document, as discussed in section 4.2.1. For instance, ST_Term = "Part" can be used to indicate that this term is a "Part" in the source document. Finally, RegDocRef is used to contain a reference to the source regulation document where the term is defined. The information found in ST_Term and in RegDocRef is for traceability and understanding only, and is not taken into consideration by the analysis algorithm formalized in the next section.

Stereotype Name	Stereotype Value	GRL Element
ST_CLASSTYPE	User enumeration	Goal
ST_CONDITIONTYPE	User enumeration	Resource
acceptStereotype	User enumeration	Strategy
ST_NO	"No"	Goal
IgnoreNodeInEvaluation	N/A (<i>ignored</i>)	Goal, Resource
Runtime Contribution	Computed contribution value	Contribution Link
ST_Term	User enumeration	Goal
RegDocRef	Reference to source document	Goal

Table 42, Measured Compliance Profile Metadata/Stereotypes

7.3.4 New Analysis Algorithm: Formal Definition

The new algorithm that handles conditions and families for IPCF is an extended version of the evaluation algorithm described in Appendix II of the URN standard [57]. The extensions are mainly done in a set of sub-algorithms called from the main algorithm as well as by some modifications in the dependency and contribution calculation algorithms. The following algorithms make use of the data structures corresponding to the URN metamodel (Appendix D) and of the stereotypes summarized in the previous section.

During the initialization phase of the evaluation process (before the propagation of satisfaction values), the list of stereotypes defined in the currently selected strategy is first extracted. As shown in the GetStrategyStereotypes algorithm (Figure 102), this is done by iterating through the list of current strategy metadata. The value of any metadata named “acceptStereotype” (and there could be many for a strategy) is added to the list and is returned by the algorithm.

Algorithm GetStrategyStereotypes Inputs currentStrategy:EvaluationStrategy Output acceptStereotypes:List
<pre>acceptStereotypes:List = $\emptyset$ // list of stereotypes strategyMetadataList:List = currentStrategy.getMetadata() for each metadata:Metadata in strategyMetadataList { if (metadata.name == “acceptStereotype”) { acceptStereotypes.add(metadata.value) } } return acceptStereotypes</pre>

Figure 102, GetStrategyStereotypes Algorithm

An important sub-algorithm that is used in this extension is CheckIgnoredElement (Figure 103), where the list of stereotypes from the selected strategy (i.e., acceptStereotypes) as well as the intentional element being evaluated are passed as inputs. This algo-

rithm iterates through the element’s metadata. If a metadata called “IgnoreNodeInEvaluation” exists, the algorithm stops going through the rest of the element’s metadata and returns true. Furthermore, if none of the element’s stereotypes matches the strategy’s stereotypes, the algorithm returns true. If no stereotype is detected or if a stereotype that matches one of the stereotypes in the current running strategy’s acceptStereotypes list is found, then the algorithm returns false, which means the element remains in the model and is evaluated.

Algorithm CheckIgnoredElement Inputs element:IntentionalElement, acceptStereotypes:List Output ignoreSrc:boolean <pre> foundStereotype:Integer = 0 foundAcceptStereotype:Boolean = false for each elementMetadata:Metadata in element.metadata { if (elementMetadata.name == “IgnoreNodeInEvaluation”) { ignoreSrc = true break } if (acceptStereotypes.size > 0 and not(foundAcceptStereotype)) { // check the presence of appropriate ST_CLASSTYPE, ST_CONDITIONTYPE, // and ST_NO if (elementMetadata.name.startsWith(“ST_”) and not(acceptStereotypes.containsKey(elementMetadata.value)) foundStereotype = foundStereotype + 1 else if (elementMetadata.name.startsWith(“ST_”) and acceptStereotypes.containsKey(elementMetadata.value)) { foundStereotype = foundStereotype + 1 foundAcceptStereotype = true } } } // if there is no stereotype, the element will not be ignored foundAcceptStereotype = (foundAcceptStereotype or (foundStereotype == 0)) ignoreSrc = ignoreSrc or not(foundAcceptStereotype) return (ignoreSrc) </pre>
--

Figure 103, CheckIgnoredElement Algorithm

Once we have invoked GetStrategyStereotypes, the top-level evaluation algorithm (CalculateEvaluation, see Figure 104) to be used on each intentional element of the GRL model is very similar to the URN standard's algorithm. However, there is an additional step used to check the conditions (captured as GRL resources) connected to the element being evaluated through dependency links.

Algorithm CalculateEvaluation Inputs element:GRLContainableElement, currentStrategy:EvaluationStrategy, acceptStereotypes:List Output satisfactionValue:EvaluationValue
<pre> decompValue:EvaluationValue // intermediate result contribValue:EvaluationValue // intermediate result if not(element in currentStrategy.evaluations.intElement) // is the element not initialized? { <u>CheckConditions(element, acceptStereotypes) // new!</u> // calculate based on decompositions, contributions, and dependencies decompValue = CalculateDecompositions(element) // unchanged contribValue = CalculateContributions(element, decompValue, <u>acceptStereotypes</u>) satisfactionValue = CalculateDependencies(element, contribValue) // unchanged } return satisfactionValue </pre>

Figure 104, CalculateEvaluation Algorithm

Figure 105 describes the new CheckConditions algorithm. This algorithm iterates through the dependency links of the element, if any. If it finds a dependency link connected to a resource, it first checks whether the condition is valid for the current strategy (i.e., whether it has the right stereotype) using the CheckIgnoredElement algorithm discussed earlier (see Figure 103). The algorithm also calculates the evaluation value of the valid conditions and if a condition is not satisfied, it disables the dependent element by adding an IgnoreNodeInEvaluation tag to that element. Consequently, the element is no longer considered in the rest of the evaluation procedure.

Algorithm CheckConditions**Inputs** element: GRLmodelElement, acceptStereotypes:List

```
for each link:Dependency in element.linksDest
{
  srcElement:GRLmodelElement = link.getSrc()
  if (srcElement.typeName = "Ressource")
  {
    if (CheckIgnoredElement(srcElement, acceptStereotypes))
    {
      // add an ignore tag to the condition to avoid considering it in the evaluation process
      addIgnoreNodeInEvaluation (srcElement)
    }
    else
    {
      evaluationvalue:int = srcElement.calculateEvaluation()
      if (evaluationvalue == 0)
      {
        // if condition is not satisfied, eliminate the dependent element from the evaluation
        addIgnoreNodeInEvaluation (element)
      }
    }
  }
}
```

Figure 105, CheckConditions Algorithm

As explained in the comments of Figure 104, the handling of decomposition and dependency links is not different from the URN standard's algorithms. However, contribution links need to be handled in a different way. In fact, the calculation of the contribution values based on the active and disabled contribution links is the most complex part of the algorithm. The main challenge in this case is to find the contribution links from the sources that need to be ignored. Therefore, the enhanced CalculateContribution algorithm (Figure 106) first iterates through all the contribution links and passes them to the CheckIgnoredElement algorithm discussed in Figure 103. Once the algorithm has the list of ignored links and considered links, it uses the considered links to calculate the contribution. However, it also adjusts their contribution level by distributing the sum of contribution of all ignored links between them according to their weight. The rest of the algorithm is similar to the algorithm described in the URN standard [57].

Algorithm CalculateContribution**Inputs** element:IntentionalElement, contribValue:Integer, acceptStereotypes:List**Output** contribValue:Integer

```

ignoredArrayIt :Integer = 0           // counter for ignored links
consideredArrayIt:Integer = 0         // counter for considered links
totalIgnoredContributionValue:Integer = 0 // the total of all ignored contributions
contributionLinksValue:Array          // stores the considered links contribution
evaluationValues:Array                // stores the considered links source evaluation value

tolerance:Integer                     // predefined tolerance, between 0 and 49
oneCont:Integer                       // one weighted contribution
totalCont:Integer = 0                 // weighted sum of the contribution links
hasSatisfy:Boolean                   // a weighted contribution of 100 is present
hasDeny:Boolean                      // a weighted contribution of -100 is present

hasSatisfy = (decompValue == 100)
hasDeny = (decompValue == -100)

// iterate through the contribution links to find the ignored and considered links
for each link:Contribution in element.linksDest
{
    // find the ignored elements
    if (CheckIgnoredElement (link.getSrc()), acceptStereotypes)
    {
        // add ignore tag to the source element
        addIgnoreNodeInEvaluation (link.getSrc())
        // store all the ignored contribution links to distribute among other links
        totalIgnoredContributionValue += link.quantitativeContribution
        ignoredArrayIt++
    }
    else
    {
        // store each (and the total of the) considered links contribution level
        // and each evaluation value
        contributionLinksValue[consideredArrayIt] = link.quantitativeContribution
        sumConsideredContributionLinks += link.quantitativeContribution
        evaluationValues[consideredArrayIt] = link.src.quantitativeVal
        consideredArrayIt++
    }
}

```

```

// go through all considered links and calculate the contribValue
for j:Integer = 1 to consideredContribArrayIt .size
{
    // increase the contribution level of the considered links using the
    // totalIgnoredContributionvalue if any link has been ignored
    if (totalIgnoredContributionValue > 0 )
    {
        contributionLinksValues[j] += (totalIgnoredContributionValue *
            contributionLinksValues[j] / sumConsideredContributionLinks)

        // adjust the values if they go above or below the range
        if (contributionLinksValues[j] > 100) {
            contributionLinksValues[j] = 100
        } else if (contributionLinksValues[j] < -100) {
            contributionLinksValues[j] = -100
        }
    }
    addMetadataToLink("Runtime Contribution", contributionLinksValues[j])

    oneCont = (contributionLinksValues[j] * evaluationValues[j])
    totalCont = totalCont + oneCont
    if (oneCont == 100) hasSatisfy = true
    if (oneCont == -100) hasDeny = true
}

// What is below comes from the URN standard
totalCont = totalCont / 100
contribValue = totalCont + decompValue

// contribution value cannot be outside [-100..100]
if (|contribValue| > 100)
    contribValue = 100 × (contribValue/|contribValue|)

// take tolerance into account if a weighted contribution of 100 or -100 is not present
if ((contribValue ≥ 100 – tolerance) and not(hasSatisfy))
    if (totalCont > 0) // positive contribution
        contribValue = max (decompValue, 100 – tolerance) // case A
        // else there is nothing to do, contribValue remains unchanged.
else if ((contribValue ≤ -100 + tolerance) and not(hasDeny))
    if (totalCont < 0) // negative contribution
        contribValue = min (decompValue, -100 + tolerance) // case B
        // else there is nothing to do, contribValue remains unchanged.

return contribValue

```

Figure 106, CalculateContribution Algorithm

It is important to note that the overall complexity of this new algorithm is comparable to the one from the URN standard, i.e., the complexity is directly proportional to the number of intentional elements found in the GRL model under analysis (as `CalculateEvaluation` is invoked on each of them) multiplied by the average number of links per intentional element. The impact of executing `GetStrategyStereotypes` and `CheckConditions` in that context is negligible.

7.3.5 Measured Compliance Profile: OCL Well-Formedness Rules

To ensure the quality of input models before analysts start their analysis, well-formedness rules must be defined and checked. A set of ten well-formedness rules, written in OCL and supported by jUCMNav [62], is presented in Appendix C. These rules are part of the profile for measured compliance. For example, one rule will ensure that a GRL resource with an `ST_CONDITIONTYPE` metadata must be a dependee of an intentional element. These rules take advantage of an OCL library of over 120 pre-defined functions used to query and check URN models, hence simplifying the definition of profile rules.

Violations to any rules are reported in jUCMNav's Problems view as a list of problems. By clicking on a problem in the Problems view, the violating element or diagram of the model is highlighted. Figure 107 shows a small example where seven out of ten rules have been violated. Note that three of these rules report warnings only as these are not severe enough to affect the results of the profile's propagation algorithm.

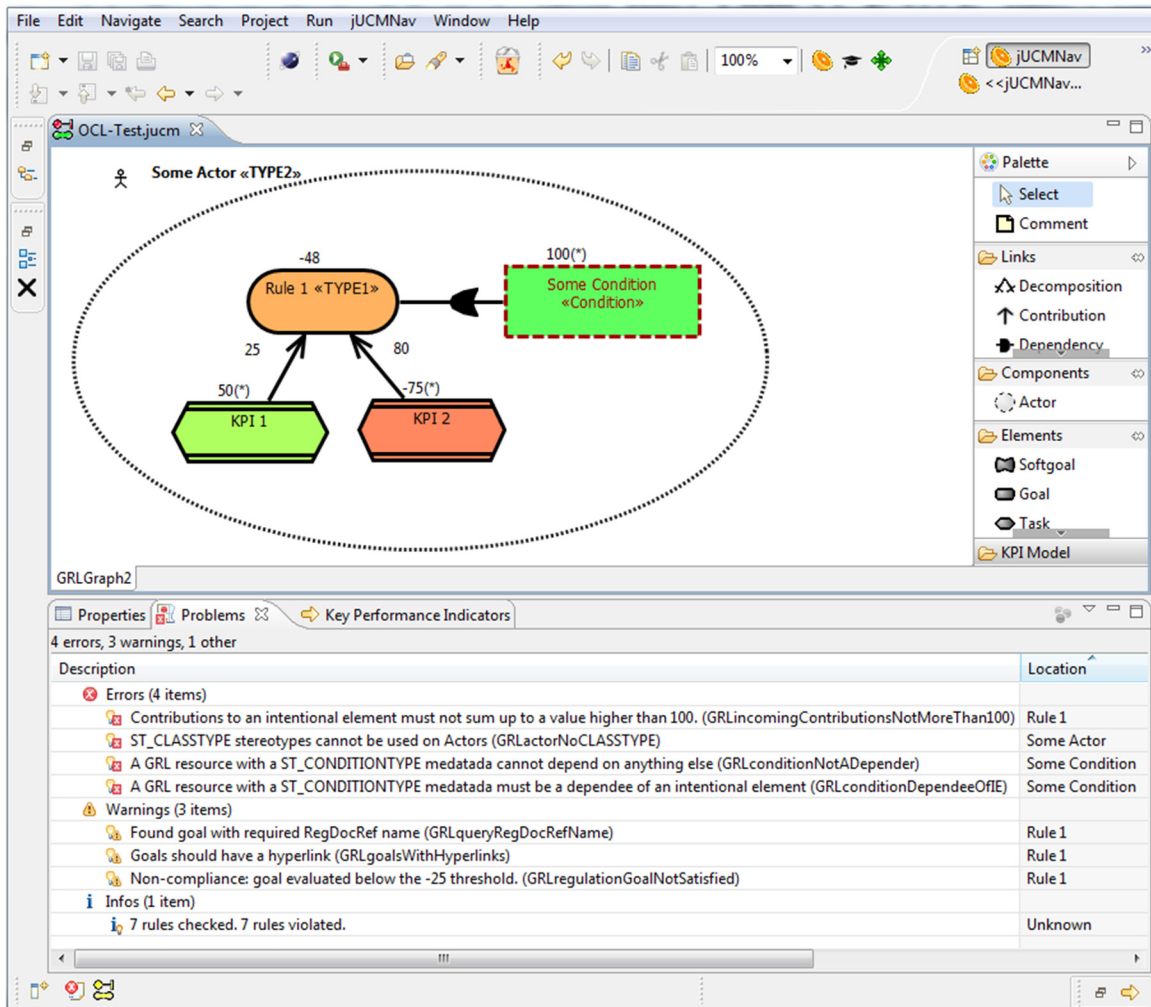


Figure 107, Example of Violations of the Profile's OCL Rules in jUCMNav

7.4. Limitations and Threats to Validity

Although using existing GRL modeling elements and links (i.e., resource, dependency and decomposition) to model conditions addressed the basic needs identified in section 7.1.2, this approach can be confusing for current users of GRL models in other application domains. Therefore, a better approach might require defining new model elements for conditions. For now, IPCF tries to mitigate this problem to some extent by using a different symbol color in the GRL profile for measured compliance in a way that is compatible with the URN standard. Adding a new type of condition element to the URN standard is technically simple but requires time, effort, and international support, howev-

er. The runtime contribution information is currently only as metadata in the tool implementation (requiring mouse hovering to be visible), and this might also be confusing to the user.

In addition, this profile does not solve the issue of how to choose appropriate contribution levels in goal models. However, this is mitigated by the recent availability of features in jUCMNav such as *contribution overrides* (with which one can store alternative weights for contributions and use them in combination with GRL strategies during analysis) and *sensitivity analysis* (through which intervals rather than simple values can be attached to contributions and initial satisfaction levels, and then used with jUCMNav's analysis algorithms) [8].

This profile has been used on real sets of policies and rules for aviation security, with models containing hundreds of intentional elements. No scalability issue has been observed at the moment, but there is no guarantee this approach will fit other policies, or other domains outside compliance, and validation experiments will be needed to address these issues. The concept of model families could be adapted to other goal-modeling languages, but in general other languages do not provide all the facilities provided for free by the URN language (e.g., strategies, and extension mechanisms) and by the jUCMNav tool, hence porting these ideas might prove to be difficult.

7.5. Summary

In this chapter, based on the challenges observed through the modeling of aerodrome security regulations with GRL, the concept of families of goal models was defined. This led to the creation of a GRL profile for measured compliance, comprised of a set of stereotypes and OCL well-formedness rules exploited by a novel propagation algorithm, with support for modeling, analysis, and visualization provided by the jUCMNav tool.

