A Comprehensive Approach to Compliance Management in Inter-organizational Service Integration Platforms

Laura González and Raúl Ruggia
Instituto de Computación, Facultad de Ingeniería, Universidad de la República,
J. Herrera y Reissig 565, Montevideo, Uruguay

Keywords: Compliance Management, Integration Platforms.

Abstract: Organizations increasingly collaborate with each other using the service-oriented approach. Such collaboration is usually supported by integration platforms which process all inter-organizational service interactions. In turn, these collaborative environments have to satisfy compliance requirements originating from different sources (e.g. laws, standards). This paper proposes a comprehensive approach to compliance management in inter-organizational service integration platforms. The approach defines a compliance management life cycle for this context and a common framework to homogeneously manage compliance issues in different areas.

1 INTRODUCTION

Organizations increasingly collaborate with each other following the service-oriented approach. This has led to large-scale systems which interconnect the software applications of different, autonomous and geographically distributed organizations (González and Ruggia, 2015). Such systems are usually supported by integration platforms which are specialized infrastructures providing connectivity and mediation capabilities to facilitate the integration of applications (Golluscio et al., 2016). By these means, rather than interacting directly, organizations communicate by exchanging messages through the platform. These messages may be processed by mediation flows which have the goal of solving integration issues by applying operations such message transformation and routing.

These collaborative environments have to satisfy compliance requirements established by various sources (e.g. laws), concerning different areas (e.g. quality of service) and which may apply to each organization or to the whole inter-organizational system (Elgammal et al., 2016). Some aspects of these requirements may impact on the interactions between organizations. In these cases, integration platforms mechanisms (e.g. transformations) can be used to deal with such requirements.

Taking this approach, solutions for controlling compliance requirements have been proposed in areas such as quality of service (QoS) (González and Ruggia, 2011), data quality (DQ) (Pidre et al., 2017) and data protection (DP) (González et al., 2016). The common approach in these proposals is: i) processing messages exchanged through the platform, ii) checking if they comply with the established requirements, and iii) in case requirements are not met, taking actions leveraging integration platforms mechanisms (e.g. transformations).

This work goes a step forward by proposing a comprehensive approach to compliance management in inter-organizational service integration platforms. The approach defines a compliance management life cycle for this specific context and a common framework to homogeneously manage compliance issues.

The rest of the paper is organized as follows. Section 2 shows a motivational scenario. Section 3 characterizes the working context. Section 4 describes the proposed approach. Section 5 analyses related work. Section 6 presents conclusions and future work.

2 MOTIVATIONAL SCENARIO

The scenario is inspired in the Uruguayan e-Government Interoperability Platform (eIP) (González et al., 2012) which was developed by the Uruguayan e-Government Agency (AGESIC). The eIP allows and facilitates government organizations to offer business services leveraging the web services technology. These web services, which are usually hosted on organizations' infrastructure, are exposed and invoked through proxy services

González, L. and Ruggia, R.
A Comprehensive Approach to Compliance Management in Inter-organizational Service Integration Platforms.
DOI: 10.5220/0006915406880696
In *Proceedings of the 13th International Conference on Software Technologies (ICSOFT 2018)*, pages 688-696
ISBN: 978-989-758-320-9

deployed on the eIP. This way, the eIP is able to process all service invocations and apply them security controls as well as mediation operations. For example, Figure 1 presents how web services messages are processed by the eIP when the Ministry of Public Health (MSP) invokes, via a proxy service, the Basic Information Service provided by the Civil Identification National Directorate (DNIC). This service receives a citizen identifier and returns basic information about citizens (e.g. their names).

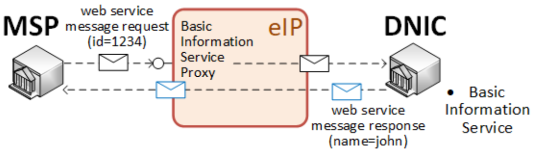

Figure 1: e-Government Interoperability Platform (eIP).

The eIP is not only intended to aid general purpose e-government operations but also to contribute to the development of supporting platforms in strategic sectors, such as health. Indeed, the Uruguayan e-Health Platform (Abin et al., 2015), which supports the National Electronic Health Record (EHR) in Uruguay, leverages and exposes services in the eIP.

2.1 Business Services

For the context of the motivational scenario, six business services are considered.

The Basic Information Service, provided by DNIC, makes available basic information about citizens. It has one synchronous request-response operation, named GetPersonById which, given a national identification number (NIN), returns data including names, last names, sex, birthdate and nationality.

