Towards a Reference Model for Integrated Governance, Risk and Compliance

Pedro Vicente[1], Nicolas Racz[2] and Miguel Mira da Silva[1]

[1] Instituto Superior Técnico, Universidade Técnica de Lisboa,
Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
{pedro.vicente,mms}@ist.utl.pt
[2] TU Vienna, Institute for Software Technology and Interactive Systems,
Favoritenstr. 9-11, 1040, Vienna, Austria
racz@ifs.tuwien.ac.at

Abstract. More regulations are on the way, along with demanding transparency, accurate information about company operations, robust and comprehensive risk management, regulatory compliance and efficient governance. Consequently, organizations are seeking to improve their GRC activities, by implementing integrated GRC solutions that provide a holistic view of the organization and help in the automation of activities. After analysing and researching the emerging domain of integrated GRC, the lack of references that provide guidance to organizations in the implementation and optimization of processes, activities and information is an alarming issue.
In this paper we propose a reference model for GRC, combining two architectural layers - Business and Information Systems - modelled with ArchiMate. The reference model is presented and described through several viewpoints. We then apply a framework to evaluate the quality of the reference model and discuss the obtained results.

Keywords: GRC, reference model, integrated, archimate, information systems architecture

1 Introduction

The myriad of activities, processes and behaviours that lay on the Governance, Risk and Compliance (GRC) domain can be overwhelming. Although each area is well defined separately, the integration of the three areas is known to be a major challenge, since they became truly complex [1]. Traditional siloed GRC activities reinforced decreasing transparency, and hence governance agility, impacting effectiveness of decision making [2].

To better address GRC requirements such as internal policies, external regulations and risks, a holistic view of the organizations is needed to enhance efficiency and effectiveness. This view can be accomplished by integrating certain processes and activities that are common across the GRC functions, such as risk assessments, or functions that work better together, such as agreeing on the most significant risks or compiling one consensus list of the most critical open issues across the GRC units. Also, by better sharing knowledge, data and technology, a collaborative culture in organizations is enhanced. The ultimate goal is to identify, integrate and optimize processes and activities that are common across the GRC domain.

Vendors and organizations all agree on the paramount importance of GRC activities and the significance of taking an integrated and holistic view of these activities, not only from an internal perspective, but also from an outward perspective. However, asking organizations to define or describe governance, risk and compliance, is getting very distinct definitions [3, 4]. There are probably as many definitions of GRC as there are companies that provide technology or professional services to address GRC challenges [5].

The absence of references for integrated GRC is alarming. A study performed by Racz *et al.* showed that vendors' perceptions of GRC functionalities are diverse and present a low degree of congruence [6]. This study also showed that the scope of the existing market research GRC frameworks (AMR, Forrester and Gartner) varies enormously. Additionally, technology architectures differ in their degree of integration. Nonetheless, vendors and organizations strongly agree on the benefits delivered through integrated GRC suites.

Disagreements and inconsistencies between vendors and organizations are not positive, but it is not an abnormal circumstance. The more alarming issue is the absence of scientific research on GRC as an integrated concept, in a market that is controlled by vendors, analysts and consultancies [7]. Thus, the incongruence in this domain increased considerably and organizations may not be taking full advantage of integrated GRC systems. Much of the problem about GRC is a lack of standardized guidance [4]. A complete reference for the GRC domain is missing; mainly, the need for a reference, non-market-driven, is paramount to make progress in this domain.

To address this set of problems, the ultimate goal of our research is to develop a reference model for integrated GRC, representing an architecture with a main focus on the context of Information Systems and aligned with processes. In this paper we present part of our research, focusing on the information systems architectural layer.

A reference architecture can be seen as a specialization of a reference model. "A reference model is a generic abstract representation for understanding the entities and their significant relationships" in a defined domain; it defines "a common basis for understanding and explaining (at least at a high level of abstraction) the different manifestations of the paradigm" [8]. In this specific case, a reference architecture can help organizations develop and optimise their information management systems that may be more suitable than standard GRC solutions [9]. In order to facilitate this understanding, we use an independent and well-accepted modelling language - ArchiMate - to represent the architecture.

Architecture is positioned between business and IT [10], and in the GRC domain the gap between business and IT is a major concern since vendors are very focused on standard technological solutions and business knowledge is fragmented and inconsistent [3,4]. Having said this, a complete architecture definition is paramount to align and serve both business and IT.