Although regulators (such as Transport Canada) define regulations (e.g., aviation security) that apply to all the organizations they regulate (e.g., aerodromes and airlines), not all rules are usually applicable to all types of organization. This is a common situation that is not limited to aviation security. A perimeter security example was used to illustrate that when regulations apply to various types of organization, modeling them using exist-

ing goal-modeling approaches can lead to various issues including model noise, scalability and maintenance problems, ambiguity with how conditions are represented, and misleading evaluation and analysis results. After illustrating the problems, the requirements were characterized for potential solutions and one solution was proposed that allows modelers to define a generic family goal model for all types of organizations and tag the model elements to specify which ones are applicable to which family member. The solution is formalized as a profile for GRL, with suitable stereotypes, well-formedness constraints, and a modified analysis algorithm that exploits this new information. This solution is illustrated through examples and compared to related work. Several limitations and items for future work have also been identified.

The approach proposed in this thesis shares similarities with the work of Lapouchnian and Mylopoulos [73][74], as elements are also tagged with appropriate context information. However, prior to this thesis, GRL, which was selected as the goal modeling language for IPCF, did not support the concept of Goal Model Families. Furthermore, in this thesis' approach, this concept is taken further and used for quantitative evaluation of the goal models (and not just Boolean evaluation) while automatically adjusting the contribution links to produce valid results. In addition, the tags are visualized with stereotypes, conditions with special intentional elements, and non-member elements with gray shading.

Families of goal models fit nicely as a solution to the problems observed in regulatory compliance, but they can potentially address a much larger class of problem domains.

The next section will provide a more complete and formal evaluation of the Indicator-based Policy Compliance Framework proposed in this thesis.

Chapter 8. Evaluation

This chapter presents the evaluation of the Indicator-based Policy Compliance Framework (IPCF). This evaluation is divided into four parts. First, it provides a gap analysis based on the results of systematic review discussed in Chapter 3. Second, it assesses IPCF based on the eight dimensions proposed by Kharbili *et al.* [66] (and introduced in section 3.4.1) to assess Compliance Management Systems (CMS). Third, Cabanillas *et al.* [22] describe all the features that a Business Process Compliance Management System (BPCMS) should support during the entire business process lifecycle, and hence how well IPCF does against each feature is discussed. Finally, the implementation of the new GRL profile, with suitable stereotypes, well-formedness constraints, and a modified analysis algorithm defined for GRL model families is implemented in the jUCMNav tool.

8.1. Gap Analysis Based on the Systematic Review

This section includes a comparison between this framework and existing frameworks discussed in Chapter 3, where two research questions are identified:

- What are the methods based on Key Performance Indicators (KPIs) used for measuring the compliance of business processes against policies and laws?
and
- What goal-oriented modeling methods are used for compliance measurement?

Some of the key points that IPCF addresses are:

- Compliance measurement using Key Performance Indicators;
- Guidelines for extracting policy and regulation terms and mapping them to goal models;
- Computation of the importance level of business processes and rules based on the organization's goals;

- Impact assessment of compliance-related process modifications on business goals, including conflicting goals between stakeholders, and on policies;
- Support for goal model families through a GRL profile for compliance measurement;
- Tool support for compliance management, including OCL constraints to improve model accuracy, and an improved propagation algorithm for automated analysis; and
- Use of Business Intelligence software for visualization and reporting;

Although related works address some of these key points, none supports all key points in one cohesive framework.

Table 43 gives a comparison between IPCF and three of the closest related frameworks. The details of these frameworks were discussed in Chapter 3.

Criteria	IPCF	Silveira <i>et al</i>	Rifaut <i>et al</i>	Ghanavati <i>et al</i>
Compliance Measurement using KPI	Yes	Yes	Yes	No
Guidelines for extracting policy and regulation	Yes	No	No	No
Importance level of business processes and rules	Yes	No	No	Yes
Impact of compliance-related process modifications on business goals	Yes	No	No	No
Support for goal model families	Yes	No	No	No
Tool support for compliance management	Yes	Yes	Yes	Yes
Use of Business Intelligence	Yes	Yes	No	No
Use of different deontic modalities (obligations and permissions) in legal models	No	No	No	Yes
Formal framework based on a measurement standard	No	No	Yes	No
Reporting part of the framework supports drill-down and roll-up	No	Yes	No	No

Table 43, Comparison between IPCF and other Related Frameworks

Silveira *et al.* [124] use key compliance indicators to measure the compliance level of processes. They discuss the conceptual model of a dashboard for visualization and reporting on the most critical regulatory and policy indicators, the compliance level of the main processes, as well as an overall compliance level for the organization. Furthermore, Silveira's approach allows drill-down and roll-up using dimensional models, enabling one to see the value of the KPIs for various locations and time periods or any other dimension that is required. Although the current reports and dashboards in the examples discussed in this thesis do not support dimensional analysis of the KPIs, nothing prevents the analysts to design the BI portion of the IPCF framework to enable these capabilities. The main difference between IPCF and this framework is that IPCF has the graphical models of the policies helping the analysts to better understand the policies, trace the relationship between regulation documents and model, compute compliance levels along the structure of the regulation document, track down problem areas, detect conflicts manually, and find their relationship with business processes and goals.

Rifaut and Dubois [113] propose a method to combine and model the regulations and business requirements for processes. They use i^* goal models and indicators to assess and measure process success. However, they do not provide a final value on the compliance level of different regulations. In addition, their framework has no method for prioritizing non-compliance instances. In order to increase the formality of the measurement aspects, their framework is specifically focused on the ISO/IEC 15504 standard [58]. However, some regulations cannot easily be described with this standard. The way that indicators are defined in the IPCF is ad-hoc and based on analysts judgment, however indicators in models could be created based on such formal standards.

Ghanavati *et al.* [39], [40], and [41] have proposed a URN-based requirements framework for compliance management involving business goals (in GRL) and processes (in UCM) linked to policies and legal documents (in GRL). With this framework, they define and analyze different types of traceability and compliance links between organization models and regulation models. Although the modeling notation used in their framework is the same as in IPCF, IPCF not only establishes traceability links between organization and regulation models but also *measures* the level of compliance of business processes against policies/regulations with KPIs, and helps assess how business process

modifications can affect organization goals. Furthermore, IPCF suggests a new method to calculate the relative importance of rules in this context. Furthermore, while Ghanavati's framework allows capturing deontic modalities using stereotypes, IPCF does not identify different types of deontic modalities explicitly from legal documents, but it can support deontic modalities to some extent. Permissions can be captured in a way similar to the approach used to capture conditions in IPCF (see section 4.2.2). Interdiction and obligation at the term level are captured in a descriptive manner when the term is written in the model. Consequently, the modelers need to adjust the model in order to support modalities with IPCF, which is not as straightforward as with Ghanavati's framework. Nevertheless, having to support different types of modalities was not an issue in the regulation and policy documents that were used to evaluate the IPCF framework, and supporting families of goal models is also a technique that can be used to identify and handle terms that are not considered obligations in a given context.

8.2. Assessment Against CMS Criteria

Kharbili *et al.* [66] define eight dimensions (or simply criteria) used to assess compliance management systems (CMS). In this section, these properties are used to evaluate IPCF and identify opportunities for improvement as well as threats to the framework's overall validity.

Transport Canada is a federal department that develops policies and regulations to make the Canadian transportation system safe and secure. IPCF was evaluated within Transport Canada, in the team working towards a performance framework [46], whose main purpose is to help develop performance-based regulations, define measurable and traceable compliance objectives, and define and assess performance expectations. Various regulations were modeled to validate the framework. These regulations are related to aerodromes security and, since they are not public, the details of the models cannot be discussed. However, the lessons learned and the limitations observed in the applicability of the framework are reported.

Change Management: The framework should be able to support regulation evolution and propagate these changes to the whole domain of jurisdiction of compliance

policies. IPCF does not support this property automatically. However, as discussed in section 6.1.3, a DocRef metadata enables modelers to query the model to spot the elements corresponding to a given part of a legal document, on a name basis (see Figure 68). Such a query can be formalized in OCL (see Rule 6 of Appendix C, and the impact of a “violation” shown as a warning in Figure 107). In addition, hyperlinks can be added model elements to establish traceability links to online regulation / policy documents. Since this information should be available in the models, another OCL constraint was created to detect the absence of hyperlinks on goals (Rule 3 of Appendix C). Finally, jUCMNav offers advance searching capabilities for URN models.

Traceability & Accountability: A compliance management framework should have the ability to trace and document who made which action for what reason. IPCF partially supports this property. URN supports the concept of *actor* for both UCM and GRL. When business processes are modeled in UCM, actors who are responsible for performing the business processes are included, and these UCM actors can be linked to GRL actors, hence providing rationales. In addition, as discussed in Figure 83, it is possible to capture the records of process execution and report on them via BI tools. This provides traceability to the actors who executed the process instances and allows the organizations to hold them accountable. However, this part of the framework and its supporting tools are as good as their implementation in the organization. If the reporting part is not fully implemented and if process instance data is not captured, there will be no traceability at the execution level.

In a compliance context, traceability and accountability must also apply to the models themselves. jUCMNav was recently extended to answer the following question: “How can we highlight, understand, and control model evolution?” [8]. The approach currently implemented in jUCMNav reuses the facilities of the *EMF Compare* plugin [35], a generic difference engine for modeling tools based on the Eclipse Modeling Framework (EMF). EMF Compare represents a simple and yet efficient solution to the comparison of URN/GRL models by showing, in a tree-like representation, which model elements were added, deleted, or modified when compared to another version of the model (where versions of a model are stored in some repository).

Complexity: This criterion refers to the representation of regulations in models. In general, a compliance management framework should not focus on a specific domain (e.g., only for transportation security, or for healthcare privacy). IPCF supports this property well. The modeling of several policies and regulations from domains as varied as human resources [118] (see Chapter 5), healthcare [40], and aviation security regulations (see Chapter 6) shows that the framework and the selected modeling language are not limited to a particular domain. In addition, as discussed in Chapter 7, in order to solve the maintenance and ambiguity issues of the models, a new profile was created to manage goal model families within GRL.

Efficiency: This criterion is related to policy and compliance checking algorithms. The question: “Do my policies really constrain my business processes in the way I want them to?” has to be answered. “The framework must offer functionalities and elements to check and enhance efficiency of designed policies as well as checking and enforcement tools” [66]. IPCF partially supports this property through the propagation algorithm of the framework’s measured compliance profile for GRL. An OCL constraint (Rule 7 in Appendix C) is also used to assess compliance to rules and diagnose non-compliance elements (through traceability links).

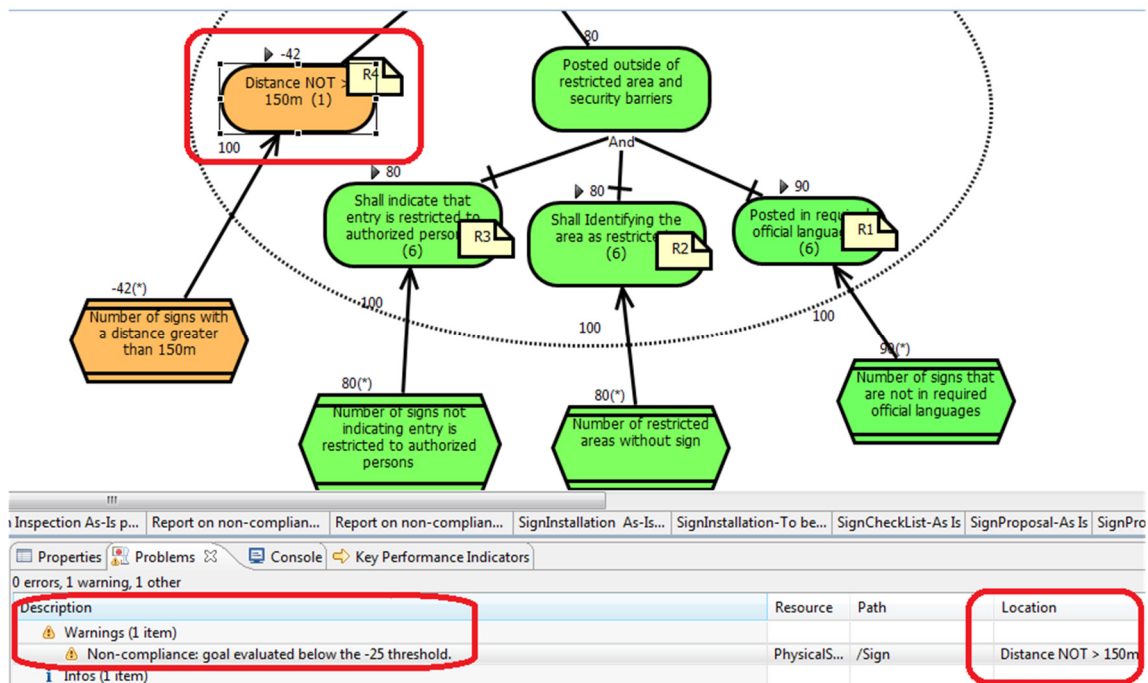


Figure 108, OCL Compliance Rule

This constraint highlights the goals whose satisfaction level is evaluated below a specific threshold (set by default to -25 in the rule), as seen in Figure 108. In addition to what Kharbili *et al.* [66] argue for efficiency of compliance management frameworks, it is also important for such frameworks to be able to identify whether the amount of effort the organization is spending on compliance management is required or not. An organization might be exceeding what is required from a compliance perspective, with a negative impact on costs or other organization objectives. For instance, in the sign distance example that was discussed in Chapter 6, according to Rule4, an aerodrome should have signs installed every 150 meters, at the most. Have signs every 100 meters also makes the organization compliant, but with increased costs for sign creation, installation, and maintenance. IPCF enables organizations to reason about this situation as well, by doing less on the process side when there is some slack on the compliance side.

Note that an organization might also *consciously* choose not to be fully compliant (at least for the moment) if the negative impact of full compliance on the business objectives is too high. Such trade-off analysis, which is most needed across domains, is also possible with IPCF.

Enforcement: A compliance management framework should provide mechanisms to enforce policies on business processes and make sure the latter are compliant. IPCF does not enforce the policies and rules. However, through the measurement approach, the framework will make any non-compliance with the policies visible and ready for consumption to managers and decision makers in general. For instance, an aerodrome operator is far from being compliant with R4 in Figure 109. The UCM processes related to this policy can be modified by defining and adding tasks that are required in the process to enforce compliance. New compliance-induced tasks are highlighted in red in Figure 110 and Figure 111.

Combining compliance measurements with the ability to ensure that required tasks are performed in business processes can help preventing major non-compliance issues.