The Passport Service, also provided by DNIC, allows citizens scheduling an appointment to get or renew their passport. It has two synchronous request-response operations. The GetAvailableDates operation receives a NIN and returns a list of available dates and times for the appointment. The ConfirmAppointment operation allows confirming the appointment by receiving a NIN, a date and a time, and returning whether or not the appointment was confirmed.

The Judicial Records Certificate Service, provided by the Technical Police National Directorate (DNPT) allows checking if a citizen has judicial records. It has one asynchronous request-response operation, named HasJudicialRecords, which receives a NIN and returns if the citizen with this NIN has judicial records.

The Local EHR Service, provided by Health Service Providers, allows providers to obtain clinical documents stored within other providers. It has one synchronous request-response operation, named ObtainDocument, which receives a document identifier and returns the clinical document associated with it.

The Procedures Status Service, provided by AGESIC, allows organizations to notify AGESIC the status of e-government procedures so it can be communicated to citizens (e.g. through a portal). It has one one-way operation, named NotifyProcedureStatus, which receives a NIN, a procedure identifier, an status and complementary information.

The Disability Records Service, provided by the Ministry of Social Development (MIDES), allows checking if citizens have disabilities. It has one synchronous request-response operation, named HasDisability, which receives an NIN and returns if the citizen is registered as having a disability.

2.2 Compliance Requirements

Compliance requirements arising in the motivational scenario are organized in four areas: QoS, Data Quality (DQ), Data Protection (DP) and Collaborations.

QoS requirements concerns aspects such as interoperability, performance and dependability. Interoperability requirements are mainly defined by AGESIC and Salud.uy (i.e. the e-health initiative in Uruguay). AGESIC requires web services to comply with SOAP 1.1 and with the WS-I Basic Profile 1.1. Salud.uy requires EHR services to use HL7 Messaging Standard Version 2.5 for exchanging clinical information and HL7V3 Clinical Document Architecture (CDA) R2 for structuring clinical documents. Performance requirements are mainly defined by organizations when they publish services in the eIP. Regarding throughput, the Basic Information Service is expected to handle seven transactions per second and the Disability Records Service ten transactions per second. In addition, this last service is expected to have a response time of five seconds. Dependability requirements are also defined by organizations when they publish services. The Basic Information Service and the Disability Records Service are expected to have an availability of 99% and 90%, respectively. Within the motivational scenario the succesability (i.e. the percentage of responses returned without unhandled errors) of all services is expected to be greater than 80%.

DQ requirements concerns aspects such as interoperability, completeness, accuracy and consistency (Pidre et al., 2017). Regarding interoperability, AGESIC requires the use of reference data models for exchanging data of people and addresses. Salud.uy requires the use of SNOMED-CT and ICD-10 for specifying clinical information such as causes of death. With respect to completeness, Salud.uy established minimal data sets to register specific clinical events such as centralized urgent emergency medical consultations. AGESIC also established syntactic accuracy requirements (e.g. countries should be specified using the Alpha-3 codes of the ISO 3166-1 standard). It also established allowed values for civil status, sex, gender and citizenship, among others. Regarding consistency, there are relational integrity requirements (e.g. the locality and department of an address should be consistent with each other as well as the disease and sex specified in a clinical document). There are also temporal integrity requirements (i.e. data should be consistent over time).

DP requirements concerns aspects such as privacy, integrity and confidentiality. Regarding privacy, organizations are not allowed to share sensitive personal data of citizens unless they provide explicit consent for that. With respect to integrity, Salud.uy requires Health Service Providers to sign the clinical documents they provide with advanced digital signature. Finally, in order to ensure confidentiality, data regarding the racial origin and sex of citizens are required to be encrypted when they are exchanged.

Collaboration requirements originate when two or more organizations agree to carry out collaborative processes. For example, the Passport Application collaboration allows citizens to get or renew their passport and it involves three organizations: AGESIC, DNIC and DNPT. The collaboration starts when a citizen requests an appointment through the portal. AGESIC interacts with DNIC, through the Passport Service, to get the appointment and DNIC returns a list of available dates and times. After the citizen selects a date and a time, AGESIC confirms these data to DNIC via the Passport Service. DNIC checks if the citizen has judicial records by interacting with DNPT through the Judicial Records Certificate Service. If the citizen has judicial records or if DNIC does not receive a response from DNPT in twenty four hours, the appointment is canceled and DNIC informs AGESIC of this decision via the Procedure Status Service. Otherwise, DNIC informs AGESIC if the citizen could get or renew the passport. For this collaboration two requirements are considered: i) messages should flow as specified in the collaboration, and ii) the collaboration has to be completed in less than one month.

3 WORKING CONTEXT

This section characterizes the working context taken as starting point for the proposed approach. This working context constitutes a generalization of the motivational scenario presented in Section 2.