2 Research Methodology

During this research we used the Design Science Research (DSR) methodology, based on a continuous build and evaluate cycle. Our research began with the analysis and selection of GRC artefacts present in the knowledge base of the domain (Fig. 1). We opted for scientific research that addressed GRC as an integrated topic. The chosen reference was a business process viewpoint, based on several valid reasons. First, the viewpoint is based on the combination of two models that address integrated GRC (a process model [11] and a conceptual model [12]. Additionally, the viewpoint was designed using the ArchiMate modelling language - that we have chosen to use in this paper. Moreover, a business process viewpoint is a central piece in the business layer, and can be very useful to develop the subsequent layer (information systems architecture). Finally, the design "by reuse" is a well accepted practice in DSR consisting in adapting and/or extending them to create one or more artefacts [13].

Figure 1 represents the stages conducted throughout this research.

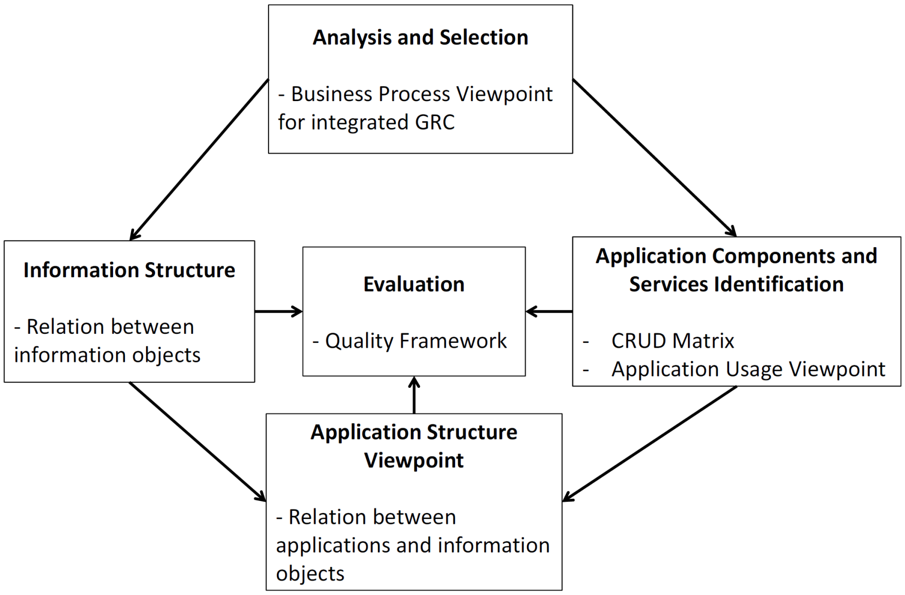

Analysis and Selection
- Business Process Viewpoint for integrated GRC
Information Structure
- Relation between information objects
Evaluation
- Quality Framework
Application Components and Services Identification
- CRUD Matrix
- Application Usage Viewpoint
Application Structure Viewpoint
- Relation between applications and information objects

Fig. 1. Research Methodology

The information objects from the business viewpoint were separated from the processes in order to construct an information structure. Using information objects and processes, application components were identified. Additionally, the application services realized by these components and used by the processes were identified. We also mapped the relations between application components through sharing of information and services. Finally, we evaluated all the viewpoints (or artefacts) using the data model quality framework from Moody and Shanks [14].

3 Theoretical Background

3.1 ArchiMate

A high-level modelling language is needed to describe the architecture. ArchiMate represents a standard language and vendor-independent concepts [15]. The architectural layers used in this paper are the business and application layers.

The selected concepts from ArchiMate are present in Fig. 2. We also highlighted the viewpoints described in this research. Viewpoints define abstractions on the set of models representing the enterprise architecture, each aimed at particular set of concerns [16]. We will use viewpoints to represent the concepts in isolation, and for relating two or more concepts.

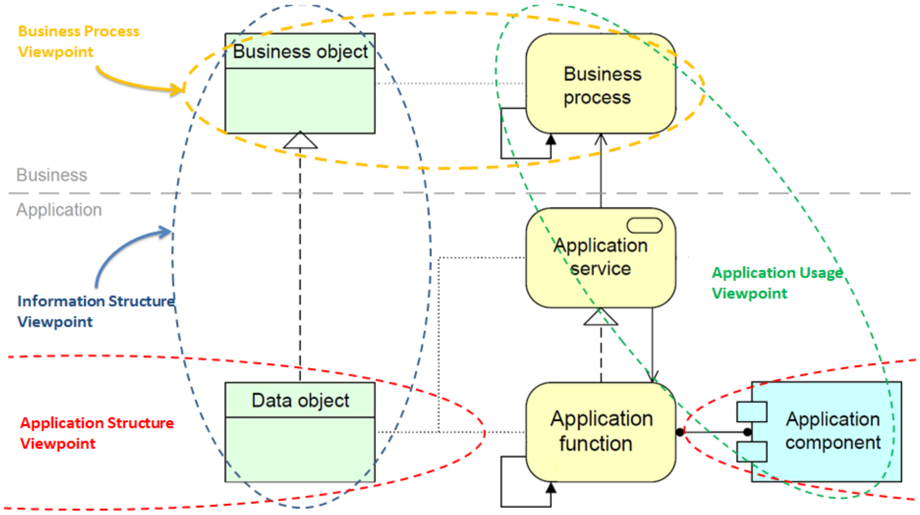


Fig. 2. Selected concepts and viewpoint examples from ArchiMate [16]