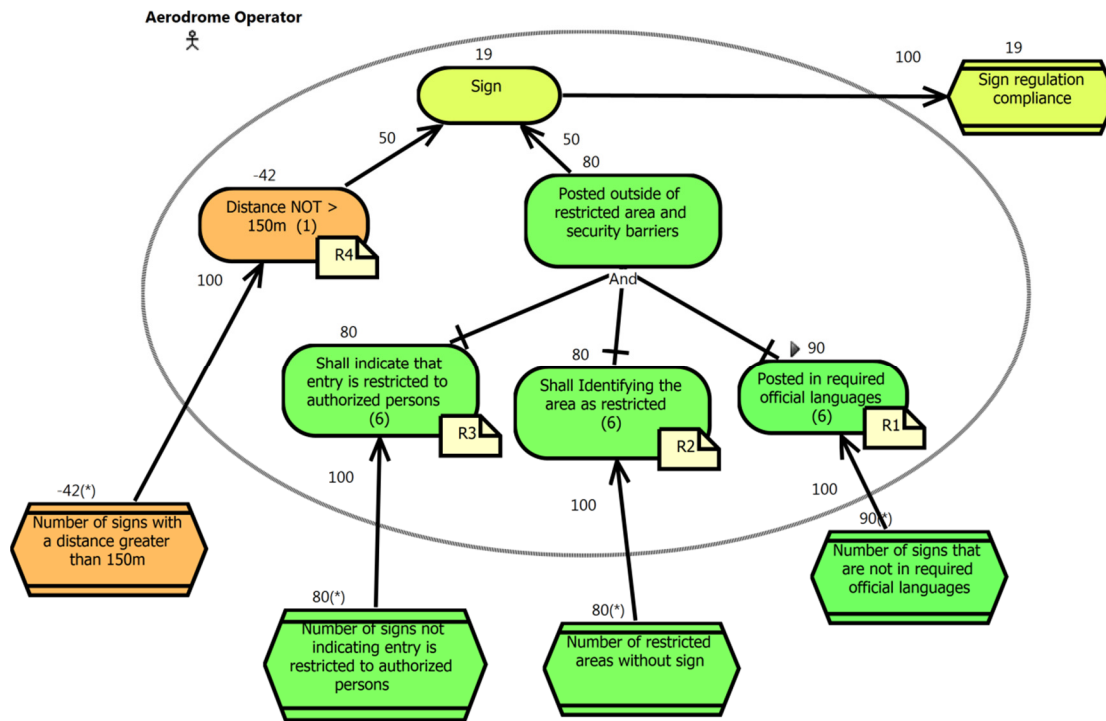


Figure 109, Policy Model

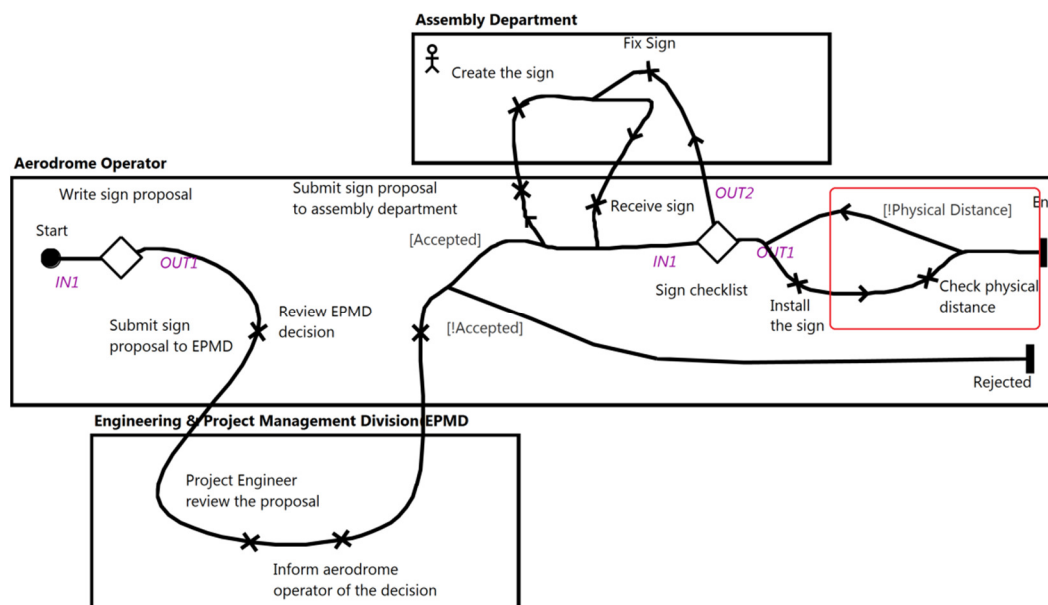


Figure 110, Tasks Required Enforcing Compliance for Sign Installation

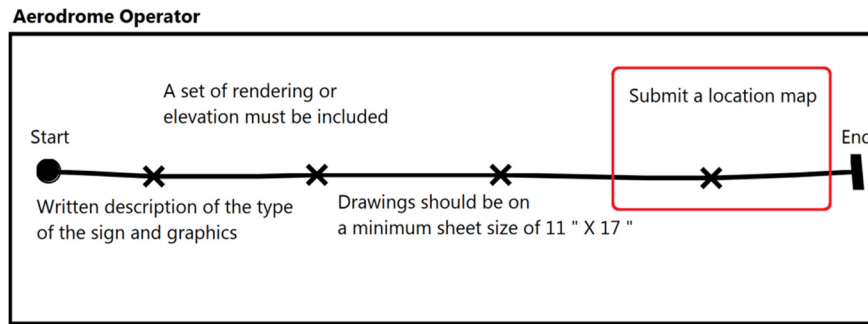


Figure 111, Tasks Required Enforcing Compliance Write Sign Proposal

Scalability: As regulations are often very large, compliance management systems should not suffer from regulation size. IPCF partially supports this property. Various regulations were modeled at Transport Canada. For example, Physical Security (about 50 rules), Security Policies and Procedures (about 120 rules), and Security Screening Operation (about 20 rules) regulations were modeled without any observable problem using IPCF. A few thousand such rules are expected to be modeled in the future. One of the advantages of URN and jUCMNav as supporting tool is that they allow having several views against the same model. This prevents many scalability issues at a display level for the analysts by allowing them to organize their views in an appropriate and digestible fashion. Furthermore, since the evaluation algorithm used by IPCF is a bottom-up analysis and unlike top-down approaches does not require many solutions to be considered, the scalability of the algorithm is not a concern from a theoretical point of view (as explained in section 7.3.4, its complexity is the same as the quantitative evaluation algorithm of the URN standard).

However, it was found that very large models (i.e., with more than 100 sub-rules connected to a rule) will cause scalability issues to arise. When modeling regulations, one of the steps in the guideline (step 9 in section 4.2.2) is to divide the contribution value between sub-rules or sub-conditions. The maximum value for a contribution is currently 100. If the number of sub-rules and sub-conditions exceeds 100 (in one level, or more likely through multiple levels of nested contributions), then dividing 100 between more than 100 links will become a problem, as we are dealing with integer values. A similar issue occurs with the computation of importance values. One solution would be to increase the contribution value range currently at -100..100 to a range with more values

such as $-10000..10000$ (depending on the number of instances to be handled), or to use real numbers instead of integers. This would require changes to URN and to jUCMNav.

In addition, some regulations are applicable only to specific categories of organizations. Stereotypes are used in step 7 of the guidelines (section 4.2.2) to distinguish between these categories and solve the noisiness and scalability issues discussed in Chapter 7. The IPCF approach was used on real sets of policies and rules for aviation security, with models containing hundreds of intentional elements. No scalability issues have been observed on that side at the moment, but there is no guarantee this approach will fit other kinds of complex policies, and validation experiments will be needed to raise the current confidence level. For example, when modeling some of Transport Canada's regulations, the maximum number of categories observed in any given regulation was four (e.g., TYPE1, TYPE2, TYPE3, OTHER), and this was easily manageable. However, if the number of categories increases, or if many groups of categories need to co-exist simultaneously, then it becomes more complicated and time consuming to add these categories to rules and possibly to conditions.

Impact Analysis: This criterion relates to how changing a policy or a business process impacts goal satisfaction and compliance. IPCF supports this property well. In IPCF, one can do both *what-if analysis* at the time a change to a policy, goal, or business process is considered by creating GRL strategies based on expected results and low-risk/high-risk variants, and *impact analysis* based on real data once that data becomes available. As discussed in the steps of the framework, GRL strategies are created before and after modifications to a business process (or to a business goal or a policy), and analysts and decision makers can then observe different impacts on organization goals, policies and business processes. This is also an opportunity to improve the models in case major discrepancies are observed between expected results and real results [108].

Reporting on Compliance: Kharbili *et al.* [66] included *cost* as a criterion in their original eight dimensions. However, it is premature to say anything about the cost of deploying and using IPCF at this time. Nevertheless, another common dimension in the literature (according to Koliads and Ghose [69] and to Silveira *et al.* [124]) is that compliance management frameworks should also report on the overall compliance of the or-

ganization. This is hence the eighth dimension used here. Although work remains to be done in that area, it was shown through an example how BI tools such as IBM Cognos Report Studio can be used within IPCF to create dashboards for decision makers that enable them to visualize and query compliance-related information, analyze the current state of the organization, and plan for the future.

Criteria	IPCF
Change Management	☞
Traceability & Accountability	☞
Complexity	👍
Efficiency	☞
Enforcement	👍
Scalability	☞
Impact Analysis	👍
Reporting on Compliance	☞

Table 44, Compliance Management Framework Properties, with Assessment of IPCF
 Supports: 👍 Partially Supports: ☞ Does Not Support: ☹

Table 44 summarizes the assessment of IPCF against the dimensions/criteria defined by Kharbili *et al.* [66], where *cost* was replaced by *reporting on compliance*. IPCF does not do badly on any of these criteria, and it supports well properties such as complexity, enforcement, and impact analysis.

8.3. Assessment Against BPCMS Features

Based on their literature review, Cabanillas *et al.* [22] describe important features that a Business Process Compliance Management System (BPCMS) should support during the

different phases of a business process lifecycle, including design, analysis, configuration, enactment, evaluation, and audit.

In the **design phase**, the business process should be modeled using a particular notation, and similarly for business rules. Business process and compliance experts should model these separately. When modeling a business process, if a modeler knows the rules that affect the business process, the modeling activity could be affected. Therefore, Cabanillas *et al.* suggest these two views should be modeled by different modelers and then combined to create a compliant business process (Collaborative capabilities). Furthermore, they argue that it would be very useful if the tool could automatically assist modelers in defining compliant business processes. This requires having rules in the tool that already know the activities of a business process (Automatic assistance).

In IPCF, modelers can model organization business processes and regulations in any order. These modelers can be the same person, or more likely different people. The modeling of these two views can be done independently or collaboratively. Afterwards, finding the rules that affect business processes and connecting them through URN links is simple. IPCF however does not support automatic assistance for modeling business processes.

Next is the **analysis phase**, where the business processes are analyzed to find non-compliance instances. In this phase a BPCMS should contain the following features:

- Yes/No compliance checking: The systems should illustrate whether a business process is compliant with a rule without getting into the detail of the business process;
- Explanatory compliance checking: An explanation of the non-compliance problems would be very useful for the modelers;
- Corrective advising: Giving advice to user of how to solve the detected problem would again be very useful to users; and
- Simulation of compliance issues: Simulate the compliance issues to detect unexpected behaviors.

In IPCF, by looking at the policy model, one can find the least compliance rules based on the compliance level, and then find the corresponding business processes through URN links (Yes/No compliance checking). IPCF also includes an OCL constraint that assesses compliance and finds compliance rules that are not sufficiently satisfied (Explanatory compliance checking). Furthermore, IPCF offers a prioritization mechanism to help analysts determine the non-complying rule with the highest impact on the business objectives and take corrective actions to improve business processes related to that rule (Corrective advising). In IPCF, one can define GRL strategies and analyze different what-if situations on organization goals, policies and business processes (Simulation of compliance issues).

Another phase discussed by Cabanillas *et al.* is **configuration**, which requires that “mechanisms to manage rule repositories and a compliance-aware process engine have to be considered during this phase” [22]. Then comes **enactment**, which “encompasses the actual run time of the business process, in which process monitoring plays an important role for providing accurate information on the status of business process instances” [22]. In this phase, a BPCMS should contain the following features: Compliance alert, Recovery actions, and Predictive analysis. Both these phases are out of IPCF’s scope.

In the **evaluation phase**, a BPCMS should contain the following features:

- Process mining: After process execution, the information should be saved in an event log that should contain all the information required to cover all the previous phases of a business process. This is again out of IPCF’s scope.
- Display of compliance result: A mechanism should show the result of the compliance in form of a dashboard. In IPCF, IBM Cognos is used to generate reports and dashboard on the status of the compliance.
- Root-cause-analysis: Find the root cause of the non-compliance from event logs or dashboard. In IPCF such analysis is done at the dashboard level as well as in the jUCMNav tool, and one can find the root cause of the non-compliance.

As for the **audit phase**, which is about managing compliance evidence, IPCF and jUCMNav enable the storing of monitored indicators (with the models where they apply) at different moments in time, hence providing partial support for audits.

Table 45 summarizes the assessment and identifies the phases where IPCF can be valuable and those where it can be improved or supported by complementary techniques.

Lifecycle phases	Feature	IPCF
Design	Collaborative capabilities	👍
	Automatic assistance	👎
Analysis	Yes/No compliance checking	👍
	Explanatory compliance checking	👉
	Corrective Advising	👉
	Simulation of compliance issues	👍
Configuration	Management of rule repository	👎
	Use of compliance-aware process engine	👎
	Recovery capabilities as for compliance problems	👎
Enactment	Compliance alert	👎
	Recovery actions	👎
	Predictive analysis	👎
Evaluation	Process mining	👎
	Display of compliance result	👉
	Root-cause analysis	👉
Audit	Compliance evidence	👉

Table 45, Assessment of IPCF against Common BPCMS Features

8.4. Tool Support

This section reports on the implementation of the new GRL propagation algorithm and OCL rules for the *measured compliance profile* in jUCMNav, with related visualization features. This implementation not only helped demonstrate that the proposed framework

and supporting analysis algorithm are realizable, it also enabled further evaluation of the framework using real-life examples.

The existing GRL quantitative evaluation algorithm supported by jUCMNav was extended to be able to evaluate the satisfaction of individual goal models that are members of a larger family model (see Chapter 7). To demonstrate that the implemented algorithm works, a sample GRL model is used, together with several strategies.

As illustrated in Figure 112, the sample model includes five goals and four types of organizations (namely, TYPE1, TYPE2, TYPE3, and OTHER). Goal1 is the top-level element and receives contributions from four sub-elements. Goal2 is only applied to organizations of TYPE1 and OTHER. Condition1 applies to Goal1 regardless of the organization type. Condition2 applies to OTHER organizations and Condition3 applies to organizations of TYPE1. Goal3 only applies to TYPE2 organizations, whereas Goal4 applies to TYPE1, and finally Goal5 to OTHER organizations.

Five strategies are defined, as shown on the bottom-left of Figure 112. In addition, metadata is added to each strategy (the name is *acceptStereotype*, and the value is the value of the type of organization targeted by the scenario, for instance TYPE1). For strategy TYPE1, highlighted in this figure, the algorithm ignores all nodes that are not tagged with TYPE1. Therefore, Goal3 and Goal5 are expected to be ignored and hence they (and their corresponding KPIs and links) are grayed out. In addition to goals, conditions that do not have TYPE1 will be ignored (see Condition2). When a condition has no stereotype, this condition is applied to all goals regardless of the organization type. For instance, Goal2 depends on condition1 regardless of what type it has.

Since Goal3 and Goal5 are ignored from the model, their contribution levels will be divided proportionally between the contribution levels of the remaining active intentional elements. As illustrated in Figure 112, the algorithm updates the runtime contribution of active intentional elements.

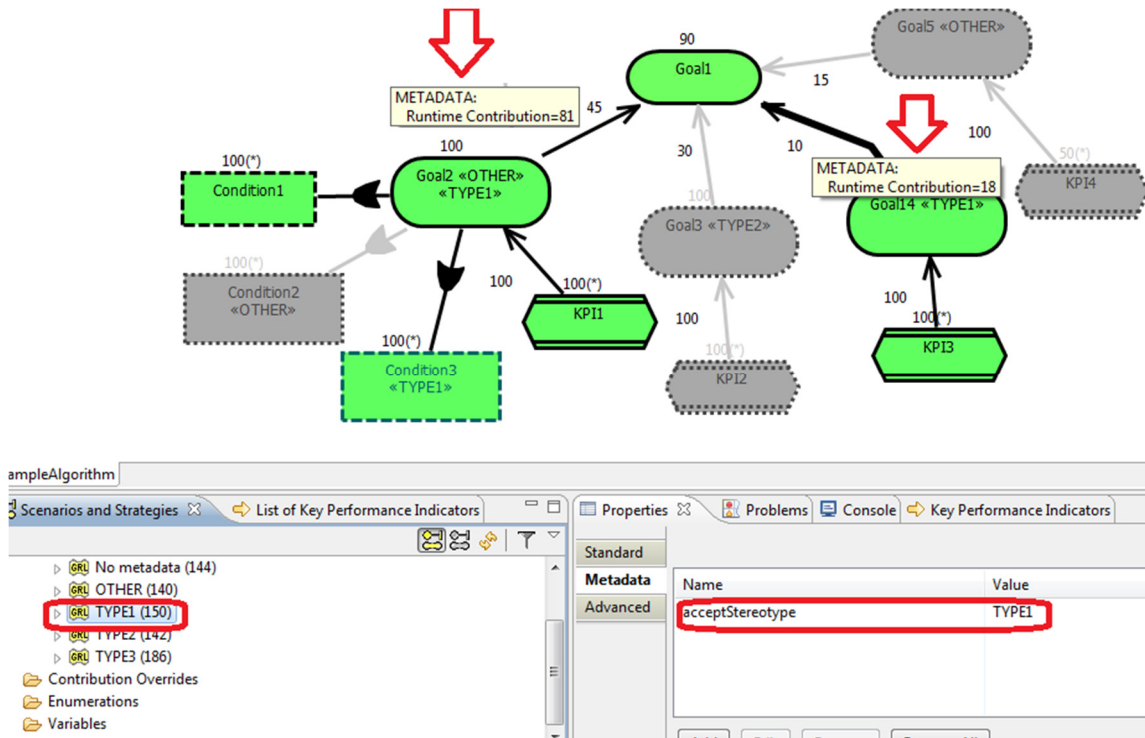


Figure 112, Evaluation of TYPE1 with the New Propagation Algorithm

Figure 113 shows a strategy for TYPE1 or TYPE2 (highlighted in red). Only goals and conditions tagged with TYPE1 or TYPE2 are accepted while the rest of the intentional elements are ignored and grayed out (i.e., Goal5 and Condition2 are ignored). The contribution value of Goal5 is divided proportionally between the contribution levels of the remaining intentional elements (Goal2, Goal3, and Goal4).

Figure 114 illustrates another strategy for TYPE1 or TYPE2 (highlighted in red), this time with Condition1 initialized to 0. The goals related to this condition should also be ignored. Goal2 is indeed ignored because the condition is not satisfied. Goal5 is also ignored since this it only applies to OTHER organizations. The contribution values of Goal5 and Goal2 are divided proportionally between the contribution levels of the remaining intentional elements (Goal3 and Goal4).