The working context comprises organizations collaborating through an integration platform via service-based interactions (González and Ruggia, 2015). To this end, as shown in Figure 2, business services running in organizations (e.g. BS1) are exposed through proxy services (e.g. S1) deployed on the integration platform. For the context of this work, business and proxy services are assumed to be implemented as web services.

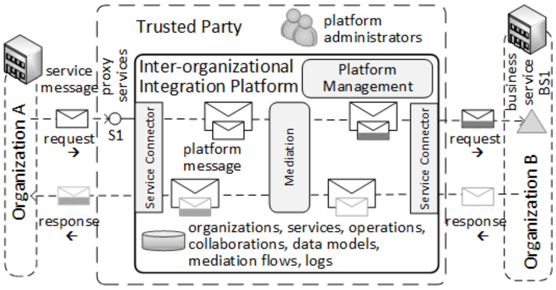

Figure 2: General Description of the Working Context.

When an organization (e.g. Organization A) invokes a business service provided by another organization (e.g. BS1 provided by Organization B), service messages (e.g. SOAP messages) are exchanged through the platform between these organizations. Service messages are first processed by a connector which creates platform-specific messages containing a service message and message properties (e.g. a message id). Service messages can include business data elements. Messages properties specify the origin (e.g. an organization), destination (e.g. a service) and identification related data (e.g. a message id). These properties may be obtained from the service message or may be automatically generated by the platform (e.g. message ids). Message properties allow specifying, for example, that a message is sent by a user (e.g. smith) belonging to an organization (e.g. Organization A) in order to invoke a service (e.g. S1) provided by other organization (e.g. Organization B). The platform processes these messages and may apply them different mediation operations.

The integration platform is hosted on a trusted party and managed by platform administrators. Administrators maintain data required by the platform in order to operate (e.g. integrated organizations, services provided by organizations, the operations each service has, collaborations, data models).

3.1 Working Context Concepts

The main concepts of the working context are: organizations, services, operations, message types, collaborations, data models and data elements. Figure 3 shows these concepts as well as their relationships.

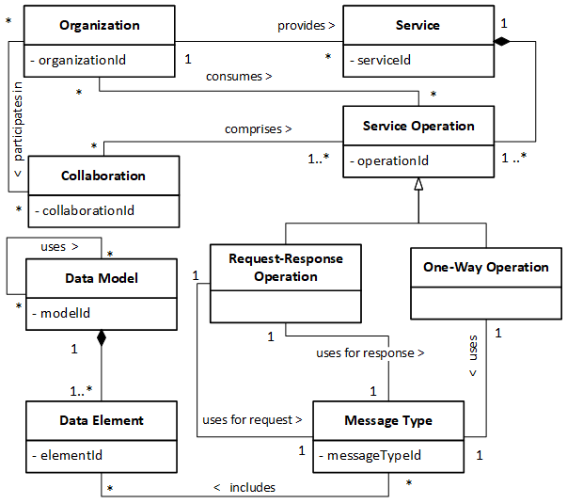

Figure 3: Working Context Concepts.

Organizations provide services and consume operations of services exposed through the platform. For example, DNPT provides the Judicial Records Certificate service which has the operation HasJudicialRecords that is consumed by DNIC. Services have one or more operations which can be either request-response operations (e.g. HasJudicialRecords) or one-way operations (e.g. NotifyProcedureStatus).

Data models specify the structure of data (e.g. person) exchanged in invocations. A data model (e.g. person model) may use others (e.g. address model) and comprises at least one data element (e.g. name). Message types specify the structure of messages that organizations exchange when invoking service operations. Message types may include data elements defined within data models.

Organizations participate in collaborations which comprise one or more service operations (e.g. the Passport Application collaboration comprises the operations: GetAvailableDates, ConfirmAppointment, NotifyProcedureStatus and HasJudicialRecords).

3.2 Business Transactions Concepts

At runtime, organizations carry out business transactions by collaborating with each other through the platform. Figure 4 presents the main concepts related to business transactions. The concepts in gray were already introduced in Figure 3 and their relations are not included in order to simplify the diagram.

Business transactions can be either operation transactions or collaboration transactions. An operation transaction corresponds to the invocation of an operation by a client and can be either a request-response transaction or a one-way transaction. Operation transactions comprise one or more platform messages which may include a service message of a specific type. A collaboration transaction corresponds to the execution of a collaboration and it includes one or more operation transactions.