Each concept has its meaning. Business processes describe the internal behaviour that is required to achieve certain objectives. A business object is defined as a unit of information that has relevance from a business perspective. A data object is defined as a coherent, self-contained piece of information suitable for automated processing. An application service is defined as an externally visible unit of functionality. An application component is defined as a modular, deployable, and replaceable part of a system. It performs one or more application functions.

4 Reference Model

In this Section we present our proposed reference model that encompasses concepts from both business and information systems architecture.

Following the selected viewpoints presented in the previous Section we will start by using and complementing the business process viewpoint [17], followed by the information structure, application usage and application structure viewpoints.

4.1 Business Process Viewpoint

The business process viewpoint is used to show the relations of one or more business processes with each other and/or their surroundings. In this case it is used to create a high-level design of business processes within their context and to describe the use of shared information [16].

A business process viewpoint [17] (see Fig. 3) has already been developed through the combination of two models from the knowledge base of this domain: a conceptual model for GRC [12] and a process model for ITGRC [11]. Although the viewpoint was developed for a particular domain of GRC - ITGRC - it is applicable for the overall enterprise GRC. A point in favour lies with the fact that the viewpoint is already modelled using the ArchiMate structure.

However, the viewpoint presented in Fig. 3 was modified and some business objects were added and removed. The Reporting process was extended through the three macro processes of governance, risk and compliance.

This viewpoint is crucial for the development of the remaining viewpoints. It presents an important baseline for defining business objects and the necessary applications to support the processes.

4.2 Information Structure Viewpoint

The information structure viewpoint is identical to the traditional information models created in the development of almost any information system. It shows the structure of the information used in the enterprise or in a specific business process or application [16]. This viewpoint aggregates concepts from both the business and application layer.

Given the abstraction chosen for this research there is no practical distinction between data and business objects. The objects presented in Fig. 4 represent

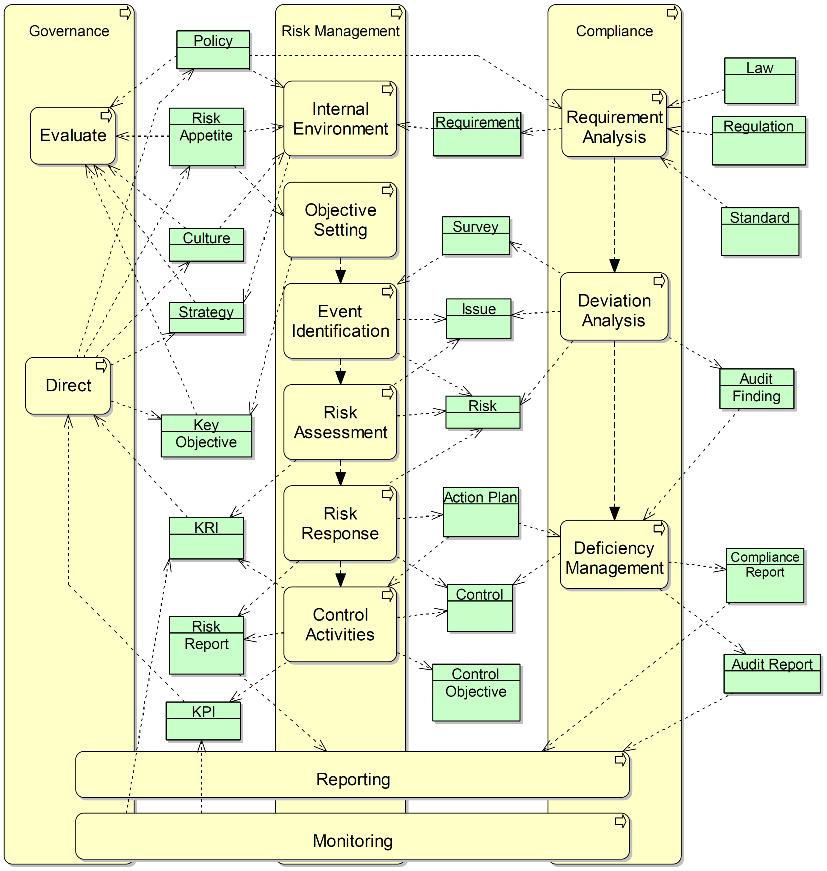


Fig. 3. Integrated GRC - Business Process Viewpoint adapted from [17]

business objects that can be seen as information entities or concepts that are necessary to support the business.

