Compliance Evaluation Featuring Heat Maps (CE-HM): A Meta-Modeling-Based Approach

Dimitris Karagiannis[1], Christoph Moser[1], and Arash Mostashari[2]

[1] University of Vienna, Research Group Knowledge Engineering Bruennerstraße 72, 1210 Vienna, Austria
{dk,c.moser}@dke.univie.ac.at
[2] BOC IS GmbH, Wipplingerstr. 1, 1010 Vienna, Austria
arash.mostashari@boc-eu.com

Abstract. The recent global economic crisis and the growing reliance on information technology pile pressure on organizations to comply with regulations, legal rules and laws. Organizations tend to struggle with paper work for the mere purpose of proving compliance. Compliance Management should be subject to existing management frameworks. Otherwise, ineffective procedures will evolve, and the organization will fail to combine Compliance Management with continuous improvement measures. We advocate for a generic compliance evaluation method, which builds upon existing enterprise modeling frameworks, for three reasons: First, synergies in data acquisition will arise. Second, reusing organization-wide accepted viewpoints will create trust among stakeholders and ease communication of the compliance status. Third, taking steps to improve compliance will be part of daily operations based on institutionalized processes geared to the established management frameworks. In addition, the prototypical implementation of the 'Compliance Evaluation Featuring Heat Maps (CE-HM)' method based on a meta-modeling platform is presented.

Keywords: Compliance, Evaluation, Heat Maps, Meta-Modeling.

1 Introduction

Leveraging internal auditing is the bedrock of Compliance Management, regardless of whether compliance audit refers to internal procedures in organizations, external regulatory requirements, such as Sarbanes Oxley, Basel II/III, and Solvency II, or industry codes of conduct, such as ISO 14001 for Environmental Management.

While the definition of the term Compliance and Compliance Management varies among different sources, one can point out a number of similarities between these definitions. For this paper we define *Compliance* in a broad sense, namely as the set of laws, regulations, policies, or best practices an organization needs to fulfill, regardless of whether they are self-imposed or forced by governmental regulations. We define *Compliance Management* akin to [24], who refers to it as the processes for accomplishing, monitoring and managing compliance of an organization.

J. Ralyté et al. (Eds.): CAiSE 2012, LNCS 7328, pp. 414–428, 2012.

Organizations often pursue Compliance Management merely to comply with legal rules and laws, without any context to the organization's continuous improvement measures. Our method is based on enterprise modeling methods, such as Business Process Management and Enterprise Architecture Management. The advantages that accrue from the synergy between enterprise modeling methods and Compliance Management are as follows: first, the existing enterprise models provide an ideal starting base increasing the productivity by sharing the efforts for creating and maintaining the underlying information base. Second, synergies arise by reusing established and well-known viewpoints, such as process maps or application architecture diagrams. Third, as Compliance Management activities are based on established BPM/EAM processes, resolving compliance issues will be part of day-to-day work activities. However, it must be indicated, that although the presented method supports both, a green-field approach as well as the reuse of an existing information base and established viewpoints, the latter can only be achieved if the existing content is held in a meta-modeling platform.

An intuitive and coherent visualization of the organization's compliance state will support internal audits and help the organization to pass external audits [24]. In our method, we utilize heat maps to visualize the degree of conformance with regulations. The term heat map originates from the field of cartography. Cartographers use choropleth maps to highlight specific areas on maps by coloring or shading them. However, in enterprise modeling literature, the preferred term for this type of maps is referred to as heat map (see e.g. [14] and [17]). We see heat maps as a powerful tool quantifying compliance, enabling organizations to visualize their compliance gaps and to take steps to improve compliance. By applying to Shneiderman's visualization mantra [25]: 'overview first', 'zoom and filter', and 'details on demand', our method combines a variety of viewpoints, such as diagrams and matrices [27]. We implemented our CE-HM method (according to the definitions established by the Open Model Initiative [13]) on the meta-modeling platform ADO*xx*. This method is designed for tools that enable direct and simple access to the meta-model of the provided modeling method.

The remainder of the paper is organized as follows: In section 2 related approaches to Compliance Management, some of them laying the groundwork of our method, are summarized. Furthermore, a number of general requirements for compliance management frameworks are briefly discussed. Subsequently, section 3 discusses the theoretical grounding we apply, namely the definition of the modeling method, followed by our main contribution, which emphasizes a compliance evaluation method based on meta-modeling and heat maps (CE-HM). Section 4 briefly presents a CE-HM prototype utilizing the meta-modeling platform ADO*xx*. Finally, section 5 gives a summary followed by an outlook on future work.