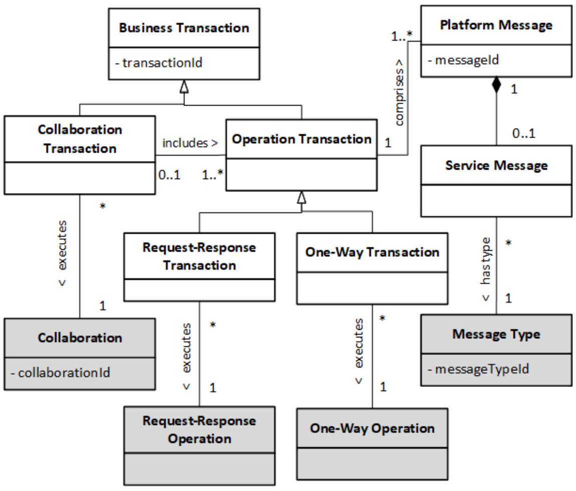

Figure 4: Business Transactions Concepts.

4 COMPLIANCE APPROACH

This section presents the compliance management approach for inter-organizational service integration platforms which: i) defines a life cycle for compliance management within the working context presented in Section 3 and, ii) defines a common framework, comprising conceptual models and components, in order to homogeneously manage compliance issues.

4.1 General Description

Figure 5 presents a high-level description of the proposed approach showing the new compliance related actors and how the compliance management system extends integration platforms to support the proposed compliance management life cycle.

Compliance actors are either Compliance Business Experts or Compliance Technical Experts. Compliance business experts are responsible for the business related aspects of compliance management. In particular, they are aware of the applicable regulations, how these regulations impact on inter-organizational interactions carry out through the platform and what actions (e.g. sanctions) should be taken in case these regulations are not met. Compliance technical experts are responsible for the technical related aspects of compliance management. For instance, they know how to setup technical compliance mechanisms within the platform (e.g. the available system level compliance actions) and how to im-

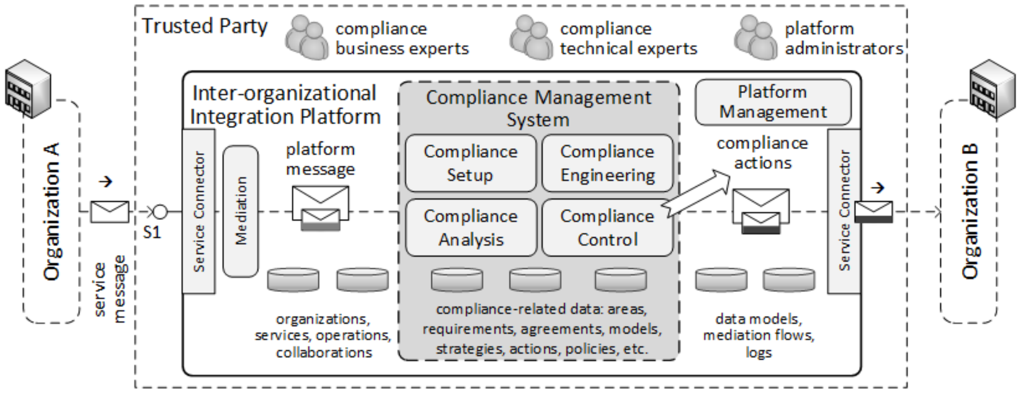
Trusted Party
compliance business experts
compliance technical experts
platform administrators
Organization A
service message
S1
Inter-organizational Integration Platform
Service Connector
Mediation
platform message
organizations, services, operations, collaborations
Compliance Management System
Compliance Setup
Compliance Engineering
Compliance Analysis
Compliance Control
compliance-related data: areas, requirements, agreements, models, strategies, actions, policies, etc.
Platform Management
compliance actions
data models, mediation flows, logs
Service Connector
Organization B

Figure 5: Compliance Management Approach.

plement solutions which control (e.g. monitor, enforce) compliance within the platform.

The compliance management life cycle proposed in this work comprises four phases: Compliance Setup, Compliance Engineering, Compliance Control and Compliance Analysis. The Compliance Management System extends inter-organizational integration platforms in order to deal with compliance management within them. As shown in Figure 5, it comprises four subsystems geared towards supporting the four phases of the compliance life cycle.

4.2 Compliance Setup

Compliance Setup involves managing elements that allow building compliance solutions and is supported by the Compliance Setup Subsystem. In particular, this subsystem allows managing system level compliance actions, business level compliance actions and external compliance services.

System Level Compliance Actions are actions taken within the platform (e.g. transforming a message) in order to enforce compliance or to repair a situation where compliance is not met. For example, a ”Remove Data Values” action may remove values of data elements from a message.

Business Level Compliance Actions (e.g. sanctions) are triggered by the platform when compliance with regulations is controlled. They have a business connotation as opposed to system level actions. An example of a business level action is a monetary sanction to an organization.