A description of the viewpoint follows; Policies may encompass a wide range of aspects of an organization. Internal policies reflect key objectives, strategy, risk appetite, culture, etc. of an organization. External policies are linked with external requirements - regulations, laws or standards. While policies define the *what*, procedures define the *how* and *who* will implement the policy. Policies and procedures are, in a certain extent, controls established to ensure the fulfilment of requirements and achievement of strategic objectives [18]. To each control, control objectives are defined and embedded in business processes. Usually controls are established to mitigate risks that menace the achievement of objectives or affect the normal function of business processes [18]. To business processes and risks, key performance and key risk indicators are developed to measure the

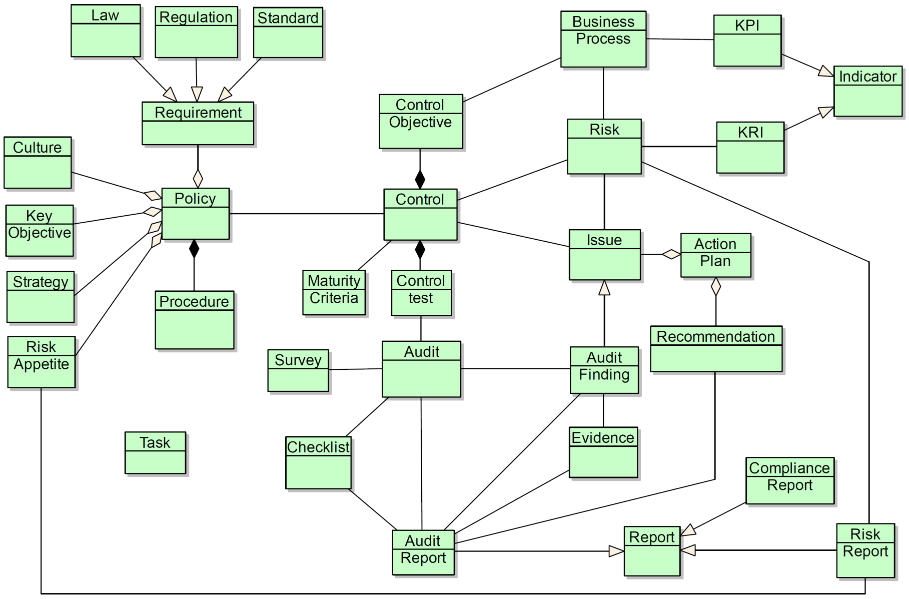


Fig. 4. Information Structure Viewpoint

performance of processes and the risk levels of certain activities. Risk reports are produced regularly and presented to the board.

Maturity criteria may be defined to measure the maturity level of controls. Normally auditors classify controls using this pre-defined criteria (e.g. COBIT maturity model, pass/fail criteria, etc.). Additionally, control tests may be specified to increase efficiency in controls assessments. During the execution of audits, audit findings are produced (a specific type of issues), along with evidences that prove it. Surveys and checklists are also associated with audits. For each audit, audit reports are produced, and include all the identified inconsistencies and the associated recommendation.