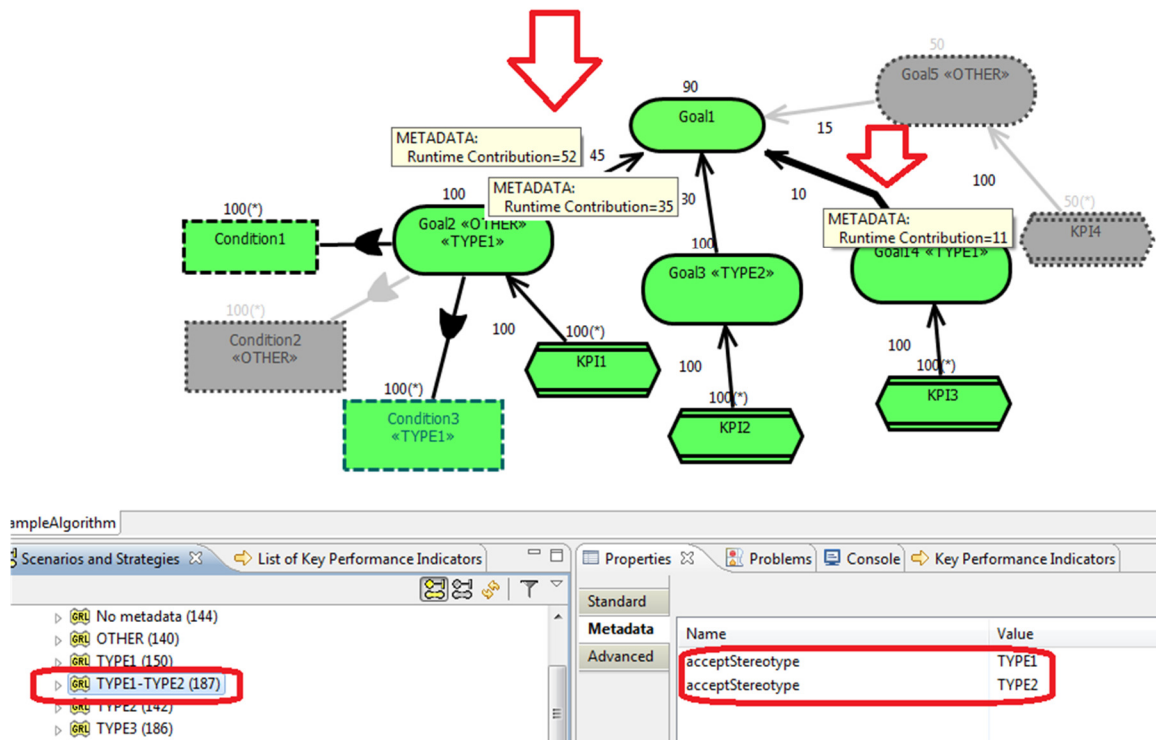


Figure 113, Evaluation of TYPE1/TYPE2 with the New Propagation Algorithm

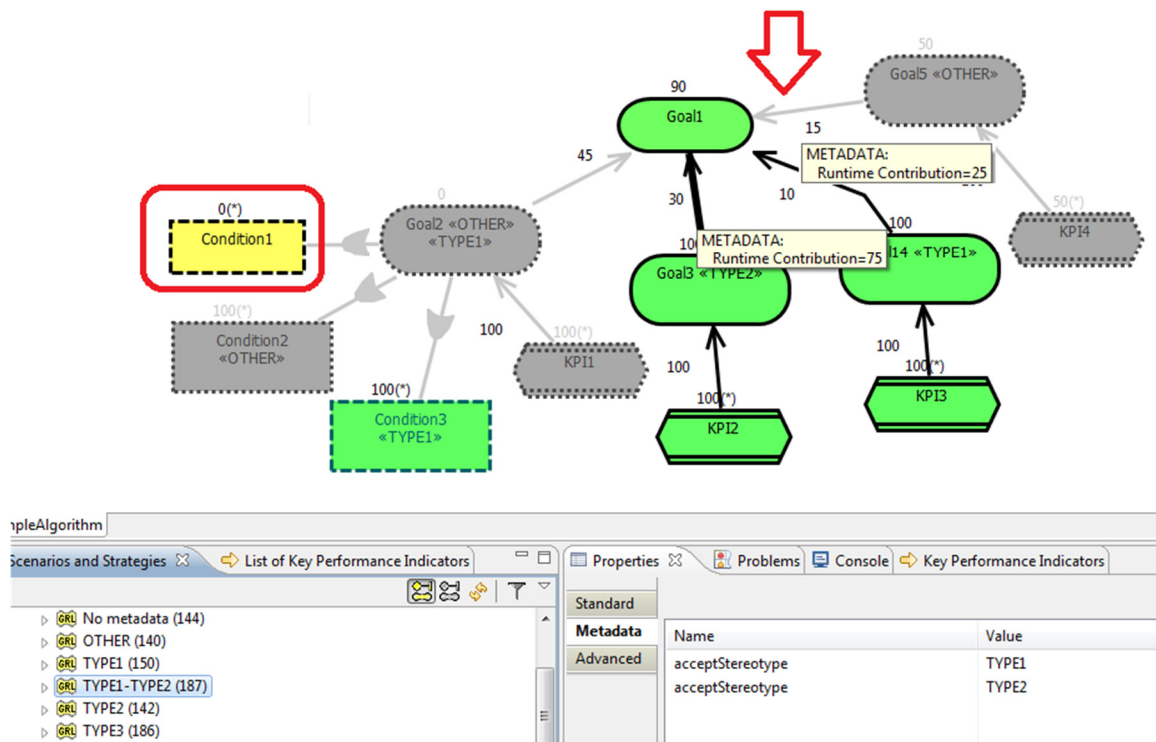


Figure 114, Evaluation of TYPE1/TYPE2 Strategies when Condition1 is 0

8.5. Summary

This chapter describes the assessment of the Indicator-based Policy Compliance Framework. All these assessments were performed by the author of this thesis and validated by the supervisor. No formal methods were used for this assessment and the ratings could be biased, which is a threat to the validity of the assessments. To improve the level of validity, a survey with more (independent) parties involved could be designed in the future.

IPCF was compared with other existing frameworks against several important criteria. One of the properties of IPCF that needs to be improved in the future is the identification of different types of constraints (obligations and permissions) that are part of the law. In addition, the reporting part of the framework can be improved to support drill-down and roll-up features. IPCF was also assessed against criteria proposed by well-known authors in the field of compliance. The features and limitations of IPCF were discussed, as well as the phases of a business process lifecycle where IPCF can be most helpful. Finally, the proof-of-concept implementation of IPCF-related modeling, analysis and visualization features in the jUCMNav tool was discussed.

The following chapter will summarize the main contributions of the thesis and present future work items.

Chapter 9. Conclusions

This chapter summarizes the contributions in section 9.1, the validation outcomes in section 9.2, and finally future work items in section 9.3.

9.1. Contributions

This thesis defines the *Indicator-based Policy Compliance Framework* (IPCF), which enables organizations to measure their compliance level to different policies as well as other types of rules, regulations, and laws. Defining the KPIs and monitoring them constantly helps regulators and regulated parties to detect non-compliance issues as soon as they are observed through the KPI values and to be proactive about addressing the issues.

The thesis has two major contributions and several minor contributions. The first major contribution is the IPCF framework consisting of a *unique structure for modeling the objectives of policies*, organization goals, and key performance indicators for *measuring compliance level of policies*. The framework also includes *guidelines for moving from regulations to models*, and indirectly from a document-based compliance approach to a model-based one. The second major contribution of the thesis is the tool-supported GRL profile and companion algorithm for handling compliance, conditions, and goal models families. The minor contributions of the thesis include a systematic literature review related to goals and compliance, a GRL importance algorithm, a technique for prioritizing non-compliance issues, many jUCMNav extensions, the use of BI tools for interactive compliance reporting, and finally validation through examples and comparisons with other frameworks. To highlight some of these contributions, the framework steps are summarized in this section.

IPCF consists of four main steps. For the **modeling step**, modelers must create goal and business process models of the organization, respectively with GRL and UCM.

URN links are used to specify traceability relationships. A GRL model of the policies also needs to be created.

Guidelines based on a formal metamodel are provided that enable modelers to create GRL models from textual policies and regulations. Furthermore, several OCL rules are available for checking the well-formedness of the resulting models, as well as for checking the compliance status. Model elements can be stereotyped to reflect the structure of source policy documents. In addition, model elements can have metadata as well as hyperlinks in order to establish fine-grained traceability to source policy documents. OCL queries are available to find model elements that correspond to the parts of policy documents under change.

While modeling real regulations, it was observed that not all rules are usually applicable to all types of organizations. Therefore, the GRL profile for measured compliance was extended to allow modelers to define a generic family of goal models for all types of organizations while tagging its model elements to specify which ones are applicable to which family member.

In the **evaluation step**, GRL strategies are defined to initialize KPI values in the model in order to calculate the compliance level of rules. An importance level computation algorithm is proposed that enables an organization to discover the default importance level of its business processes based on the organization's goals. Furthermore, jUCMNav's propagation algorithm is extended to support the evaluation of satisfaction levels of individual goal models that are members of a larger family model. Appropriate visualization of the results (graying out of non-member model elements) is also provided to simplify the analysis interpretation. For one of the examples in this thesis (sign regulation targeting aerodromes), BI reports created with Cognos IBM Report Studio are provided in order to access the raw data and feed KPI values to the GRL model strategies.

In the **improvement step**, a technique is also proposed to prioritize non-compliance issues based on a combination of importance *and* compliance level values. Such prioritization can guide managers in making appropriate decisions on how to improve business processes in order to increase their compliance level intelligently. BI tools

such as IBM Cognos Business Insight can be used to generate interactive dashboards with filters for decision makers who want to perform ad-hoc analysis on the data.

Finally, in the **monitoring step**, analysts can observe whether past decisions have led to the expected compliance level by feeding KPI values based on the latest data to GRL strategies. Current and past strategies (and even models) can be compared in jUCMNav. The same techniques can be used to do what-if analysis based on GRL strategies for predicting the impact on organization goals, policies and business processes and helping decision makers choose the best potential solution to improve the compliance level in the context of the organization.

From a research perspective, this thesis has demonstrated that a framework such as IPCF, which combines goals, processes, and indicators, is valuable for measuring compliance to regulations and later for helping decision makers prioritize what business processes and other organizational aspects should be improved. Along the way, many new tool features for analysis and visualization were developed, and they likely will be beneficial outside the compliance and business improvement contexts.

As for industrial impact, part of IPCF is now being explored by a national regulator in its transition from prescriptive-based compliance to outcome-based compliance, where goals and KPIs play an essential role [127]. IPCF has the potential to influence the process of creating policies and regulations, and the new trend is that goals together with indicators to measure them are being developed while writing/evolving regulations rather than just after the facts [21]. This is hoped to have a positive impact on the clarity of regulations and the precision of the compliance assessments. IPCF is also attracting the attention of other regulators, in Canada and elsewhere, and in various domains including finances and healthcare.

9.2. Validation Outcomes and Threat Mitigation

This section discusses some of the findings after validating the framework. The drawbacks of each step of the framework are discussed separately.

9.2.1 Modeling Step

In the modeling step, it was found that some regulation elements are only applicable to specific types of organizations. For instance, some of the Transport Canada policies only apply to specific aerodromes categories (or types). In addition, some rules are applicable only under certain conditions (independent of the type, and more dynamic by nature). If the conditions are true, then the associated rule should be imposed. Therefore a new GRL profile was added to IPCF as discussed in Chapter 7 to support various organization types and conditions. IPCF did not support this fully before evaluating the framework using Transport Canada's example about sign regulations for aerodromes. A first threat to validity here is that a large case study might be missing to fully validate IPCF's profile and tool support. However, this was mitigated by successfully using the full IPCF and jUCMNav on other (non-public) aviation security regulations such as Physical Security (about 50 rules), Security Policies and Procedures (about 120 rules), and Security Screening Operation (about 20 rules). Along the way, careful attention was given to make sure other types of terms from legal documents were not missing from those already mapped to GRL models.

Before the evaluation of the framework, there were no guidelines for extracting GRL models from legal documents. After observing that different modelers were coming up with inappropriate models, a more formal metamodel-based procedure was proposed for creating GRL models from regulation and policy documents. In an informal exercise meant to evaluate the accuracy of a previous version of the procedure (without the metamodel), six people working for a regulator or studying at the University of Ottawa used the procedure to model specific parts of a sample public regulation. After reviewing the models produced in collaboration with the participants, several suggestions were received and helped improve the procedure and its guidelines. In particular, optimization steps were much clarified. The final result is the procedure described in section 4.2.2. Although the guidelines help with the definition of the KPIs, there is still a good chance that different modelers could come up with different sets of KPIs for same policy. In some cases, due to ambiguities in some regulations, it is necessary to discuss with policy writers in order to be able to define appropriate KPIs for the rules. This issue is mainly due to the fact that KPIs have to be inferred from existing prescriptive legal document, from which

KPIs are usually absent. This issue should fade out in the future as policy makers move towards outcome-based regulations, where goals and indicators must be identified.

9.2.2 Evaluation Step

In the evaluation step, the jUCMNav tool and its propagation algorithm were extended to support goal model families and conditions, with appropriate visualizations. The new algorithm was tested and used on Transport Canada examples. There were four different types in Transport Canada's regulations. The proposed algorithm worked well for analyzing the models. However, one threat is that if the number of types increases substantially, then strategy maintenance could become challenging. In addition, as discussed in section 8.2 under the scalability criterion, the current URN scale of -100..100 for contributions and the 0..100 scale for importance values are not sufficient for analyzing large models accurately.

9.2.3 Improvement Step

Although IPCF has an improvement step, it does not provide any concrete guidelines on how to actually improve the processes to achieve higher level of compliance. Only the identification of high-impact business processes is provided. Although this can be considered one shortcoming of the framework, this is due the fact that depending on the context, existing processes, and target regulations, the improvement approaches could be very different. Therefore, it is very challenging to come up with domain-independent guidelines for business process improvement and this remains a challenge for the analysts and decision makers who use the framework.

9.2.4 Monitoring Step

The evaluation of the monitoring step is the weakest part of this thesis. To be able to perform proper evaluation of the monitoring step, historical data used for prediction (through GRL strategies) and results of changes that happened because of a business process modification after the improvement step are required. However, because such data was unavailable (as we did not go through real organizational improvements), the evaluation of the monitoring step of the framework is limited. However, to mitigate this threat to the

validity of the IPCF, several hypothetical situations were defined for both examples in order to be able to observe potential outcomes of the monitoring step, and at least to validate the technical feasibility of such monitoring.

In terms of tool support, the integration between BI tools and the jUCMNav modeling tool still needs much improvement. Currently, data needs to be input manually (e.g., in GRL strategies) or exchanged via comma-separated value files (which can be imported to or output from GRL strategies). To mitigate this threat to the validity of the tool results, a set of BI reports and a BI dashboard were designed for the sign regulation example (section 6.3) in such a way that an analyst can observe and monitor the KPI values directly.

9.3. Future Work

Future work can be broadly grouped into the following areas:

- Proper empirical evaluations of the usability of IPCF should be done.
- One of the important dimensions of compliance management frameworks is cost [65]. As the cost of IPCF was not evaluated in this thesis, this criterion should be investigated as part of future work.
- The suitability and generality of IPCF should be investigated in other application domains such as accounting and the financial sector.
- A better integration between jUCMNav and BI tools such as IBM Cognos should be pursued.
- Better support for qualitative indicators (and not just quantitative indicators) [127], together with better guidance on how to select appropriate indicators, should be provided.
- The current GRL evaluation algorithms are all bottom-up, and hence they can only be used to assess strategies defined explicitly. In order to be able to suggest appropriate KPI target values given the satisfaction values required for high-level compliance goals, a top-down quantitative evaluation algorithm (i.e., a search algorithm) should be designed and implemented.

- The current URN scale for GRL contributions and importance values is too limited for analyzing large compliance models, and so a solution should be investigated.
- IPCF does not identify different deontic modalities from legal documents (such as obligations, interdictions, permissions, and rights). Whether such modalities bring value to IPCF should be investigated.
- A better handling of conflict resolution between conflicting policies is required. Although the modeling helps with the detection of conflicting rules, this is a manual activity at this point. Using OCL constraints for detecting conflicts can be helpful to improve this aspect of the framework. For example, one potentially interesting constraint could be written to detect business processes with more than one rule or policy applied to them.

References

- [1] Abdullah, S., Hikmi, S., Indulska, M., and Sadiq, S.: “A study of compliance management in information systems research”. In: *17th European Conference On Information Systems (ECIS 2009)*, Verona, Italy, pp. 1711-1721 (June 2009)
- [2] Ali, R., Dalpiaz, F., and Giorgini, P.: “A Goal-based Framework for Contextual Requirements Modeling and Analysis”. *Requirements Engineering Journal*, Springer, Vol. 15, pp. 439-458 (2010)
- [3] Allstream: *Internet Access and Hosting Service Level Agreement*, Version 03/12/04Allstream, <http://www.allstream.com/home/> (accessed April 2011)
- [4] Amyot, D.: “Introduction to the User Requirements Notation: Learning by Example”. *Computer Networks*, Elsevier, Vol. 42(3), pp. 285-301 (2003)
- [5] Amyot, D., Horkoff, J., Gross, D., and Mussbacher, G.: “A lightweight GRL profile for i* modeling”. In: *ER 2009 Workshops (CoMoL, ETheCoM, FP-UML, MOST-ONISW, QoIS, RIGiM, SeCoGIS) on Advances in Conceptual Modeling - Challenging Perspectives*, Brazil, LNCS 5833, Springer-Verlag, pp. 254-264 (November 2009)
- [6] Amyot, D., Ghanavati, S., Horkoff, J., Mussbacher, G., Peyton, L., and Yu, E.: “Evaluating Goal Models within the Goal-oriented Requirement Language”. *International Journal of Intelligent Systems*, John Wiley & Sons, Inc , Vol. 25, Issue 8, pp. 841-877 (2010)
- [7] Amyot, D. and Mussbacher, G.: “User Requirements Notation: The First Ten Years, The Next Ten Years”. *Journal of Software (JSW)*, Vol. 6, No. 5, pp. 747–768 (May 2011)
- [8] Amyot, D., Shamsaei, A., Kealey, J., Tremblay, E., Miga, A., Mussbacher, G., Alhaj, M., Tawhid, R., Braun, E., and Cartwright, N.: “Towards Advanced Goal Model Analysis with jUCMNav”. In: *3rd Int. Workshop on Requirements, Intentions and Goals in Conceptual Modeling (RIGiM'12)*, Florence, Italy, LNCS 7518, Springer, pp. 201-210 (October 2012)
- [9] Anderson, C.: *What's the Difference Between Policies and Procedures?* <http://www.bizmanualz.com/blog/whats-the-difference-between-policies-and-procedures.html> (accesses September 2012)
- [10] Awad, A., Smirnov, S., and Weske, M.: “Towards Resolving Compliance Violations in Business Process Models”. In: *Governance, Risk and Compliance on Information systems (GRCIS'09)*, Netherlands, CEUR-WS.org, Vol. 459, pp. 16-30 (June 2009)