External Compliance Services provide access to data attributes (e.g. additional information of a user) or functionality (e.g. validation functions) required for compliance control. Some examples of external services are: ”User Roles” (it returns the roles of a user) and ”Alpha 3 - Correct” (it returns true if the country is specified using Alpha 3).

4.3 Compliance Engineering

Compliance Engineering focuses on the development of compliance solutions for controlling compliance within the platform and it is supported by the Compliance Engineering Subsystem. Compliance engineering comprises Compliance Modeling, Compliance Specification, Compliance Development and Compliance Deployment which are supported by specific subsystems of the compliance engineering subsystem.

4.3.1 Compliance Modeling

Compliance Modeling involves managing compliance aspects relevant for the integration platform. In particular, compliance models define the relevant compliance areas (e.g. QoS, DQ) and relevant characteristics within these areas (e.g. availability, completeness). Compliance requirements specify general requirements (e.g. response time greater than 1ms) applying to specific objects types (e.g. operation, service). Compliance profiles define a set of requirements for the same object type, in order to make more agile the specification of a set of requirements for different objects of the same type. Regulations are also managed, which allows relating requirements with the regulations from which they come from. Compliance modeling is mainly performed by compliance business experts. The main concepts related to compliance modeling are presented in Figure 6.

Compliance Object Types represent the types of objects that are target of compliance control. The objects types identified in this work as well as examples of requirements for these types, within the motivational scenario, are:

- Platform: SOAP web services must comply with the WS-I Basic Profile 1.1.
- Organization: The average availability of services provided by AGESIC must be greater than 95%.

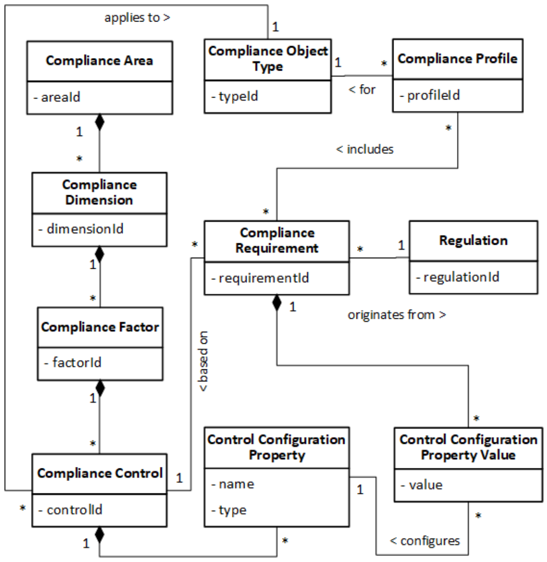

Figure 6: Compliance Modeling Concepts.

- Collaboration: Messages exchanged within the Passport Application collaboration should follow the specified message flow.
- Service: Racial origin data must be returned encrypted by the Basic Information Service.
- Operation: The response time of the HasDisability operation must be less than 5 seconds.
- Message Type: The civil status data included in the message type associated with the getPersonById operation should be syntactically correct.

Compliance Areas represent broad areas of compliance (e.g. QoS, DQ). Compliance areas comprise Compliance Dimensions which capture a high level compliance facet (e.g. performance) within an area. Compliance Factors represent a particular aspect of a dimension (e.g. response time). Examples of compliance areas and dimensions originating from the motivational scenario are: i) Quality of Service (dimensions: Performance, Dependability, Interoperability), ii) Data Quality (dimensions: Accuracy, Completeness, Consistency, Interoperability), iii) Data Protection (dimensions: Privacy, Integrity, Confidentiality), and iv) Collaborations (dimensions: Collaboration Messages, Collaboration Execution).

Examples of compliance factors in the QoS area are: i) for performance: Response Time, Throughput; ii) for dependability: Availability, Succesability; iii) for interoperability: Standards Adoption / Conformance. Examples of compliance factors in the DQ area are: i) for accuracy: Syntactic Correctness, Precision; ii) for completeness: Density, Coverage; iii) for consistency: Relational / Time Integrity; iv) for interoperability: Standards / Recommendations Adoption. Examples of compliance factors in the DP area are: i) for privacy: Message / Data Element Privacy; ii) for integrity: Message / Data Element Integrity; iii) for confidentiality: Message / Data Element Confidentiality. Examples of compliance factors in the Collaborations area are: i) for messages: Messages Flow; ii) for collaboration execution: Processing Time.

Compliance Controls (e.g. max response time) are used to control compliance factors for a specific compliance object type (e.g. service). They have configuration properties (e.g. response time in seconds) that allow reusing the control. Within the motivational scenario, a max response time control may be used for all the response time requirements by specifying the specific value for each service.