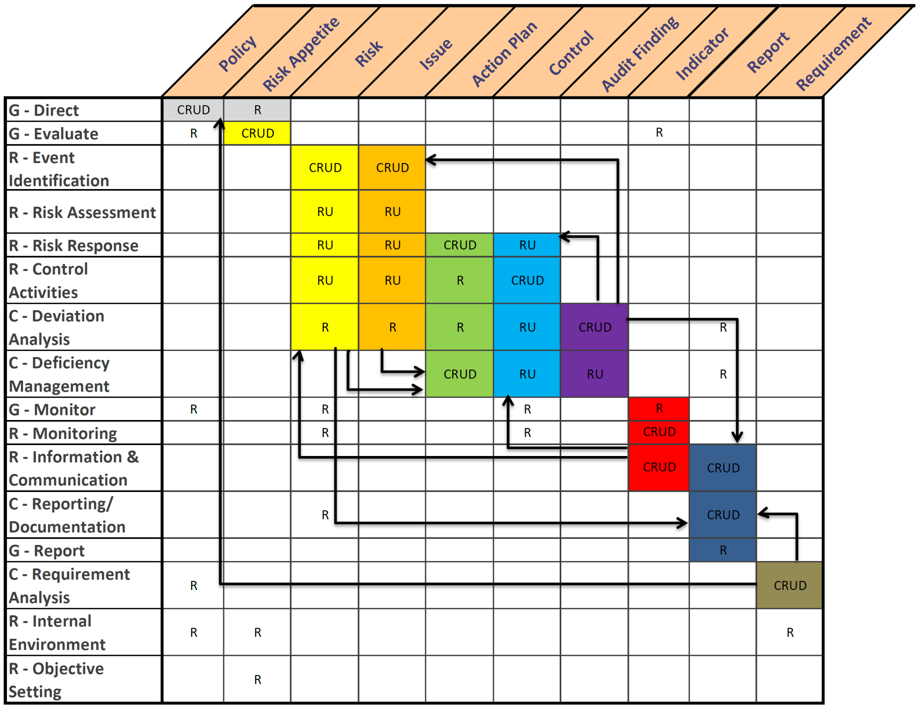
4.3 Application Usage Viewpoint

The application usage viewpoint describes how applications are used to support one or more business processes. It can be used in designing an application by identifying the services needed by business processes [16]. This viewpoint also presents itself as the connection between the business and information systems architectural layers. To establish this connection some other concepts need to be defined - application services and components.

In order to define consistently the necessary applications to support the processes, we present a CRUD (Create Read Update Delete) matrix (see Fig. 5) that relates processes (or actions) with informational entities described below.

CRUD Matrix This matrix was built in order to identify clusters that represent application solutions. The relation between processes and information entities provides a more structured approach to the identification of application components and services needed to support the processes.

We opted not to include all information entities in order to simplify the matrix. For example, the entity Report represents all type of reports - audit, risk and compliance. Additionally, the entity Requirement aggregates the entities Law, Standard and Regulation. The same applies to the Policy entity.



	Policy	Risk Appetite	Risk	Issue	Action Plan	Control	Audit Finding	Indicator	Report	Requirement
G - Direct	CRUD	R								
G - Evaluate	R	CRUD						R		
R - Event Identification			CRUD	CRUD						
R - Risk Assessment			RU	RU						
R - Risk Response			RU	RU	CRUD	RU				
R - Control Activities			RU	RU	R	CRUD				
C - Deviation Analysis			R	R	R	RU	CRUD		R	
C - Deficiency Management					CRUD	RU	RU		R	
G - Monitor	R		R			R		R		
R - Monitoring			R			R		CRUD		
R - Information & Communication								CRUD	CRUD	
C - Reporting/ Documentation			R						CRUD	
G - Report									R	
C - Requirement Analysis	R									CRUD
R - Internal Environment	R	R								R
R - Objective Setting		R								

Fig. 5. CRUD Matrix

⬜	Policy Management	🟪	Audit Management
🟨	Risk Management	🟥	Monitoring
🟧	Issue Management	🟦	Reporting & DashBoarding
🟩	Workflow Management	🟫	Compliance Management
🟦	Controls Management		

Fig. 6. Application Components

Through the analysis of the obtained clusters (see Fig. 5) some optimization could be suggested by integrating some systems. For example, issue and risk management are very similar, but they manage information entities that are, by definition, distinct, so we opted to maintain both. The integration between applications was explicitly represented in the form of arrows.

The matrix also came to support the expansion of both reporting and monitoring processes across Governance, Risk and Compliance proposed in Fig. 3, because the processes manage the same information.

In Fig. 6 the proposed application components are listed. Some applications match some references [6, 12].

With all the necessary components defined, the application usage viewpoint can be described. In this viewpoint (see Fig. 7) we chose to maintain the original processes, i.e. not expanding the monitor and report processes through the governance, risk and compliance processes, in order to simplify the viewpoint.