- [11] Bach, J.: “The immaturity of CMM”. *American Programmer*, Vol. 7, No. 9, pp. 13-18 (1994)
- [12] Bajwa, I.S., Lee, M.G., Bordbar, B.: “SBVR Business Rules Generation from Natural Language Specification”. In: *AAAI Spring Symposium 2011 – Artificial Intelligence 4 Business Agility*, San Francisco, USA, pp. 541-545 (March 2011)
- [13] Base II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework, <http://www.bis.org/publ/bcbs107.htm> (accessed October 2011)
- [14] Basili, V. R.: “Using Measurement to Build Core Competencies in Software”. In: *Seminar sponsored by Data and Analysis Center for Software* (2005)
- [15] Basili, V. R.: “Applying the Goal/Question/Metric Paradigm in the Experience Factory”. In: *Tenth Annual CSR (Centre for Software Reliability) Workshop, Application of Software Metrics and Quality Assurance in Industry*, Amsterdam, Holland (September-October 1993)
- [16] Becker, J., Bergener, P., Delfmann, P., Eggert, M., Weiß, B.: “Supporting Business Process Compliance in Financial Institutions – A Model-Driven Approach”. In: *Proceedings of the 10 Internationale Tagung Wirtschaftsinformatik (WI 2011)*, Zürich, Switzerland, pp. 335-364 (February 2011)
- [17] Behnam, S.A., Amyot, D., Forster, A.J., Peyton, L., and Shamsaei, A.: “Goal-Driven Development of a Patient Surveillance Application for Improving Patient Safety”. In: *4th International MCE Tech Conference on eTechnologies*, Ottawa, Canada, Springer Berlin Heidelberg, LNBIP, Vol. 26, pp. 65-76 (May 2009)
- [18] Berender, P. and Jönsson, P.: “A Goal Question Metric Based Approach for Efficient Measurement Framework Definition”. In: *Proceedings of the 2006 ACM/IEEE international symposium on Empirical software engineering (ISESE '06)*, Rio de Janeiro, Brazil, ACM New York, pp. 316-325 (September 2006)
- [19] Boehmer, W.: “Cost-Benefits Trade-Off Analysis of an ISM Based on ISO 27001”. In: *International Conference on Availability, Reliability and Security. ARES '09*, Fukuoka, Japan, IEEE Computer Society, pp. 392-399 (March 2009)
- [20] Borba, C., and Silva, C.: “A Comparison of Goal-Oriented Approaches to Model Software Product Lines Variability”. In: *ER 2009 Workshops on Advances in Conceptual Modeling - Challenging Perspectives*, Springer, LNCS, Vol. 5833, pp. 244-253 (November 2009)
- [21] Braun, E., Cartwright, N., Shamsaei, A., Behnam, S.A., Richards, G., Alhaj, M., and Mussbacher, G.: “Drafting and Modeling of Regulations: Is It Being Done Backward”. In: *5th Requirements Engineering and Law (RELAW 2012)*, Chicago, USA. IEEE CS, pp. 1-6 (September 2012)
- [22] Breux, T., and Antón, A.: “Analyzing goal semantics for rights, permissions, and obligations”. In: *13th IEEE Int. Conf. on Requirements Eng. (RE'05)*, Paris, France, pp. 177-186 (August-September 2005)

- [23] Cabanillas, C., Resinas, M., and Ruiz-Cortes, A.: “Exploring Features of a Full-Coverage Integrated Solution for Business Process Compliance. In: *Governance, Risk and Compliance on Information systems (GRCIS'11)*, London, UK, Springer, LNBIP, Vol. 83, pp. 218-227 (June 2011)
- [24] *Canadian Airport Operations, Chapter 6*. http://www.aerotraining.com/reference/AC%2061-23C_Chapter_6_Canada.pdf (last accessed April 2012)
- [25] Canada Gazette – *Government Notices*. <http://canadagazette.gc.ca/rp-pr/p1/2011/2011-12-10/html/notice-avis-eng.html#d101> (accessed February 2012)
- [26] Card, D.: “Practical software measurement”. In: *25th Int. Conf. on Software Engineering (ICSE '03)*, Portland, Oregon, IEEE Computer Society, pp. 738-739 (May 2003)
- [27] Cleven, A., and Winter, R.: “Regulatory Compliance in Information Systems Research - Literature Analysis and Research Agenda”. In: *Enterprise, Business-Process and Information Systems Modeling*, Springer, LNBIP, Vol. 29, pp. 174-186 (2009)
- [28] *COBIT Framework for IT Governance and Control*, <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx> (accessed January 2011)
- [29] Compliance LLC: *The Sarbanes-Oxley Act*, <http://www.sarbanes-oxley-act.biz/SarbanesOxleyAct.htm> (accessed October 2011)
- [30] Cost Advisors, Inc.: “SOX Compliance: 10 steps to Savings”. http://www.costadvisors.com/downloads/SOX_Article.pdf (2009)
- [31] Dang, J., Hedayati, A., Hampel, K., and Toklu, C.: “An ontological knowledge framework for adaptive medical workflow”. *Journal of Biomedical Informatics*, Elsevier Science San Diego, USA, Vol. 41, pp. 829-836 (2008)
- [32] Dictionary.com: <http://dictionary.reference.com/browse/compliance> (accessed January 2011)
- [33] DifferenceBetween.net: *Difference Between an Act and Regulation* (September 2009). <http://www.differencebetween.net/business/difference-between-an-act-and-a-regulation/> (accessed August 2011)
- [34] DifferenceBetween.net: *Difference Between Rules and Policies* (May 2011). <http://www.differencebetween.com/difference-between-rules-and-vs-policies/> (accessed August 2011)
- [35] Eclipse Foundation: *EMF Compare*. 2012. <http://www.eclipse.org/emf/compare/> (last accessed June 2012)
- [36] Fenton, N. E., and Pfleeger, S. L.: “Software Metrics: A Rigorous & Practical Approach”. In: *PWS Publishing Company*, Second Edition, ISBN:0-534-95425-1 (1997)

- [37] Foorthuis, R., and Bos, R.: "A Framework for Organizational Compliance Management Tactics". In: *Governance, Risk and Compliance on Information systems (GRCIS'11)*, London, UK, Springer, LNBIP, Vol. 83, p. 259-268 (June 2011)
- [38] Gerke, K., Cardoso, J., and Claus, A.: "Measuring the Compliance of Processes with Reference Models". In: *On the Move to Meaningful Internet Systems (OTM 2009)*, Vilamoura, Portugal, Springer-Verlag Berlin, Heidelberg, pp. 76-93 (November 2009)
- [39] Ghanavati, S., Amyot, D., and Peyton, L.: "A Requirements Management Framework for Privacy Compliance". In: *The 10th Workshop on Requirements Engineering (WER 2007)*, Toronto, Canada, pp. 149-159 (May 2007)
- [40] Ghanavati, S., Amyot, D., and Peyton, L.: "Towards a Framework for Tracking Legal Compliance in Healthcare". In: *19th International Conference on Advanced Information Systems Engineering (CAiSE'07)*, Trondheim, Norway, Springer-Verlag Berlin, Heidelberg, LNCS, Vol. 4495, pp. 218-232 (June 2007)
- [41] Ghanavati, S.: *A Compliance Framework for Business Processes Based on URN*, M.Sc. thesis, University of Ottawa, Canada (May 2007)
- [42] Ghanavati, S., Amyot, D., and Peyton, L.: "Compliance Analysis Based on a Goal-oriented Requirement Language Evaluation Methodology". In: *17th IEEE International Requirements Engineering Conference (RE'09)*, Atlanta, USA, IEEE CS, pp. 133-142 (August-September 2009)
- [43] Ghanavati, S., Siena, A., Perini, A., Amyot, D., Peyton, L., and Susi, A.: "A Legal Perspective on Business: Modeling the Impact of Law". In: *4th International MCeTech Conference on eTechnologies*, Ottawa, Canada, Springer Berlin Heidelberg, LNBIP, Vol.26, pp. 267-278 (May 2009)
- [44] Ghanavati, S., Amyot, D., Peyton, L., Siena, A., Perini, A., and Susi, A.: "Integrating business strategies with requirement models of legal compliance". *International Journal of Electronic Business (IJEB)*, Vol.8, N.3, pp. 260-280 (2010)
- [45] Ghanavati, S., Amyot, D., and Peyton, L.: "A Systematic Review of Goal-oriented Requirements Management Frameworks for Business Process Compliance". In: *4th Int. Work. on Requirements Engineering and Law (RELAW)*, IEEE CS, pp. 25-34 (2011)
- [46] Government of Canada: *Audit of Aviation Security Regulatory Oversight*, April 2011. <http://www.tc.gc.ca/eng/corporate-services/aas-audit-870.htm>
- [47] Government of Ontario: *Personal Health Information Protection Act, 2004*, <http://www.e-laws.gov.on.ca/index.html> (accessed January 2011)
- [48] *Gramm-Leach-Bliley Act*, <http://www.ftc.gov/privacy/glbact/glbsub1.htm> (accessed October 2011)
- [49] Hammer, M.: "What is Business Process Management?". In: Brocke, J.v., and Rosemann, M. (Editors) *Handbook on Business Process Management 1*, Springer-Verlag, pp. 3-16 (2010)

- [50] Hamou-Lhadj, AK., and Hamou-Lhadj, AW.: “Towards a compliance support framework for global software companies”. In: *11th IASTED Int. Conf. on Software Engineering and Applications*, USA, ACTA Press, pp. 31-36 (November 2007)
- [51] Henver, A.R., March, A.T., Park, J., and Ram, S.: “Design science in information systems research”. In: *MIS Quarterly*, Vol. 28, No.1, pp. 75-105 (March 2004)
- [52] *HIPAA Regulations*, <http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php> (accessed October 2011)
- [53] *HR Management: Laws and regulations*. http://www.cliffsnotes.com/study_guide/HR-Management-Laws-and-Regulations.topicArticleId-8944,articleId-8892.html (accessed April 2011)
- [54] *HRdownloads Website*. <http://www.hrdownloads.com/> (accessed October 2010)
- [55] Illinois Banker Association: *IBA Survey on Impact of Dodd-Frank Act*, http://www.ilbanker.com/Adobe/GR/Washington_Visit_ExecSummary_2010.pdf, (2010)
- [56] IEEE Computer Society: *IEEE Std 610.12-1990 - Standard Glossary of Software Engineering Terminology*. E-ISBN: 0-7381-0391-8 (1990)
- [57] International Telecommunication Union: *Recommendation Z.151 (11/08), User Requirements Notation (URN) – Language definition*, November 2008, <http://www.itu.int/rec/T-REC-Z.151/en> (accessed September 2012)
- [58] ISO/IEC: *ISO/IEC 15504-1:2004, Information technology — Process assessment — Part 1: Concepts and vocabulary* (2004)
- [59] ITIL: *Information Technology Infrastructure Library*, <http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp> (accessed January 2011)
- [60] IT Policy Compliance Group: *Why Compliance Pays*. Research report, July 2007. <http://www.itpolicycompliance.com/research-reports/why-compliance-pays/> (accessed October 2012)
- [61] *Job Canada*, <http://www.jobcanada.org/salary.html> (accessed April 2010)
- [62] *jUCMNav*, Version 5.2.0, University of Ottawa <http://softwareengineering.ca/jucmnav> (accessed September 2012)
- [63] Karagiannis, D., Mylopoulos, J., Schwab, M.: “Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act”. In: *15th IEEE International Requirements Engineering Conference (RE '07)*, Delhi, India, IEEE CS, pp. 315-321. (October 2007)
- [64] Karagiannis, D: “A Business Process-Based Modelling Extension for Regulatory Compliance”. In: *MKWI 2008*, Berlin, Germany, CEUR Workshop Proceedings 328 CEUR-WS.org 2008, pp. 1159-1173. (February 2008)
- [65] Kharbili, M.E., and Stein, S.: “Policy-Based Semantic Compliance Checking for Business Process Management”. In: *MobIS Workshops 2008*, Saarbrücken, Germany, CEUR-WS.org, pp. 178-192 (November 2008)

- [66] Kharbili, M.E., Stein, S., Markovic, I., and Pulvermuller, E.: “Towards a Framework for Semantic Business Process Compliance Management”. In: *Governance, Risk and Compliance on Information systems (GRCIS’08)*, Montpellier, France, CEUR-WS.org, pp.1-15 (June 2008)
- [67] Kitchenham, B.: *Procedures for performing systematic reviews*. Technical Report, Keele University and NICTA, Staffordshire, UK (2004)
- [68] Kiyavitskaya, N., Zeni, N., Breaux, T., Antón, A., Cordy, J., Mich, L., and Mylopoulos, J.: “Automating the Extraction of Rights and Obligations for Regulatory Compliance”. In: *Proc. 27th International Conference on Conceptual Modelling (ER’08)*, Barcelona, Spain, pp. 154-168 (October 2008)
- [69] Koliads, G., and Ghose, A.: *Service Compliance: Towards Electronic Compliance Programs*. Technical Report, Decision Systems Lab, University of Wollongong, Australia (2008)
- [70] Kilbridge, P.: “The Cost of HIPAA Compliance”. *New England Journal of Medicine (NEJM)*, Vol. 348, pp. 1423-1424 (2003)
- [71] Kronz, A.: “Managing of Process Key Performance Indicators as Part of the ARIS Methodology”. In: *Corporate Performance Management*, Springer Berlin Heidelberg, pp. 31-44 (2006)
- [72] Kurian, R.: *The Benefits to Management of using GQM, Continuous GQM and V-GQM in a Measurement Program*. M.Sc. thesis, Kent State University, UK (2009)
- [73] Lapouchnian, A., Mylopoulos, J.: “Modeling domain variability in requirement engineering”. In: *28th Int. Conf. on Conceptual Modeling (ER’09)*, Springer, LNCS, Vol. 5829, pp. 115–130 (November 2009)
- [74] Lapouchnian, A., Mylopoulos, J.: “Capturing Contextual Variability in *i** Models”. In: *Proc. 5th Int. *i** Workshop*, Trento, Italy, CEUR, Vol. 766, pp. 96-101 (September 2011)
- [75] *LAX Tenant Signage Standards*, <http://www.lawa.org/uploadedfiles/lax/pdf/LAX%20Standards.pdf> (July 2008)
- [76] Library and Archives Canada: *Retention Guidelines for Common Administrative Records of the Government of Canada*, <http://www.collectionscanada.gc.ca/government/products-services/007002-3160.3-e.html> (accessed April 2011)
- [77] Lu, R., Sadiq, S., Governatori, G.: “Measurement of Compliance Distance in Business Processes”. *Info. Sys. Management*, Taylor & Francis, Inc., USA, Vol. 25, pp. 344-355 (2008)
- [78] Ly, L.T., Göser, K., Rinderle-Ma, S., and Dadam, P.: “Compliance of Semantic Constraints A Requirements Analysis for Process Management Systems”. In: *Governance, Risk and Compliance on Information systems (GRCIS’08)*, Montpellier, France, CEUR-WS.org, pp. 31-45 (June 2008)
- [79] Mahnic, V., and Zabkar, N.: “Using COBIT indicators for measuring scrum-based software development”. In: *WSEAS Transactions on Computers*, World Scientific

- and Engineering Academy and Society (WSEAS), Vol. 7, Issue 10, pp. 1605-1617 (2008)
- [80] Mahnic, V., and Zabkar, N.: "Assessing Scrum-based software development process measurement from COBIT perspective". In: *ICCOMP'08 Proceedings of 12th WSEAS International Conference on Computers*, Heraklion, Greece, World Scientific and Engineering Academy and Society (WSEAS), pp. 589-594 (July 2008)
 - [81] Marino, D., Massacci, F., Micheletti, A., Rassadko, N and Neuhaus, S.: "Satisfaction of Control Objectives by Control Processes". In: *Service-Oriented Computing, 7th International Joint Conference, ICSOC-ServiceWave 2009*, Stockholm, Sweden, Springer, LNCS, Vol. 5900, pp. 531-545 (November 2009)
 - [82] Massacci, F., Yautsiukhin, A.: "An algorithm for the appraisal of assurance indicators for complex business processes". In: *QoP'07 Proceedings of the 2007 ACM workshop on Quality of protection*, Alexandria, VA, USA, ACM, pp. 22-27 (October 2010)
 - [83] Martin, C., and Refai, M.: "A Policy-Based Metrics Framework for Information Security Performance Measurement". In: *Second IEEE/IFIP International Workshop on Business-driven IT Management (BDIM'07)*, Munich, Germany, IEEE 2007, pp. 94-101 (May 2007)
 - [84] Martinez, A., Gonzalez, N., and Estrada, H.: "A Goal-Oriented Approach for Workflow Monitoring". In: *Fourth Int. i* Workshop*, Tunisia, CEUR-WS.org , pp. 118-122 (June 2010)
 - [85] Moody, D.L., Sindre, G., Brasethvik, T., and Solvberg, A.: "Evaluating the Quality of Information Models: Empirical Testing of a Conceptual Model Quality Framework". In: *The 25th International Conference on Software Engineering (ICSE 2003)*, Portland, Oregon, USA, IEEE Computer Society, pp. 295-305 (May 2003)
 - [86] Morandini, M., Sabatucci, L., Siena, A., Mylopoulos, S., Penserini, L., Perini, A., and Susi, A.: "On the use of the Goal-Oriented Paradigm for System Design and Law Compliance Reasoning". In: *Fourth Int. i* Workshop*, Tunisia, CEUR-WS.org, pp. 71-75 (June 2010)
 - [87] Morrison, E., Ghose, A., and Koliadis, G.: "Dealing With Imprecise Compliance Requirements". In: *Enterprise Distributed Object Computing Conference Workshops (EDOCW 2009)*, Auckland, New Zealand, IEEE Computer Society, pp. 6-14 (September 2009)
 - [88] Mussbacher, G. and Amyot, D.: "Assessing the Applicability of Use Case Maps for Business Process and Workflow Description". *3rd Int. MCeTech Conference on eTechnologies*, Montréal, Canada, IEEE Computer Society, pp. 219-222 (January 2008)
 - [89] Mussbacher, G., Araújo, J., Moreira, A., and Amyot, D.: "AoURN-based Modeling and Analysis of Software Product Lines". *Software Quality Journal*, Springer, published online (July 2011)