Compliance Requirements represent requirements that can be applied to different objects of the same type (e.g. availability of a service greater than 90%). A compliance requirement is based on a compliance control (e.g. availability of a service greater than a percentage value) and defines a value for all its configuration properties (e.g. percentage value = 90%).

Compliance Profiles group compliance requirements for the same object type (e.g. service) with the goal of facilitating the specification of a group of requirements for different objects of the same type.

Finally, compliance requirements originate from regulations (e.g laws, agreements).

4.3.2 Compliance Specification

Compliance Specification involves the specification of compliance requirements (e.g. response time greater than 1ms) for concrete compliance objects (e.g. Basic Information Service). Requirements are specified in agreements which may define actions (e.g. notify an administrator) for different situations (e.g. if requirements are not met). Figure 7 presents the main concepts related to compliance specification.

Object Compliance Requirements (i.e. compliance requirements applied to concrete objects) are specified in Compliance Agreements in which at least one organization participates. For instance, when an organization publish a service in the platform, it can establish an agreement where it commits to provide an availability of 99% by leveraging the requirement ”Availability greater than 99%”.

Compliance Agreements also comprise Agreement Actions which specify the actions to be taken in case the specified Compliance Conditions for these actions hold. Agreement actions are based on Business Level Compliance Actions (e.g. sanctions, incentives) provided by the platform. An agreement action should specify a value for each configuration property of the associated compliance action.

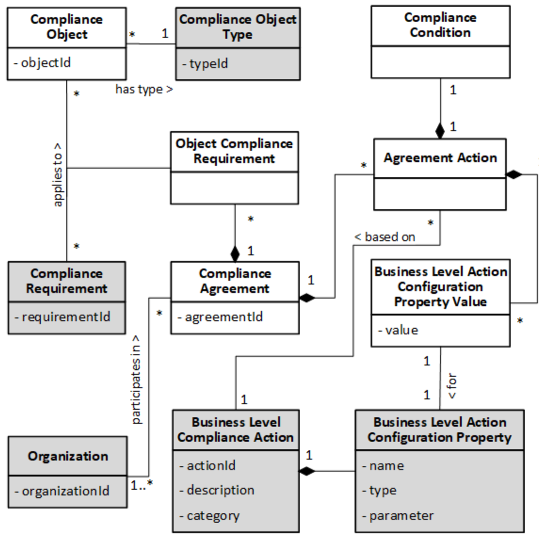

Figure 7: Compliance Specification Concepts.

In the context of the motivational scenario, a compliance agreement may be set up between DNIC, DNPT and AGESIC in order to control the compliance requirements of the Passport Application Collaboration. Compliance conditions may establish that if the specified message flow for the collaboration is not followed more than three times at day, a monetary sanction has to be issued for the three organizations.

4.3.3 Compliance Development

Compliance Development involves defining how compliance requirements have to be controlled within the integration platform. In particular, this comprises managing compliance strategies (e.g. reactive, preventive) and compliance methods (e.g. enforce privacy). This work takes a policy-based approach to control compliance (González and Ruggia, 2017), that is, compliance methods are specified in terms of compliance policies. Figure 8 presents the main concepts related to compliance development.

Compliance Method Templates are blueprints for implementing compliance controls (e.g. regarding service availability) within the platform. They are specified in terms of Compliance Policy Templates. Neither the methods templates nor the policy templates are completely specified given that they depend on the specific requirement (e.g. availability greater than 90%) and the specific object (e.g. Disability Records Service) to which the requirement applies.

Compliance Methods control compliance requirements for specific compliance objects in the platform. They may be generated from compliance method templates according to the values of configuration properties for the associated compliance control. These methods comprise a set of Compliance Policies which may also be generated from policy templates associated with the method template. Also, a compliance developer may implement compliance methods from scratch or may modify the generated methods and policies in order to suit the required needs.

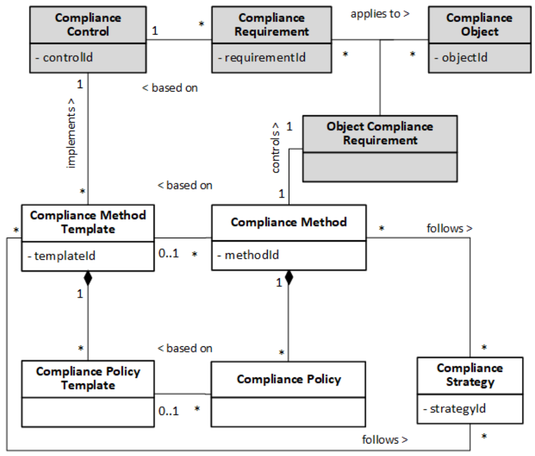

Figure 8: Compliance Development Concepts.