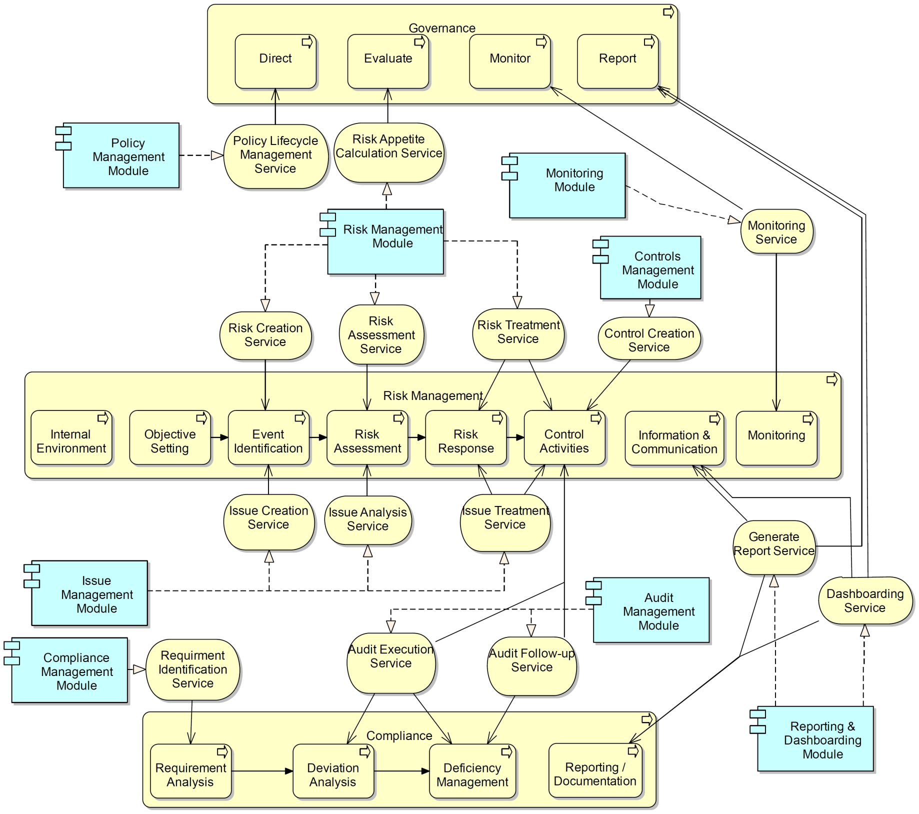


Fig. 7. Application Usage Viewpoint

According to the ISO/IEC38500 [19], the Direct process is based on the assignment of responsibilities, direct preparation and implementations of policies. In order to support this process, a Policy Life Cycle Service should be defined to support all actions needed to manage policies across the organization.

On the other hand, the Evaluate process is based on the current and future organizational objectives, thus the service provided by the risk management application - Risk appetite calculation service - is an important method to evaluate the readiness of the organization to apply new strategies and proposals.

An automated monitoring service should also be present to support the monitoring process of governance and risk management.

During this research, we defined an event as a risk or an issue. Following the same line of thought, the Event Identification process, uses two separate application services from two different application components, but with the same behaviour: risk and issue creation. Similarly, to support the assessment of these events, assessments or analysis should be supported by application components, using once again, two separate application services to risks and issues. Risk Response and Control Activities processes are closely related to the treatment of the identified and assessed events, in order to address and resolve the event. Consequently, both processes use the risk and issue treatment service. Controls may also need to be created, thus a control creation service is needed.

The Control Activities process also has a direct relation with audits, since their function is to improve internal controls. For that reason, the audit execution and follow-up services are used by this process. These two services, may assist the Deviation Analysis and Deficiency Management processes, in order to support the execution and follow-up of audits.

The Requirement Analysis process, should be simplified through an application service, in order to ease the management of requirements and its relations across other information components in the organization.

As stated before, reporting is truly a common and important factor in integrated GRC, mainly due to the extensive relation among information structures. A reporting service may aid the documentation and communication of important information across the organization, and facilitate the implementation of a dashboarding service, that is much valued in organizations.

4.4 Application Structure Viewpoint

The application structure viewpoint shows the structure of one or more application components. This viewpoint is useful in designing or understanding the main structure of applications and the associated information [16].

The viewpoint presented in Fig. 8 describes the structure of the applications through the sharing of information. This view re-enforces the problem that integrated GRC addresses. Traditionally, the application components present in this viewpoint, represent departments, that usually do not communicate effectively and efficiently because they are isolated. The usage of mutual information between at least seven out of nine application components is impressive, and an integrated and holistic approach to all GRC activities makes indeed much more sense.