- [90] Namiri, K., and Stojanovic, N.: "Towards a Formal Framework for Business Process Compliance". In: *Multikonferenz Wirtschaftsinformatik (MKWI 2008)*, München, Germany, GITO-Verlag, Berlin, pp. 1185-1196 (February 2008)
- [91] Negash, S., and P. Gray.: "Business Intelligence". Burstein. B., and Holsapple, C.W. (Editors). In: *Handbook on Decision Support Systems 2*. Springer, Berlin Heidelberg, pp. 175-193 (2008)
- [92] Nigam, A., Jeng, J., Chao, T., Chang, H.: "Managed Business Artifacts". In: *2008 IEEE International Conference on e-Business Engineering (ICEBE '08)*, China, IEEE Computer Society, pp. 390-395 (October 2008)
- [93] Open Compliance & Ethics Group (OCEG): *GRC Capability Model*, <http://www.oceg.org/> (accessed October 2012)
- [94] Open Management Group: *Business Process Modeling Notation (BPMN) website*. <http://www.bpmn.org> (accessed October 2012)
- [95] Open Management Group: *Semantics of Business Vocabulary and Business Rules (SBVR)*, v1.0 (January 2008)
- [96] Open Management Group: *Unified Modeling Language (UML) website*. <http://www.uml.org> (accessed October 2012)
- [97] Otto, P.N., and Antón, A.I.: "Addressing legal requirements in requirements engineering". In: *15th IEEE Int. Conf. on Requirements Engineering (RE'2007)*, Delhi, India, IEEE CS, pp. 5-14 (October 2007)
- [98] Pasic, A., Bareno, J., Gallego-Nicasio, B., Torres, R., and Fernandez, D.: "Trust and Compliance Management Models in Emerging Outsourcing Environments". In: *The 10th IFIP Conference on e-Business, e-Services, and e-society (I3E 2010)*, Buenos Aires, Argentina, International Federation for Information Proceeding (IFIP) Springer, Vol. 341, pp. 237-248 (November 2010)
- [99] Papazoglou, M.P.: "Making Business Processes Compliant to Standards and Regulations". In: *15th IEEE International Enterprise Distributed Object Computing Conference, EDOC 2011*, Helsinki, Finland, IEEE Computer Society 2011, pp. 3-13 (August 2011)
- [100] *Practical Software and Systems Measurement (PSM)* http://www.psmc.com/Downloads/Other/PSMMethodsofOperations_Nov2006.pdf (accessed June 2011)
- [101] *Penalties for HIPAA Violations - Biometrics Direct* <http://www.biometricsdirect.com/Biometrics/laws/HIPAA/hipaaviolations.htm> (accessed March 2011)
- [102] Phelps, B.: *Smart Business Metrics: Measure what really counts and manage the difference*. Financial Times Prentice Hall, ISBN: 0273663968 (2004)
- [103] Popova, V., and Sharpanskykh, A.: "Formal modelling of organisational goals based on performance indicators". *Data & Knowledge Engineering*, Vol. 70, Issue: 4, pp. 335-364 (2011)
- [104] Pourshahid, A., Mussbacher, G., Amyot, D. and Weiss, M.: "An Aspect-Oriented Framework for Business Process Improvement". In: *4th International MCEtech*

- Conference on eTechnologies*, Ottawa, Canada, Springer Berlin Heidelberg, LNBIP, Vol. 26, pp. 290-305 (May 2009)
- [105] Pourshahid, A., Amyot, D., Peyton, L., Ghanavati, S., Chen, P., Weiss, M. and Foster, A.: "Business process management with the User Requirements Notation". *Electronic Commerce Research*, Springer, Vol. 9, Issue: 4, pp. 269-316 (2009)
 - [106] Pourshahid, A.: *A URN-based methodology for business process monitoring*. M.Sc. thesis, E-Business Technology, University of Ottawa, Canada, <http://jucmnav.softwareengineering.ca/twiki/bin/view/UCM/VirLibPourshahidMScThesis> (March 2008)
 - [107] Pourshahid, A., Amyot, D., Chen, P., Weiss, M., and Forster, A.J.: "Business Process Monitoring and Alignment: An Approach Based on the User Requirements Notation and Business Intelligence Tools". In: *10th Workshop on Requirements Eng. (WER 2007)*, Toronto, Canada, pp. 80-91 (May 2007)
 - [108] Pourshahid, A., Richards, G., and Amyot, D.: "Toward a Goal-Oriented, Business Intelligence Decision-Making Framework". In: *5th International MCETECH Conference on eTechnologies*, Les Diablerets, Switzerland. Springer, LNBIP, Vol. 78, pp. 100-115 (January 2011)
 - [109] OCEG: *GRC Capability Model*, <http://www.oceg.org/> (accessed July 2011)
 - [110] Radovanovic, D.R., Lucic, T., and Sarac, D.: "IT audit in accordance with COBIT standard". In: *MIPRO2010*, Opatija, Croatia, Proceedings of the 33rd Convention, pp. 1137-1141 (May 2010)
 - [111] Rifaut, A.: "Compliance management with measurement frameworks". In: *4th Int. Work. on Requirements Engineering and Law (RELAW)*, Trento, Italy, IEEE CS, pp. 15-24 (August 2011)
 - [112] Thomson Reuters: *Managing to the Speed of Regulatory Change – Governance, Risk and Compliance Survey*, Report, http://accelus.com/sites/default/files/Governance_Risk_and_Compliance_Survey.pdf (accessed October 2011)
 - [113] Rifaut, A., and Dubois, E.: "Using Goal-Oriented Requirements Engineering for Improving the Quality of ISO/IEC 15504 based Compliance Assessment Frameworks". In: *16th IEEE International Requirements Engineering Conference, (RE '08)*, Barcelona, Catalunya, Spain, 16th IEEE, pp. 33-42 (September 2008)
 - [114] Rodriguez, C., Silveira, P., Daniel, F., and Casati, F.: "Analyzing Compliance of Service-Based Business Processes for Root-Cause Analysis and Prediction". In: *10th International Conference on Web Engineering (ICWE 2010)*, Vienna, Austria, Springer, LNCS, Vol. 6385, pp. 277-288 (July 2010)
 - [115] Sadiq, S.W., Governatori, G., and Namiri, K.: "Modeling control objectives for business process compliance". In: *Business Process Management (BPM 2007)*, Brisbane, Australia, Springer 2007, LNCS, Vol. 4714, pp. 149-164 (September 2007)

- [116] Simply Hired: *Airport Operations Crew Salaries in Canada*
<http://www.simplyhired.com/a/salary/search/q-airport+operations+crew/l-canada>
 (accessed April 2012)
- [117] Schaar, D., Sherry, L.: *Analysis of Airport Stakeholders*.
http://catsr.ite.gmu.edu/pubs/ICNS_Schaar_AirportStakeholders.pdf (February 2010)
- [118] Shamsaei, A., Pourshahid, A., and Amyot, D.: "Business Process Compliance Tracking Using Key Performance Indicators". In: *Business process Design (BPD 2010)*, Hoboken, NJ, USA, Springer, LNBIP, Vol. 66, pp. 73-84 (September 2010)
- [119] Shamsaei, A., Amyot, D., and Pourshahid, A.: "A Systematic Review of Compliance Measurement Based on Goals and Indicators". In: *Governance, Risk and Compliance on Information Systems (GRCIS'11)*, London, UK, Springer, LNBIP, Vol. 83, pp. 228-236 (June 2011)
- [120] Shamsaei, A., Amyot, D., Pourshahid, A., Mussbacher, G., Tawhid, R., Yu, E., Braun, E., and Cartwright, N.: "An Approach to Specify and Analyze Goal Model Families". In: *7th System Analysis and Modelling (SAM)*, Innsbruck, Austria, LNCS. Springer (October 2012) (*to appear*)
- [121] Shamsaei, A.: "Indicator-based Policy Compliance of Business Processes". In: *CAiSE'11 Doctoral Consortium*, London, UK, CEUR-WS.org, Vol. 731 (June 2011)
- [122] Shamsaei, A.: "Business Process Compliance Tracking Using Key Performance Indicators". In: *CASCON 2010*, poster, Toronto, Canada (November 2010)
- [123] Silva, C., Borba, C., and Castro, J.: "A goal oriented approach to identify and configure feature models for software product lines". In: *14th Workshop on Requirements Engineering (WER'11)*, Rio de Janeiro, Brazil (April 2011)
- [124] Silveira, P., Rodriguez, C., Casati, F., Daniel, F., D'Andrea, V., Worledge, C., and Taheri, Z.: "On the design of Compliance Governance Dashboards for Effective Compliance and Audit Management". In: *ICSOC-ServiceWave 2009*, Stockholm, Sweden, Springer, LNCS, Vol. 5900, pp. 208-217 (November 2009)
- [125] SmartKPIs.com: *The smart choice in performance management*.
<http://www.smartkpis.com/key-performance-indicator-KPI> (accessed July 2011)
- [126] Schiff, J.: *Ten Benefits of Business Intelligence Software*, November 19, 2010.
http://www.ecrmguide.com/article.php/11222_3914061_1 (accessed January 2011)
- [127] Tawhid, R., Alhaj, M., Mussbacher, G., Braun, E., Cartwright, N., Shamsaei, A., Amyot, D., Behnam, S.A., and Richards, G., "Towards Outcome-Based Regulatory Compliance in Aviation Security". In: *20th IEEE Int. Requirements Engineering Conference (RE'12)*, Chicago USA. IEEE CS, pp. 267-272 (September 2012)
- [128] The Gramm-Leach-Bliley Act, <http://epic.org/privacy/globa/> (accessed October 2011)

- [129] The Sarbanes-Oxley Act: <http://www.soxlaw.com/> (accessed January 2011)
- [130] Thomson Reuters: *Cost of Compliance Survey 2011*, http://thomsonreuters.com/content/news_ideas/white_papers/legal/406377 (accessed July 2011)
- [131] Thorjman, Sh.: *What is Policy?*, Caledon Institute of Social Policy, September 2005. <http://www.caledoninst.org/Publications/PDF/544ENG.pdf> (accessed August 2011)
- [132] US Department of Health and Human Services: *HIPAA General Information*, <http://www.cms.hhs.gov/HIPAAGenInfo/> (accessed March 2011)
- [133] Van der Aalst, W.M.P., ter Hofstede, A.H.M., and Weske, M.: "Business Process Management: A Survey". In: *First International Conference on Business Process Management*, Eindhoven, Netherlands, Springer-Verlag Berlin Heidelberg, LNCS, Vol. 2678, pp. 1-12 (June 2003)
- [134] Vicente, P., and Mira de Silva, M. "A Conceptual Model for Integrated Governance, Risk and Compliance". In: *Advanced Information Systems Engineering, CAiSE 2011*, London, UK, Springer-Verlag Berlin Heidelberg, LNCS 6741, pp. 199-213 (June 2011)
- [135] Villar, C. *A Goal-Driven Methodology for Developing Health Care Quality Metrics*. M.Sc. thesis, E-Business Technologies, University of Ottawa, Canada (February 2011)
- [136] Weber, I., Governatori, G., and Hoffmann, J.: "Approximate compliance checking for annotated process models". In: *Governance, Risk and Compliance on Information systems (GRCIS'08)*, Montpellier, France, CEUR-WS.org, pp. 46-60 (June 2008)
- [137] Weiss, M., and Amyot, D.: "Business Process Modeling with URN". *International Journal of E-Business Research*, Vol. 1(3), pp. 63-90 (July-September 2005)
- [138] Whatis.com: *Business Intelligence*. <http://searchdatamanagement.techtarget.com/definition/business-intelligence> (accessed January 2011)
- [139] WHO EMRO. *Health Systems: Concepts, Design & Performance*. Glossary. Retrieved Dec. 2010, available at <http://www.emro.who.int/mei/mep/Healthsystemsglossary.htm> (accessed March 2011)
- [140] Yu, E.: "Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering". In: *3rd IEEE Int. Symp. On Requirements Engineering (RE'97)*, IEEE Computer Society, Washington, USA, IEEE CS, pp. 226-235 (January 1997)
- [141] Yu, Y., Leite, J.C.S.P., Lapouchnian, A., Mylopoulos, J.: "Configuring features with stakeholder goals". In: *Symp. on Applied Computing (SAC'08)*, ACM, pp. 645-649 (March 2008)
- [142] Zdun, U., Bener, A., and Olalia-Carin, E.L.: "Guest Editors' Introduction: Software Engineering for Compliance". *IEEE Software*, Vol. 29, No. 23, pp. 24-27 (May-June)

- [143] ZL Technologies Inc.: *Regulation Overview Sarbanes-Oxley Act (SOX)*
<http://www.zlti.com/content/docs/Rules%20and%20Regulations/ZL.RR.SOX.pdf>
(2008) (accessed August 2011)

Appendix A: Systematic Literature Review

Regarding the systematic literature review presented in Chapter 3, Table 46 to Table 51 list the unique papers returned by each search engine or conference when searched sequentially (i.e., redundant papers are not listed). Most of the table items are actual hyperlinks in the electronic version of this thesis.

Table 52 lists the papers retained for the literature review, with their authors and affiliations.

IEEE Explorer	
	Papers
1	Dealing with imprecise compliance requirements
2	Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act
3	An IT Governance Framework of ERP System Implementation
4	Software service engineering: Tenets and challenges
5	ISO/IEC/IEEE Systems and software engineering - Vocabulary
6	Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001
7	Enterprise Architecture Integration in E-Government
8	Towards Service Engineering: Service Orientation and Business-IT Alignment
9	Optimizing the Value of Green IT Projects within Organizations
10	Draft International Standard -- Systems and Software Engineering -- Vocabulary
11	Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001
12	IT audit in accordance with Cobit standard
13	SLA: A PBNM supported information model
14	Cycle time reduction in assembly and test manufacturing factories: A KPI driven methodology
15	IT and business process performance management: Case study of ITIL implementation in finance service industry
16	Toward an Integrated User Requirements Notation Framework and Tool for Business Process Management
17	Real Time Business Intelligence for the Adaptive Enterprise
18	Inside Agile Processes: A Practitioner's Perspective
20	Innovation in operational excellence in a complex environment
21	Electronics production and process controlling
22	The analysis and development of Taiwan's industrial logistics hubs
23	S3: A Service-Oriented Reference Architecture
24	Paper Titles and Abstracts
25	IEEE Guide for Developing User Organization Open System Environment (OSE) Profiles
26	Enterprise Architecture management in Virtual Organization
27	Using a model-driven transformational approach and service-oriented architecture for service delivery management

28	Sense-and-respond supply chain using model-driven techniques
29	Towards a Procedural Model for Sustainable Information Systems Management
30	The IT Organization Modeling and Assessment Tool: Correlating IT Governance Maturity with the Effect of IT
31	Enterprise Integration Performance Modeling and Measurement Based on Category Theory
32	Business process monitoring & measurement in a large bank: challenges and selected approaches
33	Managed Business Artifacts
34	Classifying ITIL Processes; A Taxonomy under Tool Support Aspects
35	Integrating IT Service Management within the Enterprise Architecture
36	A Unified Framework for Outsourcing Governance
37	Enhancing Service Network Analysis and Service Selection Using Requirements-Based Service Discovery
38	Catalog-based service request management
39	The combined adoption of production it and strategic initiatives - Initial considerations for a Lean MES analysis
40	A Novel SOA-Oriented Federate SLA Management Architecture
41	Case Study: Utilities and Asset Management - Time For a Change
42	Managing risk in software maintenance
43	Customer-focused service management for contact centers
44	The Internal Value of Mobile Computing in Emergency Medical Services: An Australian Case Study
45	A Policy-Based Metrics Framework for Information Security Performance Measurement

Table 46, Papers Selected from IEEE Explorer

Springer	
	Papers
1	Common Capabilities for Service Oriented Infrastructures – Grid and Cloud Computing
2	An Aspect-Oriented Framework for Business Process Improvement
3	Using Software Systems to Support Environmental Accounting Instruments
4	Decision-Enabled e-EPC
5	What's in a Service?
6	A reverse logistics diagnostic tool: the case of the consumer electronics industry
7	Goal-Driven Development of a Patient Surveillance Application for Improving Patient Safety
8	SharePoint Business Solutions
9	Background
10	Monitoring, Analyzing and Optimizing Corporate Performance — State of the Art and Current Trends
11	Value Chain Management
12	Artifact-Based Transformation of IBM Global Financing
13	Operations Support System for End-to-End QoS Reporting and SLA Violation Monitoring in Mobile Services Environment
14	Introduction
15	Designing a performance measurement system
16	Business process management with the user requirements notation
17	When Infrastructure Management Just Won't Do: The Trend Towards Organizational IT Service Management
18	Industrial Asset Maintenance and Sustainability Performance: Economical, Environmental, and Societal Implications
19	SCM in a Pharmaceutical Company
20	Process-Based Decision Support