Compliance methods and method templates may follow Compliance Strategies (e.g. reactive) which provide additional information about them.

4.3.4 Compliance Deployment

Compliance Deployment involves installing and letting operational, in the platform, the compliance elements defined in the setup phase (e.g. system-level actions) and in the previous sub-phases of the engineering phase (e.g. agreements, policies). In particular, compliance policies may lead to the deployment of monitored events, if they specify certain types of conditions (e.g. temporal conditions). These events are then monitored by components of the platform.

4.4 Compliance Control

Compliance Control involves controlling compliance within the platform, based on the compliance solutions developed in the engineering phase, and it is supported by the Compliance Control Subsystem. Compliance control comprises System-level Compliance Control, Runtime Business-level Compliance Control and A Posteriori Business-level Compliance Control which, as shown in Figure 9, are supported by subsystems of the compliance control subsystem.

System-level Compliance Control involves processing platform messages in order to control compliance within messages exchanges, based on the deployed compliance elements (e.g. policies). This control, at the message level, may involve processing: i)

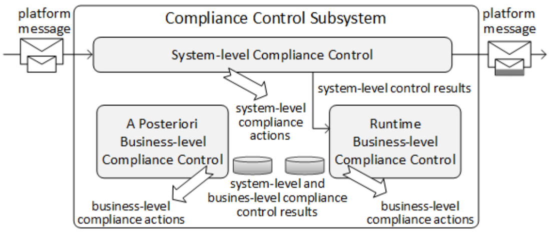
platform message
Compliance Control Subsystem
platform message
System-level Compliance Control
system-level control results
system-level compliance actions
A Posteriori Business-level Compliance Control
Runtime Business-level Compliance Control
system-level and business-level compliance control results
business-level compliance actions
business-level compliance actions

Figure 9: Compliance Control Subsystem.

only one message (e.g. to check if a data element is compliant with ICD-10), ii) two messages (e.g. to check if the temporal distance between a service request and a response is as specified by a response time requirement), iii) various messages of a collaboration (e.g. to check if they are interchanged as specified in the corresponding messages flow), or iv) various independent messages (e.g. to check if a data element, as birthdate, is consistent over time). In case a not-compliance is detected, system-level compliance actions specified in policies may be taken (e.g. taking out data from a message). System-level compliance control is automatically performed by the platform and it is supported by the System-level Compliance Control (SCC) Subsystem.

Runtime Business-level Compliance Control involves processing system-level compliance control results obtained from the SCC subsystem and controlling compliance with requirements and agreements. Business-level compliance actions can be taken (e.g. sanctions, incentives) after business-level compliance control is completed. Runtime Business-level compliance control is automatically performed by the platform and it is supported by the Runtime Business-level Compliance Control (RBCC) Subsystem.

A Posteriori Business-level Compliance Control involves processing system-level and business-level compliance control results in order to control compliance. This may be needed when such controls can not be performed by the RBCC. A posterior business-level compliance control can be either automatically performed by the platform or can be performed by compliance business experts. This a posteriori control can also lead to business-level compliance actions and it is supported by the A Posteriori Business-level Compliance Control (PBCC) Subsystem.

4.5 Compliance Analysis

Compliance Analysis involves analyzing compliance control results as well as defining compliance analysis artifacts (e.g. reports) in order to facilitate such analysis. The activities of this phase are mainly performed by compliance business experts and are supported by the Compliance Analysis Subsystem which includes three subsystems to support Compliance Traceability, Compliance Reporting and Compliance Dashboards.

Compliance Traceability comprises tracing compliance violations starting from high level elements (e.g. compliance agreements) until reaching the message level. This allows explaining how a compliance violation took place in terms of platform messages. For example, a traceability view may be set up so that a compliance expert can obtain the violations of an agreement as well as the associated compliance requirements violations and the platform messages that caused that those requirements were not met.

Compliance Reporting involves defining compliance reports, based on the defined traceability views, as well as using them to analyze compliance evaluation results. A compliance report provides a view of compliance violations for specific elements.

Compliance Dashboards group compliance reports of interest for a given user so that compliance control results are displayed in an integrated way for that user. In addition, compliance dashboards allows specifying the format in which these results are presented (e.g. summaries, graphs).

5 RELATED WORK

There are various proposals which identify different phases in a compliance management process (Sackmann and Kähmer, 2008)(Koliadis and Ghose, 2008)(El Kharbili, 2012)(Tran et al., 2012). Our work is aligned with these proposals; indeed it takes some of the phases identified by them. However, compared to our work, none of these proposals specializes the phases for inter-organizational integration platforms. There are also proposals that address compliance issues in cross-organizational business process (Knuplesch et al., 2013). Our proposal also deals with this kind of requirements, but it is not restricted to only that. Regarding comprehensive approaches to compliance management, one of the most relevant initiatives is the European project COMPAS that proposed an integrated solution for runtime compliance governance in SOA (Tran et al., 2012). However, the project focuses on compliance management within an organization while our work deals with compliance management within integration platforms that process inter-organizational service interactions.