2 Related Work

Prominent standards and frameworks for Compliance Management, such as COSO, CobiT, and SAC (for a broad overview see for example [4]), typically provide a rich

foundation of guidelines in the form of control objectives or principles. However, none of those give detailed methodical advice to measure the degree of compliance. Typically, they do not provide tool support for assessing and communicating compliance. Thus, usually spreadsheets are used for assessing the compliance status, an approach [9] referred to as document-based approach, being the most common approach for Compliance Management at the present time. [9] states as one of the major drawbacks of this manual applied approach, that reusability is significantly impacted and the approach is typically associated with high efforts for ongoing maintenance activities, status tracking and communication of compliance issues.
In the following, we focus on related work in the area of conceptual modeling, as it is one of the main pillars of our method.

As early as the end of the 1970s, [18] recognizes the potentials of supporting Compliance Management through conceptual models. [26] explicates that most present approaches focus on Business Process Management such as the Business Process Management Notation (BPMN) and Event-driven Process Chain (EPC), and advocates enterprise modeling approaches such as MEMO [8] and ArchiMate [16], usually covering the entire organization as an ideal foundation for Compliance Management. By giving advice on enriching enterprise modeling approaches in order to support internal control modeling, the authors constitute the groundwork for the compliance evaluation method at hand. However, they put a strong focus on language design. Evaluation mechanisms and specific visualizations for analyzing, visualizing and communicating the degree of compliance are not central.

According to [1], architecture principles (classified into inherent laws, imposed laws, and guidelines) are mainly imposed to limit design freedom regarding enterprise architectures. Hence, in the broader sense, architecture principles address the subject of compliance with regulations, laws and standards. EA frameworks, such as TOGAF [27], FEAF [6] and TEAF [5] exemplarily state architecture principles and give advice on how to define an appropriate set of principles. According to [7], one important quality for every principle is to clearly define how to measure its fulfillment. However, none of the aforementioned EA frameworks specify a method for measuring the fulfillment level consistently, nor suggest how to visualize and communicate the compliance posture.

[14] and [17] introduce heat maps in the fields of EA Management for visualizing business capabilities. Although, merely discussing the approach in the context of Business Capability Management, the sketched heat mapping mechanisms can be applied to any modeling domain. According to [14] '*representation of heat maps allows a high variability in itself*'. It is stated that any set of attributes (of the underlying meta-model) can be evaluated and combined using any evaluation function, assigning colors to the graphical representation of architecture artifacts represented in a diagram. However, concrete evaluation functions are not discussed.

An example of an advanced evaluation function for qualitative enterprise architecture management, based on Probabilistic Relations Models (PRM), is presented in [2]. The quality 'availability' is exemplarily used for illustration purposes although the authors state that the method is meant to be applicable more generally. The discussed method as a prerequisite requires a strong foundation of input parameters. This might

restrain organizational-wide acceptance and use. Furthermore, as the method is not explicitly intended for ongoing Compliance Management activities, mechanisms for putting the underlying architecture artifacts and their relations under control (e.g. time-related views, versioning) are not elaborated.

In the following, a short overview on requirements for compliance evaluation methods – identified for the CE-HM - is given. The requirements have been distilled from the above discussed literature as well as from [30], and above all from [29]:

Requirement 1 – Change Management: Regulations underlie continual change. The method needs to deal with this permanent change. This requirement will be covered by the time-view mechanisms, discussed in section 3.2, allowing to represent different points in time (as-is, intermediate and target architectures) in one repository.

Requirement 2 – Traceability and Accountability: This requirement is covered by the ADOxx platform providing a detailed changelog for any changes made to the models and evaluations.

Requirement 3 – Complexity: This refers to the complexity of the involved modeling effort. According to [29] '*a generic compliance management framework should not be custom-tailored to a specific purpose or a specific domain'*. This requirement is covered, as the CE-HM method works with any meta-model.

Requirement 4 – Efficiency: This requirement focuses on the efficiency of the underlying principles. The CE-HM method advocates the usage of principles derived from best practice frameworks, such as CobiT [11], but does not incorporate mechanisms to assess the efficiency of the chosen principles as such. Therefore, this requirement is only covered indirectly by the presented method in this paper.

Requirement 5 – Cost: The method must allow for economical and resource-conserving processes. CE-HM resolves this by reusing existing model base of established modeling methods, thus saving time and efforts.

Requirement 6 – Enforceability: The method should support the enforceability of defined principles. This is done implicitly by combining CE-HM with established management methods such as TOGAF [27], which typically provide the required management structures.

Requirement 7 – Scalability: The method must allow for growth (and scoping). Typically the number of principles and models will grow over time. The method needs to consider this and remain manageable.

Requirement 8 – Multi-dimensional Evaluation and Drill-Down Mechanisms: According to [30], means for '*evaluation along structural, temporal and functional aggregation dimensions of an organization*' must be possible. Furthermore, propagation of evaluations needs to be supported. Hence, it must be possible to aggregate low-level evaluations (e.g. individual organizational units) to more abstract levels (e.g. the entire organization). This requirement is covered by the discussed evaluation configurations and the corresponding propagation mechanisms of the CE-HM method (see section 3.2), which work with any established meta-model.