21	Ecotopia: An Ecological Framework for Change Management in Distributed Systems
22	Industrialization of Application Implementations
23	IT Service Management
24	The Process of Enterprise Architecting
25	Management of Process Excellence: What is it and Why do you Need It?
26	The Scope of Supply Chain Management
27	Simultaneous trend analysis for evaluating outcomes in patient-centred health monitoring services
28	Operational risk management with real-time business intelligence
29	Service Engineering for the Internet of Services
30	Integrated Controlling Based on Material and Energy Flow Analysis — A Case Study in Foundry Industries
31	Roles and Responsibilities for BPM
32	A Phase-wise Development Approach to Business Excellence: Towards an Innovative, Stakeholder-oriented Assessment Tool for Organizational Excellence and CSR
33	An Auditing Process to Improve Asset Management Performance
34	Managing Sustainability Performance Measurement and Reporting in an Integrated Manner
35	Supply Chain Management Case Studies
36	Managing Change and Innovation in Government
37	Enterprise Organization and Operation
38	SharePoint Business Solutions
39	Process Based Enterprise Architecture Building
40	Maintenance Performance Measurement (MPM) System
41	The Business Perspective on Roles Including Root Causes of Implementation Problems and Proven Ways to Overcome them
42	IT Performance Management — Managing IT Holistically
43	Fundamentals of Sustainability Performance Evaluation System in Government
44	Towards an Integrated Performance Indicator for (Energy) Benchmarking Covenants with Industry

Table 47, Papers Selected from Springer

Google Scholar	
	Papers
1	A business process-based modeling extension for regulatory compliance
2	Componentization of Business Process Layer in the SOA Reference Architecture
3	Trust and Compliance Management Models in Emerging Outsourcing Environments
4	On the Design of Compliance Governance Dashboards for Effective Compliance and Audit Management
5	Dealing With Imprecise Compliance Requirements
6	Information Services Implementation of the Cobit framework at Curtin University of Technology Information Services
7	A Business Process-Based Modelling Extension for Regulatory Compliance
8	Preventing SLA Violations in Service Compositions Using Aspect-Based Fragment Substitution
9	Towards a Framework for Tracking Legal Compliance in Healthcare
10	A business process-based modeling extension for regulatory compliance
11	A Compliance Framework for Business Processes Based on URN
12	Towards an Architecture for Self-regulating Agents: A Case Study in International Trade
13	Componentization of Business Process Layer in the SOA Reference Architecture
14	On the Design of Compliance Governance Dashboards for Effective Compliance and Audit Management
15	Task-Based Entailment Constraints for Basic Workflow Patterns

16	Green business process management: A research agenda
17	Technologies of compliance: Risk and regulation in a digital age
18	Exploring the status quo of business process modeling languages in the banking sector – An empirical insight into the usage of methods in banks
19	Trust and Compliance Management Models in Emerging Outsourcing Environments
20	Service Compliance: Towards Electronic Compliance Programs
21	RiskM: A multi-perspective modeling method for IT risk assessment
22	Green business process management: A research agenda (re-publication draft)
23	Satisfaction of Control Objectives by Control Processes
24	The influence of buyer-seller relationship on E-commerce pressures: The case of the primary metal industry
25	Information Services Implementation of the Cobit framework at Curtin University of Technology Information Services
26	Australian Government Department of Defense
27	Bringing Agility to Business Process Management: Rules Deployment in an SOA
28	Business process integration: method and analysis

Table 48, Papers Selected from Google Scholar

ACM	
	Papers
1	An ontological knowledge framework for adaptive medical workflow
2	An evaluation of business solutions in manufacturing enterprises
3	Managing an increased service heterogeneity in a converged enterprise instructiveness with SOA
4	Basic software components for economic process modeling, simulation, analysis and optimization
5	Investigating knowledge management practices in software development organizations- An Australian experience
6	Model- driven eGovernment interoperability: A review of the art
7	Deriving industrial logistics hub reference models for manufacturing based economies
8	Using COBIT Indicators for Measuring Scrum-based Software Development
9	Assessing Scrum-based Software Development Process Measurement from COBIT Perspective
10	Service oriented architectures: approaches, technologies and research issues
11	Crossing the agent technology chasm: Lessons, experiences and challenges in commercial applications of agents
12	Software Service Engineering: Tenets and Challenges
13	Assessing the strategic value of Information Technology: An analysis on the insurance sector
14	An Algorithm for the Appraisal of Assurance Indicators for Complex Business Processes
15	Operational risk management with real-time business intelligence
16	Concern-oriented business architecture engineering
17	Green sigma and the technology of transformation for environmental stewardship
18	Software Architecture Definition for On-demand Cloud Provisioning
19	Investigating Knowledge Management practices in software development organizations – An Australian experience
20	Model-driven eGovernment interoperability: A review of the state of the art
21	Emerging issues in IT Governance: implementing the corporate IT risks management model
22	Method and systems for Entity Linking In Compliance Policy Monitoring
23	Towards a business process model warehouse framework
24	Event Detection Challenges, Methods, and Applications in Natural and Artificial Systems
25	A Formal Approach Enabling Risk-aware Business Process Modeling and Simulation
26	Process Trace Identification from Unstructured Execution Logs

27	Process gatekeepers and compliance with enterprise processes
28	Toward modeling constructs for audit risk assessment: Reflections on internal controls modeling
29	Aligning Risk Management and Compliance Considerations with Business Process Development
30	Technologies of Compliance: Risk and Regulation in a Digital Age
31	Emerging Challenges in Information Systems Research for Regulatory Compliance Management

Table 49, Papers Selected from ACM

iStar	
	Papers
1	Analyzing Knowledge Transfer in Software Maintenance Organizations using an Agent- and Goal-oriented Analysis Technique
2	Software Process Alignment with Organizational Business Strategies using an Agent- and Goal-oriented Analysis Technique
3	iStarML: An XML-based Model Interchange Format for i*
4	Multi-Agent Abstractions and Organizations and the i* Framework.
5	A Service-oriented Approach for the i* Framework
6	A Metrics Definition Framework for i*
7	AGFL - Agent Goals from Lexicon - Eliciting Multi-Agent Systems Intentionality
8	Fostering Investigation, Collaboration, and Evaluation: the i* Wiki Experience
9	Ontological Foundations for Agent-Oriented Organizational Modeling
10	Qualitative, Interactive, Backward Analysis of i* Models.
11	Continuous, Requirements-Driven Support for Organizations, Networks, and Communities
12	Exploring i* Characteristics that Support Software Transparency
13	On Using i* for Modeling Autonomy, Reasoning, and Planning in Adaptive Systems
14	From i* to an Integrated Requirements Knowledge Representation, to Requirements for Services
15	Extending i* to Fit with the Requirements World
16	Defining Inheritance in i* at the Level of SR Intentional Elements
17	Improving the Syntax and Semantics of Goal Modelling Languages
18	Applying the i* Framework to the Development of Data Warehouses
19	Tropos at the Age of Eight: On-going Research at FBK, UniTN and UT
20	Improving the Modularity of i* Models
21	From i* to OO-Method: Problems and Solutions
22	The Evolution of Tropos: Contexts, Commitments and Adaptivity
23	Definition and Uses of the i* Metamodel
24	Itemized Strategic Dependency: a Variant of the i* SD Model to Facilitate Knowledge Elicitation
25	From Business Services to Web Services: an MDA Approach
26	A bit of "Persona", a bit of "Goal", a bit of "Process" ... a recipe for Analyzing User Intensive Software Systems
27	Using Intentional Actor Modeling to Support the Evolution of Enterprise Software Architectures in Organizations
28	Bridging the Gap between Goals, Agents and Business Processes
29	A Framework for Iterative, Interactive Analysis of Agent-Goal Models in Early Requirements Engineering
30	Automated Generation of Attack Routes for Service Security Analysis - A Preliminary Report
31	On Temporally Annotating Goal Models
32	Using i* to Support a Summative Evaluation

33	On the use of the Goal-Oriented Paradigm for System Design and Law Compliance Reasoning
34	Using <i>i*</i> Meta Modeling for Verifying <i>i*</i> Models
35	Using <i>i*</i> and Tropos in a Software Engineering Contest: Lessons Learnt and Some Key Challenges
36	Requirements Engineering for Control Systems
37	<i>i*</i> on ADOxx®: A Case Study
38	Deriving Adaptive Behaviour from <i>i*</i> models
39	Exploring Risk-Awareness in <i>i*</i> models
40	From Adaptive Systems Design to Autonomous Agent Design
41	Strategy Representation Using an <i>i*</i> -like Notation
42	A Goal-Oriented Approach for Workflow Monitoring

Table 50, Papers Selected from iSTAR

GRCIS	
	Papers
1	Method Engineering for Integrated Enterprise Balancing
2	Towards Resolving Compliance Violations in Business Process Models
3	Conformance Analysis of ASML's Test Process
4	A Framework for Seamless and Compliant Service Consumption in Outsourcing Scenarios
5	Risk-Aware Organizational Design
6	Assessing Business and IT Projects on Compliance with Enterprise Architecture
7	Compliance Management in Multi-actors Contexts
8	The Role of a Culture of Compliance in Information Technology Governance
9	Towards a Framework for Semantic Business Process Compliance Management
10	A Method for Integrated Management of Process-risk
11	Compliance of Semantic Constraints – A Requirements Analysis for Process Management Systems
12	Approximate Compliance Checking for Annotated Process Models
13	Supervision and Discovery of Electronic Communications in the Financial Services Industry
14	Patterns for Understanding Control Requirements for Information Systems for Governance, Risk Management, and Compliance
15	Exploring Features of a Full-Coverage Integrated Solution for Business Process Compliance
16	A Systematic Review of Compliance Measurement Based on Goals and Indicators
17	Continuous Control Monitoring-Based Regulation: A Case in the Meat Processing Industry
18	Semantic Representation of Process and Service Compliance - A Case Study in Emergency Planning
19	A Framework for Organizational Compliance Management Tactics

Table 51, Papers Selected from GRCIS

Authors	Location	Region	Year
Ahmed Awad, Sergey Smirnov, and Mathias Weske	Hasso Plattner Institute at the University of Potsdam	Germany	2009
Saeed Ahmadi Behnam, Daniel Amyot, Alan J. Forster, Liam Peyton, and Azalia Shamsaei	SITE, University of Ottawa, 800 King Edward Ave 2 Department of Medicine, University of Ottawa and OHRI	Canada Canada	2009
Wolfgang BOEHMER	Technische Universität Darmstadt,	Germany	2009
Jiangbo Dang *, Amir Hedayati, Ken Hampel, Candemir Toklu	Knowledge Management, Siemens Corporate Research	USA	2007
Sepideh Ghanavati, Daniel Amyot, and Liam Peyton	SITE, University of Ottawa, 800 King Edward Ave	Canada	2007
Sepideh Ghanavati	SITE, University of Ottawa, 800 King Edward Ave	Canada	2007

Dimitris Karagiannis John Mylopoulos Margit Schwab	University of Vienna University of Toronto BOC Information Technologies Consulting Ltd.	Austria Canada	2007
Dimitris Karagiannis	University of Vienna	Austria	2008
Marwane El Kharbili, Sebastian Stein	IDS Scheer AG, ARIS Research. Altenkes- seler Str.	Germany	2008
Marwane El Kharbili, Sebastian Stein, Ivan Markovic, Elke Pulvermüller	IDS Scheer AG, ARIS Research	Germany	2008
GEORGE KOLIADIS, ADITYA K. GHOSE	Decision Systems Lab, University of Wollon- gong	Australia	2008
Linh Thao Ly, Kevin Göser, Stefanie Rinderle- Ma, and Peter Dadam	Institute of Databases and Information Sys- tems, University of Ulm,	Germany	2008
Ruopeng Lu, Shazia Sadiq, Guido Governatori	The University of Queensland, Brisbane,	Australia	2009
VILJAN MAHNIC, NATASA ZABKAR	University of Ljubljana	Slovenia	2008
VILJAN MAHNIC, NATASA ZABKAR	University of Ljubljana	Slovenia	2008
Daniela Marino, Fabio Massacci, Andrea Miche- letti, Nataliya Rassadko, and Stephan Neuhaus	San Raffaele Hospital University of Trento	Italy	2009
Fabio Massacci Artsiom Yautsiukhin	University of Trento	Italy	2007
Clemens Martin, Mustapha Refai	University of Ontario Institute of Technology	Canada	2007
Alicia Martinez, Nimrod Gonzalez, Hugo Estrada	National Center for Research and Technologi- cal Development	Mexico	2010
Mirko Morandini, Luca Sabatucci, Alberto Siena, John Mylopoulos, Loris Penserini, Anna Perini, and Angelo Susi	Fondazione Bruno Kessler - IRST University of Trento	Italy	2010
Evan Morrison, Aditya Ghose, George Koliadis	Decision Systems Laboratory, University of Wollongong	Australia	2009
Kioumars Namiri, Nenad Stojanovic	SAP Research Center CEC Karlsruhe, SAP AG,	Germany	2008
Anil Nigam, Jun-Jang Jeng, Tian Chao, Henry Chang	IBM T.J. Watson Research Center	USA	2008
Aljosa Pasic, Juan Bareño, Beatriz Gallego- Nicasio, Rubén Torres, and Daniel Fernandez	Atos Research & Innovation	Spain	2010
Alireza Pourshahid, Gunter Mussbacher, Daniel Amyot, Michael Weiss	University of Ottawa Carleton University	Canada Canada	2009
Alireza Pourshahid, Daniel Amyo, Liam Peyton, Sepideh Ghanavati, Pengfei Chen, Michael Weiss, Alan J Forster	University of Ottawa Department of Medicine, University of Otta- wa and OHRI	Canada Canada	2009
Dalibor Radovanovi, Tijana Radojevi, Dubravka Lui, Marko Šarac	Singidunum University	Serbia	2010
André Rifaut and Eric Dubois	Public Research Centre Henri Tudor	Luxem- bourg	2008
Carlos Rodríguez, Patrícia Silveira, Florian Dan- iel, Fabio Casati	University of Trento	Italy	2010
Shazia Sadiq, Guido Governatori, Kioumars Naimiri	University of Queensland SAP Research Centre	Australia Germany	2007
Patrícia Silveira, Carlos Rodríguez, Fabio Casati, Florian Daniel, Vincenzo D'Andrea	University of Trento	Italy	2010
Ingo Weber, Guido Governatori, and Jörg Hoff- mann	SAP Research The University of Queensland	Germany Australia	2008
Kerstin Gerke, Jorge Cardoso, and Alexander Claus	SAP AG, SAP Research, CEC Dresden	Germany	2009
Jörg Becker, Philipp Bergener, Patrick Delfmann	University of Muenster	Germany	2011
Ceistina Cabanillas, Manuel Resinas, and Antonio Ruiz-Cortes	Universite de Sevilla	Spain	2011
Ralph Foorthuis and Rik Bos	Utrecht University	Netherland	2011
Popova, V., and Sharpanskykh	De Montfort University Vrije Universiteit Amsterdam	UK Netherland	2011
Pedro Vicente and Miguel Mira da Silva	Universidade Tecnico de Lisboa	Portugal	2011

Table 52, Selected Papers' Locations, Regions and Years

Appendix B: Human Resource Policy

The following detailed policy [54] is used as an example for the framework in Chapter 5.

Hiring Policy

Policy Intent

(Company Name) practices equal opportunity, and fair hiring processes when filling positions, and hires only the most qualified individuals to ensure the success of our business. (Company Name) has adopted this policy to ensure that all employees and potential candidates are considered for employment opportunities in a fair and consistent manner.

This Policy Shall:

1. Provide guidelines for personnel requests;
2. Detail procedures for all job postings;
3. Describe the application process for potential candidates;
4. Outline the interview process;
5. Discuss employee eligibility for internal transfers;
6. Summarize the process for background checks and references;
7. Supply procedures for offers of employment;
8. Present resolutions for conflict in the hiring process.

Personnel Requests

(Company Name) requires that all requests for new or additional personnel be directed in writing to the (Company Name) division head, and Human Resources for approval. Personnel requests shall include the position title, essential job functions, necessary qualifications, reasons for the opening, and the hours/shifts required.

Job Postings

Internal:

- (Company Name) requires that all new postings of employment be circulated internally on the company message board and through Human Resources for a period of one week before being made public.

- Qualified applicants under the employ of (Company Name) shall remain subject to the normal hiring processes, including interviews, etc.

External:

- External job postings shall be based on necessity and budget requirements.
- Human resources shall be responsible for the placement of all recruitment advertisements.

Application Process

- (Company Name) requires that all applicants complete an application for the consideration of employment.
- Applicants must also submit a resume and letters of reference.
- (Company Name) will review all properly completed applications, and interview the most qualified candidates.
- Candidates that for any reason do not meet the requirements for employment shall remain classified as applicants and may re-apply once each month for reconsideration.

Interviews

- Interview questions shall be compiled and reviewed by Human Resources to ensure their efficacy.
- Upon completion of all scheduled interviews, the results shall be reviewed by the hiring manager.
- Human Resources must be notified of all interviews conducted.
- Applications and resumes of applicants that were not selected for employment shall be forwarded to Human Resources to ensure the appropriate retention of information.
- Human Resources shall notify applicants not selected for employment regarding the closure of the position.

Internal Transfers

- Employees are encouraged to apply for internal job openings, and will have their applications considered on the basis of their qualifications and potential for success at the position.
- Employees applying for internal job postings must first obtain the consent of their department manager.
- Internal applicants who are not selected for the position shall be notified by Human Resources.
- In the event that an employee is selected for employment pertaining to an internal job posting, following their transfer to the new position they will begin a new probationary period.