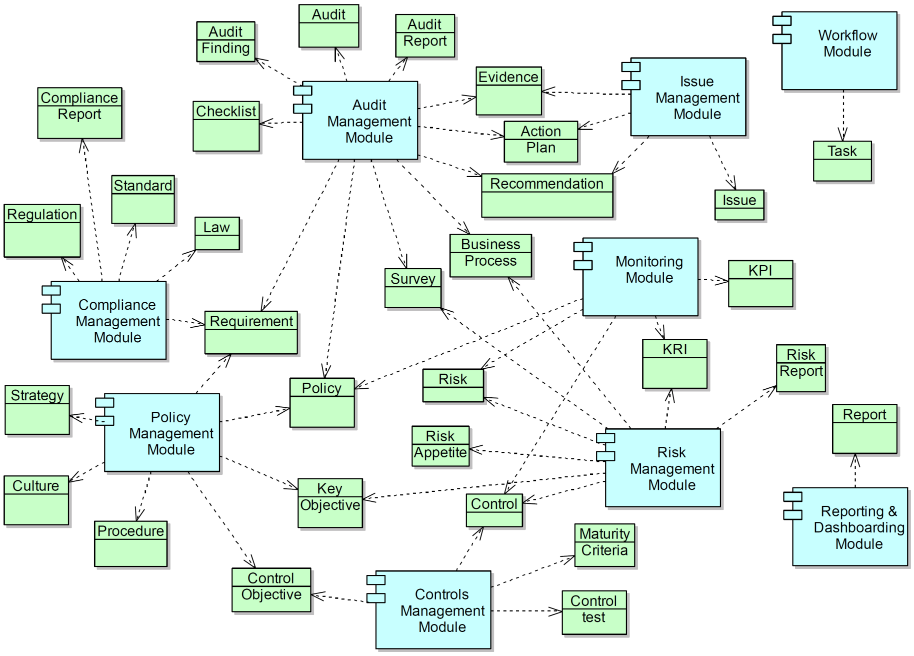


Fig. 8. Application Structure Viewpoint

5 Evaluation

To evaluate the reference model we opted for the quality factors proposed by the framework for data models from Moody and Shanks [14]. This framework is applicable not only to data models, but also to reference and conceptual models. Reference and conceptual models share common evaluation issues concerning their (re-)usability, testing and analysis [20, 21]. Another issue that difficult the evaluation of these models holds with the factor that reference or conceptual models often describe future domains, hence they cannot be evaluated against a user's perception of reality only [20].

The eight quality factors [14] are: Completeness, Integrity, Flexibility, Understandability, Correctness, Simplicity, Integration and Implementability. We will describe and discuss each individually:

- **Completeness** - *refers to whether the model contains all user requirements*: Concerning completeness for some organizations some processes or applications may be missing. However, since this research focus on the integration of the three disciplines and not so much in deepening each discipline, it is our belief that the reference model describes the key integration points between governance, risk and compliance.

- **Integrity** - *definition of business rules or constraints from the user requirements*: Given the abstraction of the constructed model, no constraints are specified or mandatory. Nonetheless, the processes used in this paper respect accepted rules in governance, risk management and compliance.
- **Flexibility** - *is defined as the ease with which the model can reflect changes in requirements without changing the model itself*: This factor has paramount importance in reference models. A good reference model must be extensible and evolvable. Given the abstraction of the architectural layers, processes and applications can be easily deepened and adaptable to diversified environments.
- **Understandability** - *is defined as the ease with which the concepts and structures in the model can be understood*: A key claim from ArchiMate is based on the understandable structure and concepts that it encompasses. For that matter, the use of ArchiMate presents an advantage for modelling architectures. Also, the use of multiple viewpoints clarifies the rationale of the model.
- **Correctness** - *is defined as whether the model conform to the rules of the modelling technique (i.e. whether it is a valid model). This includes diagramming conventions, naming rules, definition rules, rules of composition and normalisation*: In the Theoretical Background section we described the elements that have been used in this research. We have followed best practices from the ArchiMate specifications to design and relate elements using the viewpoints that better portray the structure of the architecture. Based on this arguments, we can affirm that the model is valid.
- **Simplicity** - *means that the model contains the minimum possible entities and relationships*: Although it was our objective to build a model containing the minimum, yet correct, concepts and relations, no measures were taken to ascertain this quality. A possible solution would be to discuss the obtained model with practitioners.
- **Integration** - *is defined as the consistency of the model with the rest of the organisation*: The model presents several viewpoints from different parts of the organization, and successfully relates them at the business and application level. Additionally, the application components were identified taking into account their modularity.
- **Implementability** - *is defined as the ease with which the model can be implemented within the time, budget and technology constraints of the project*: One of the claims of this research is to provide a reference concerning processes, applications and information. However, the reference architecture has not been implemented in any situation. Nonetheless, the use of reference processes, like COSO ERM and ISO 38500, ensures a certain level of applicability in specific situations.

6 Conclusion and Future Work

In this research we proposed a reference model that encompasses two architectural layers - business and information systems. Using research from the information systems knowledge base, we reinforced that design research artefacts can and should be employed in order to build new ones [22]. Scientific research can act as a source of independent, reliable and validated references in order to make improvements in this domain.

Our ultimate goal is to provide a generic reference for the implementation of integrated GRC. The use of ArchiMate facilitates the comprehension of the artefacts that compose the reference model, and was used to break down language barriers that often induce obstacles to progress in some areas [23].

As future work, we will focus in exploring the detail level of the architecture, by describing in more detail how he application layer provides the mentioned services and drilling down the processes from the business layer. Additionally, we will conduct surveys and interviews with practitioners to evaluate the pragmatic qualities of the proposed reference model.