In summary, the distinguished characteristics of our proposal are: i) the focus on compliance management in inter-organizational interactions, ii) policy-based solutions that process all interactions within an integration platform, iii) a common framework (e.g. models) that allows dealing with different compliance areas in an homogeneous way, iv) non-invasive solutions (i.e. not requiring deployments in organizations), and v) a compliance management life cycle including adapted activities for the specific context.

6 CONCLUSIONS

This work proposes a comprehensive approach to compliance management in inter-organizational service integration platforms. The approach defines a compliance management life cycle for this specific context and a common framework to homogeneously manage compliance issues.

The life cycle includes four main phases: setup, engineering, control and analysis. The engineering phase comprises compliance modeling, specification, development and deployment. The control phase comprises system-level compliance control and business-level compliance control.

The common framework includes conceptual models and components that allow managing aspects of compliance through the whole life cycle and within different compliance areas in an homogeneous way.

Future work consists in completing the specification of the compliance policy language to be used in the approach. This language is inspired in XACML, extending it to not only deal with access control issues. The example in (González and Ruggia, 2017) shows how compliance policies would look like. In addition, we plan to continue advancing in the evaluation of the technical feasibility of the approach through the development of prototypes. Finally, we aim to address other compliance areas such as privacy in the e-health domain.

REFERENCES

Abin, J., Nemeth, H., and Friedmann, I. (2015). Systems architecture for a nationwide healthcare system. In *MEDINFO 2015: Proceedings of the 15th World Congress on Health and Biomedical Informatics*.

El Kharbili, M. (2012). Business process regulatory compliance management solution frameworks: A comparative evaluation. In *Proceedings of the Eighth Asia-Pacific Conference on Conceptual Modelling - Volume 130*, APCCM '12. Australian Computer Society, Inc.

Elgammal, A., Turetken, O., van den Heuvel, W.-J., and Papazoglou, M. (2016). Formalizing and appling compliance patterns for business process compliance. *Software & Systems Modeling*, 15(1):119–146.

Golluscio, E., Thompson, J., and Guttridge, K. (2016). Market Guide for Hybrid Integration Platform-Enabling Technologies. Technical Report G00290089, Gartner.

González, L., Echevarría, A., Morales, D., and Ruggia, R. (2016). An e-government interoperability platform supporting personal data protection regulations. *CLEI Electronic Journal*, 19:8 – 8.

González, L. and Ruggia, R. (2011). Addressing QoS issues in service based systems through an adaptive ESB infrastructure. In *6th Workshop on Middleware for Service Oriented Computing - MW4SOC'11*. ACM Press.

González, L. and Ruggia, R. (2015). A reference architecture for integration platforms supporting cross-organizational collaboration. In *Proceedings of 17th International Conference on Information Integration and Web-based Applications &Services*. ACM Press.

González, L. and Ruggia, R. (2017). Towards a middleware and policy-based approach to compliance management for collaborative organizations interactions. In *Proceedings of the 12th International Conference on Software Technologies*. SCITEPRESS.

González, L., Ruggia, R., Abin, J., Llambías, G., Sosa, R., Rienzi, B., Bello, D., and Álvarez, F. (2012). A service-oriented integration platform to support a joined-up e-government approach: The uruguayan experience. In *Advancing Democracy, Government and Governance*, volume 7452 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg.

Knuplesch, D., Reichert, M., Fdhila, W., and Rinderle-Ma, S. (2013). On enabling compliance of cross-organizational business processes. In Daniel, F., Wang, J., and Weber, B., editors, *Business Process Management*, pages 146–154, Berlin, Heidelberg. Springer Berlin Heidelberg.

Koliadis and Ghose (2008). Service compliance: towards electronic compliance programs. Technical report.

Pidre, S., González, Mendoza, R., Pinatares, M., Granja, N., Serra, F., and Ruggia, R. (2017). A data quality aware enterprise service bus for e-health integration platforms. In *2017 XLIII Latin American Computer Conference (CLEI)*. IEEE.

Sackmann, S. and Kähmer, M. (2008). Expdt: A policy-based approach for automating compliance. *WIRTSCHAFTSINFORMATIK*, 50(5):366–374.

Tran, Zdun, Holmes, Oberortner, Mulo, and Dustdar (2012). Compliance in service-oriented architectures: A model-driven and view-based approach. *Information and Software Technology*, 54(6).