References and Background Checks

- The hiring manager and Human Resources shall conduct reference and background checks on all potential candidates for employment at (Company Name).
- Background checks are designed to protect the safety of our employees by minimizing the hiring of potentially dangerous individuals with violent criminal backgrounds.
- References shall be checked to ensure a candidate's qualification for the position.

Offer of Employment

- (Company Name) shall give a conditional offer of employment to applicants that have been selected through the application and interview process.
- Job offers shall be contingent on the applicant's agreement to company policies, successful reference and background checks, the ability to pass a drug test, and any other condition applicable to the position that are required of the employee.
- Should the applicant accept an offer of employment from (Company Name), he/she will be considered an employee, and provided with a start date and required location to report for duty. Employee orientation shall be provided, and will include workplace policies, rules and regulations, and other job specific information designed to assist the employee in his/her duties. Authorization forms and policies shall be signed during this period of orientation.

Potential Hiring Conflicts

Family Members:

- (Company Name) shall accept applications from, and consider a member of an employee's immediate family for employment if the candidate has all the requisite qualifications.
- An immediate family member shall not be considered for employment if by doing so, it might create a direct or indirect managerial/subordinate relationship with the family member, or if his/her employment could create a conflict of interest either real or imagined.
- For the purposes of this policy, immediate family members shall be defined as: Wife, Husband, Mother, Father, Brother, Sister, Son, Daughter, or any In-Laws.

Employee Relationships:

- Employees engaging in romantic relationships and employees that become married or live in the same household may continue their employment with (Company Name) provided that there is neither a direct or indirect managerial/subordinate relationship between the employees, or a conflict of interest, real or imagined, created as a result of the relationship.
- In the event that either a managerial/subordinate, or conflict of interest issue arise, (Company Name) will work with the employees to accommodate them in a reasonable fashion. Possible resolution may require one of the employees to transfer to another position within the company. If this is not possible, one of the employees must resign.

Former Employees:

- A former employee that left (Company Name) on amicable terms may be eligible for reemployment.
- Former employees that left (Company Name) without proper notice, or whose employment was terminated for disciplinary reasons, shall not be eligible for reemployment.

Acknowledgment and Agreement

I, (Employee Name), acknowledge that I have read and understand the Fair Hiring Policy of (company name). I agree to adhere to this policy and will ensure that employees working under my direction adhere to this Policy. I understand that if I violate the rules set forth by this Policy, I may face legal, punitive, or corrective action.

Name: _____

Signature: _____

Date: _____

Witness: _____

Appendix C: URN Measured Compliance OCL Rules

This appendix formalizes in OCL the well-formedness rules of the URN measured compliance profile discussed in section 7.3. These constraints are available in the jUCMNav tool and make use of jUCMNav's library of predefined OCL functions. Note that Rule7 is meant to be checked on a model where a GRL strategy is evaluated.

Rule 1: Contributions to an intentional element must not sum up to a value higher than 100 (Reason: ensures that *all* contributing elements must evaluate to 100 for this intentional element to be fully satisfied).

```
context grl::IntentionalElement
inv GRLincomingContributionsNotMoreThan100:
    self.linksDest
    -> select(link | link.oclIsTypeOf(grl::Contribution))
    -> collect(link | link.oclAsType(grl::Contribution))
        .quantitativeContribution
    -> sum() <= 100
```

Rule 2: A GRL resource with a ST_CONDITIONTYPE metadata must be a dependee of an intentional element (Reason: ensures that conditions are used as specified by the measured compliance profile). Note: the jUCMNav metamodel uses the term Ressource rather than Resource.

```
context grl::IntentionalElement
inv GRLconditionDependeeOfIE:
    (self.type=IntentionalElementType::Ressource and
     self.hasMetadata('ST_CONDITIONTYPE'))
    implies
    self.linksSrc
    -> select(link | link.oclIsTypeOf(grl::Dependency))
    -> collect(link | link.oclAsType(grl::Dependency)).dest
    -> select(le | le.oclIsTypeOf(grl::IntentionalElement))
    -> size() > 0
```

Rule 3: Goals should have a hyperlink (violations shown as warnings only) (Reason: ensures that the source legislative documents are accessible from the GRL model). Note: this does not ensure that the specified hyperlink is valid.

```
context grl::IntentionalElement
inv GRLgoalsWithHyperlinks:
    self.type=IntentionalElementType::Goal
    implies
    self.hasMetadata('hyperlink')
```

Rule 4: ST_CLASSTYPE stereotypes cannot be used on actors (Reason: ensures that this stereotype is used as specified by the measured compliance profile).

```
context grl::Actor
inv GRLactorNoCLASSTYPE:
    not(self.hasMetadata('ST_CLASSTYPE'))
```

Rule 5: A GRL resource with a ST_CONDITIONTYPE stereotype cannot depend on anything else (Reason: ensures that conditions are used as specified by the measured compliance profile).

```
context grl::IntentionalElement
inv GRLconditionNotADepender:
    (self.type=IntentionalElementType::Ressource and
     self.hasMetadata('ST_CONDITIONTYPE'))
    implies
    self.linksDest
        -> select(link | link.oclIsTypeOf(grl::Dependency))
        -> isEmpty()
```

Rule 6: Functions as a query: finds goals where the reference metadata equals RuleName (shown as warnings only). Note: RuleName is a parameter here and can be substituted with any name. (Reason: ensures that the GRL model can be queried for elements traceable from a specific part of a legislative document as specified by RuleName)

```
context grl::IntentionalElementRef
inv GRLqueryRegDocRefName:
    not(getDef().getMetadata('RegDocRef') = 'RuleName'
        and
        getDef().type=IntentionalElementType::Goal)
```

Rule 7: Non-compliance: goal evaluated below the -25 threshold (violations shown as warnings only). Note: the -25 value is a default threshold but could be set to a different value by the analyst. (Reason: this constraint highlights regulation goals against which the organization performs poorly)

```
context grl::IntentionalElementRef
inv GRLregulationGoalNotSatisfied:
    getDef().type=IntentionalElementType::Goal
    implies
    getDef().getNumEval() > -25
```

Rule 8: ST_CONDITIONTYPE stereotypes can only be used on resources (Reason: ensures that stereotypes are used as specified by the measured compliance profile).

```
context grl::IntentionalElement
inv GRLresourceOnlyHasCONDITIONTYPE:
    not((self.type=IntentionalElementType::Ressource))
    implies
    not(self.hasMetadata('ST_CONDITIONTYPE'))
```

Rule 9: ST_CLASSTYPE stereotypes cannot be used on resources (Reason: ensures that stereotypes are used as specified by the measured compliance profile).

```
context gr1::IntentionalElement
inv GRLresourceNoCLASSTYPE:
    (self.type=IntentionalElementType::Ressource)
    implies
    not(self.hasMetadata('ST_CLASSTYPE'))
```

Rule 10: Goals should have a reference to the source legislative document (violations shown as warnings only) (Reason: ensures that there is a name that can be queried by Constraint 9). Note: this does not ensure that the specified name is valid.

```
context gr1::IntentionalElement
inv GRLgoalsWithReferences:
    self.type=IntentionalElementType::Goal
    implies
    self.hasMetadata('RegDocRef')
```

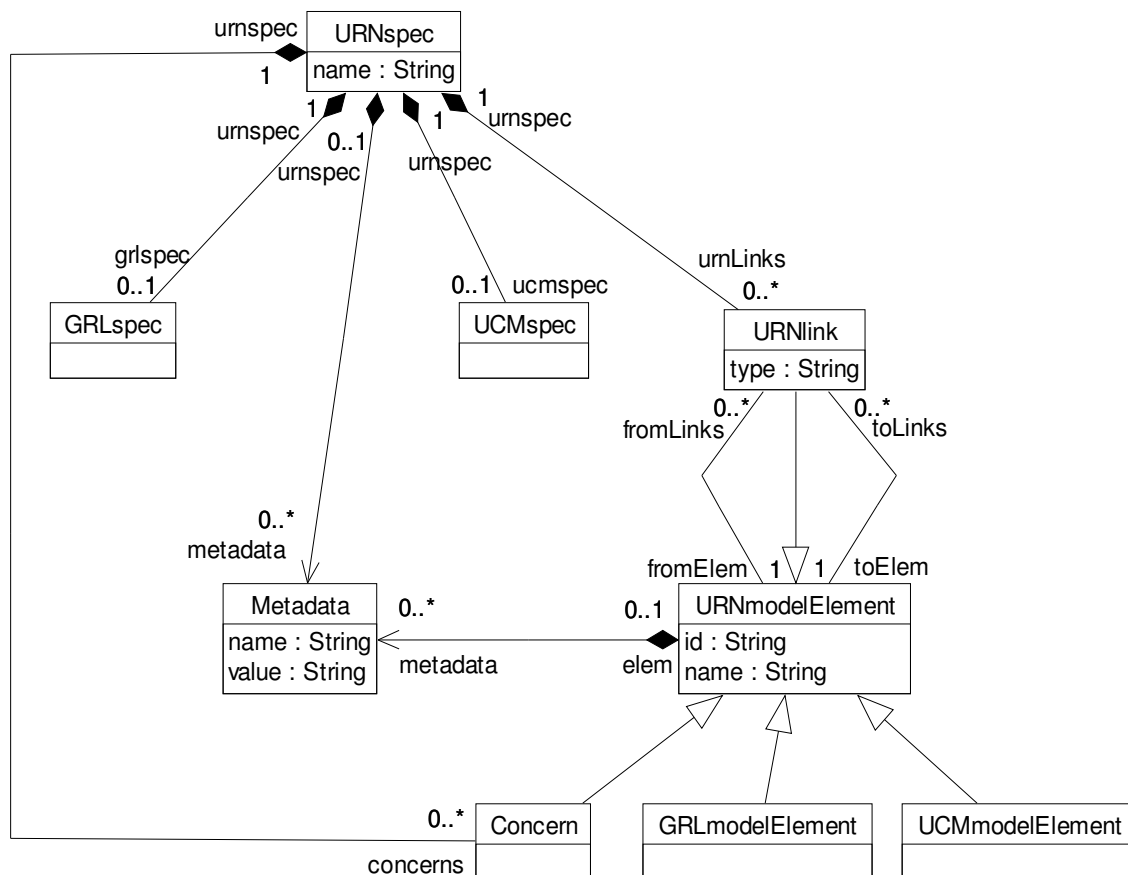



Figure 115, URN Specification, Links, Metadata and Model Elements [57]

Figure 116 illustrates the GRL specification, which serves as a container for various kinds of GRL model elements.

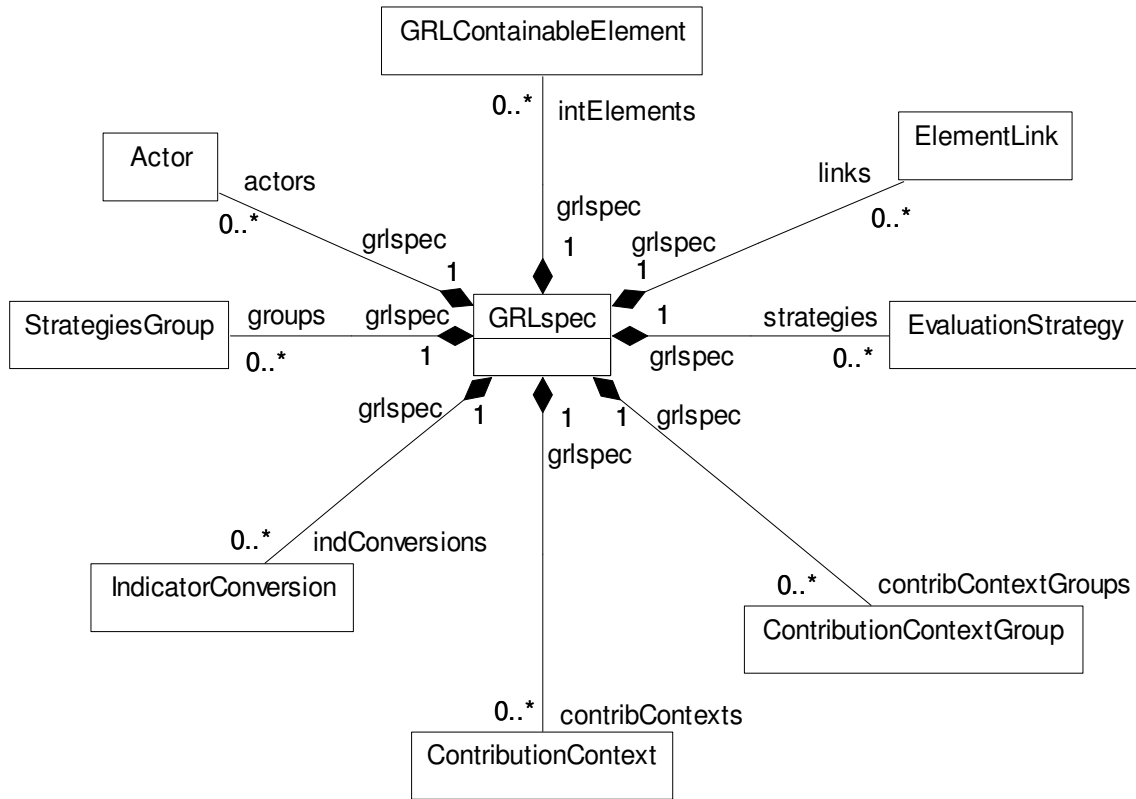


Figure 116, GRL Specification [57]

Figure 117 illustrates GRLmodelElement, which is a URN model element specialized for GRL concepts. Indicators are also shown as well.

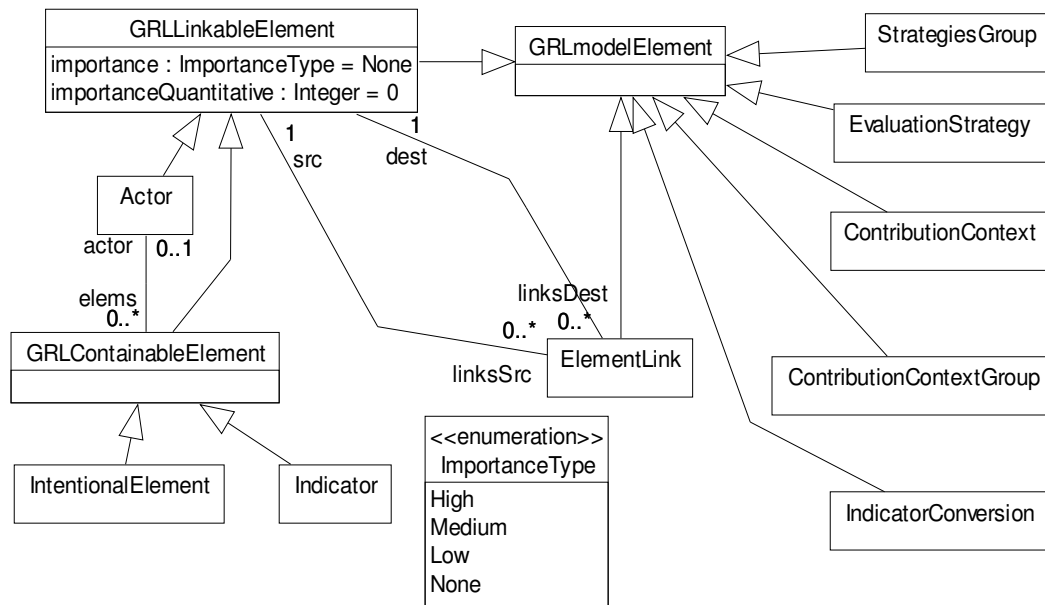


Figure 117, GRL Model, Linkable, and Containable elements [57]

Figure 118, illustrates the metaclasses for GRL actors, intentional elements, and their links.

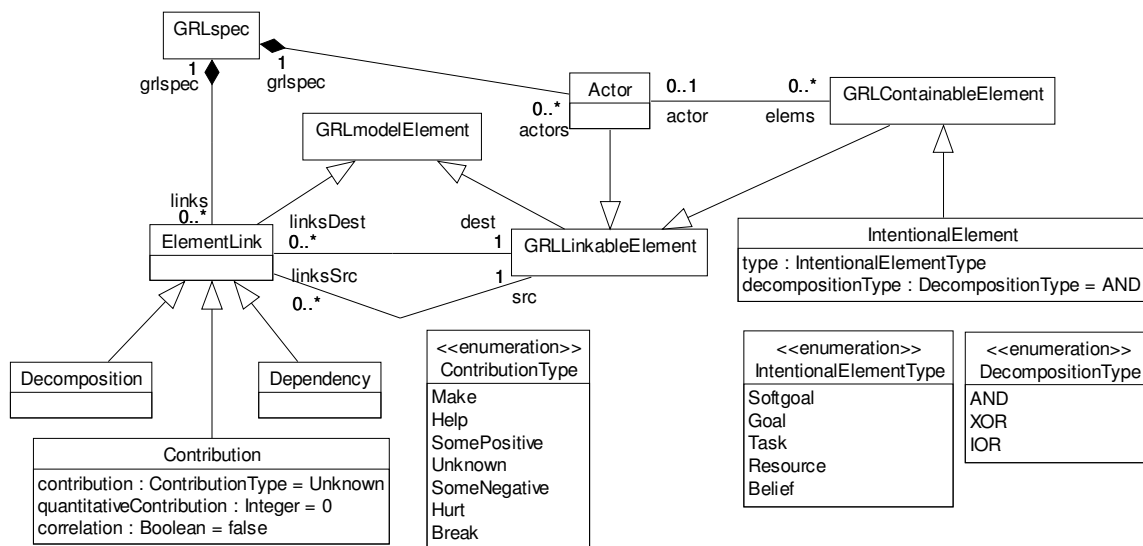


Figure 118, GRL Actors, Intentional elements, and Links [57]