References

1. Dittmar, L., Vogel, P.: Integrating GRC with Performance Management Demands Enterprise Solutions (2008)
2. Gill, S., Purushottam, U.: Integrated GRC - Is your Organization Ready to Move? In: Governance, Risk and Compliance. SETLabs Briefings (2008) 37–46
3. Hagerty, J., Kraus, B.: GRC in 2010: $29.8B in Spending Sparked by Risk, Visibility, and Efficiency. http://www.oversightsystems.com/pdf/whitepapers/AMR-GRC-in-2010.pdf (2009)
4. Rasmussen, M.: GRC 2011: Gripes & Directions. http://www.corp-integrity.com/compliance/grc-2011-gripes-directions (2011)
5. Mccuaig, B.: Building a Business Case For Governance, Risk and Compliance (GRC). http://paisley.thomsonreuters.com (2010)
6. Racz, N., Weippl, E., Seufert, A.: Governance, risk & compliance (grc) software - an exploratory study of software vendor and market research perspectives. In: HICSS, IEEE Computer Society (2011) 1–10
7. Racz, N., Weippl, E., Seufert, A.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). In Decker, B.D., Schaumüller-Bichl, I., eds.: Communications and Multimedia Security. Volume 6109 of LNCS., Springer (2010) 106–117
8. Shen, W., Camarinha-Matos, L., Afsarmanesh, H.: Towards a Reference Model for Collaborative Networked Organizations. In: Information Technology For Balanced Manufacturing Systems. Volume 220 of IFIP International Federation for Information Processing. Springer Boston (2006) 193–202
9. Dameri, R.P.: Improving the benefits of it compliance using enterprise management information systems. Information Systems Journal **12** (2009) 27 – 38
10. Schelp, J., Winter, R.: Language communities in enterprise architecture research. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology. DESRIST '09, ACM (2009) 23:1–23:10

11. Racz, N., Seufert, A., Weippl, E.: A Process Model for Integrated IT Governance, Risk, and Compliance Management. In: Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010), Riga, Latvia (2010) 155–170
12. Vicente, P., Mira da Silva, M.: A Conceptual Model for Integrated Governance, Risk and Compliance. In Mouratidis, H., Rolland, C., eds.: 23rd International Conference on Advanced Information Systems Engineering. Volume 6741 of LNCS., London, CAiSE'11, Springer (2011) 199–213
13. Brocke, J.V., Buddendick, C.: Reusable Conceptual Models - Requirements Based on the Design Science Research Paradigm. In: First International Conference on Design Science Research in Information Systems and Technology. (2006)
14. Moody, D.L., Shanks, G.G.: Improving the Quality of Data Models: Empirical Validation of a Quality Management Framework. Inf. Syst. **28** (2003) 619–650
15. Lankhorst, M., van Drunen, H.: Combining TOGAF and ArchiMate. www.via-nova-architectura.org (2007)
16. Iacob, M.E., Jonkers, H., Lankhorst, H.M., Proper, E.: ArchiMate 1.0 Specification. Technical report, The Open Group (2009)
17. Vicente, P., Mira da Silva, M.: A Business Viewpoint for integrated IT Governance, Risk and Compliance. In: Proceedings of the 1st International Workshop on IT GRC held in Conjunction with the 7th World Congress on Services (SERVICES 2011), Washington, IEEE (2011)
18. Moerdler, M.L., Boswell, C.S., Datskovsky, G., Swaminathan, M., Diebold, B.R., Ding, Y., Benton, J.D.: System and Method for Governance, Risk, and Compliance Management. Patent Application (2009) US 2009/0319312 A1.
19. ISO/IEC38500: Corporate governance of information technology (2008)
20. Frank, U.: Evaluation of Reference Models. In Fettke, P., Loos, P., eds.: Reference Modeling for Business Systems Analysis, Idea Group (2006) 118–140
21. Frank, U.: Conceptual Modelling as the Core of the Information Systems Discipline: Perspectives and Epistemological Challenges. In: Proceedings of the Fifth America's Conference on Information Systems (AMCIS99), Milwaukee, Association for Information Systems (1999) 695–698
22. Aier, S., Gleichauf, B.: Applying Design Research Artifacts for Building Design Research Artifacts: A Process Model for Enterprise Architecture Planning. In Winter, R., Zhao, J.L., Aier, S., eds.: Design Science Research in Information Systems and Technology. Volume 6105 of LNCS., Springer (2010) 333–348
23. Lang, M.: Communicating Academic Research Findings to IS Professionals: An Analysis of Problems. Informing Science **6** (2003) 21–29