3 The Compliance Evaluation Method 'CE-HM'

The CE-HM method – and according to [15], any structured modeling task – is based on modeling methods. We apply the definition of [15] regarding modeling methods as follows. Modeling methods are composed of two major components: (1) a modeling technique, divided into a modeling language and a modeling procedure, and (2) mechanisms and algorithms working on the described models in conformity with the modeling language.

The presented method can be seen as a 'method plug-in', enriching enterprise modeling frameworks to allow for compliance evaluation based on heat maps. Like a modeling method itself, the method plug-in consists of the main building blocks: modeling language, modeling technique, and mechanisms and algorithms, all of which are seamlessly integrated into a (possibly) established enterprise modeling method. In the following, the method is structured into a static component - the modeling language - and a dynamic component - the modeling technique and the required mechanisms/algorithms.

3.1 Static Component

The language for representing the relevant architecture artifacts, their interdependencies, and their relations to principles is described by its meta-model, i.e. '*the meta-model is a model of its corresponding modeling language*' [15]. The method (plug-in) can be applied to any existing meta-model in the fields of enterprise modeling. The only requirement is to extend the meta-model with the following meta-model extensions (if not already part of the given method).

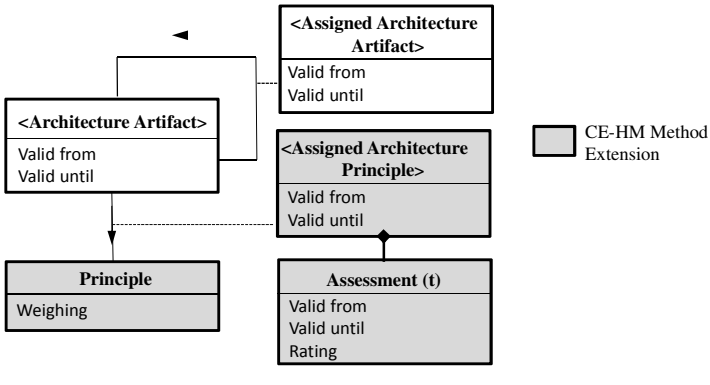

Fig. 1. Minimum Requirements on the Meta-Model

Besides the given modeling classes (which are part of the underlying modeling method we apply) for instantiating architecture artifacts (such as business processes, applications, and technology components) a modeling class representing principles is required. With *principles* we refer to control objectives, architecture principles or any

other concept constituting regulation codes, claiming compliance with regulations, laws or standards.

Principles are assigned to architecture artifacts via the relation type *Assigned Principle*. All modeling and relation classes have a time context, meaning that instances of these (relation) classes are valid only within a time frame (namely between *valid from* and *valid until*). Furthermore, principles are weighted regarding their importance. The rating-per-time interval of an architecture artifact in the context of a principle is defined via the construct *Assessment* of the relation class *Assigned Principle*. This allows for rating the compliance of an architecture artifact (considering the assigned principles) per evaluation cycle.

Fig. 2 exemplarily depicts an extract of TOGAF's core content meta-model [27] enriched with the CE-HM methods meta-model extension.

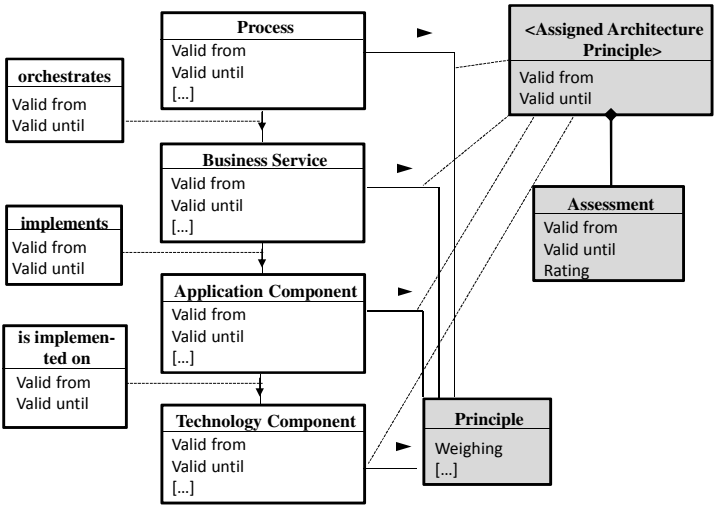

Fig. 2. Excerpt of the TOGAF9 Meta-Model

3.2 Dynamic Component

The (modeling) procedure – as one part of the dynamical component of the CE-HM method - defines the compliance evaluation processes, composed of the tasks *Define Scope and Configure Assessment*, *Conduct Principle Definition and Weighing*, *Conduct Data Acquisition*, *Assess Architecture Artifacts*, and *Conduct Analysis*.

Ideally, these tasks are integrated into the management processes of the organization. Responsibilities and stakeholders will typically differ from organization to organization. According to [12], *'the body responsible for governance will also normally be responsible for approving the architecture principles, and for resolving architecture issues'*. This body is here referred to 'Compliance Team'. The 'Architecture Artifact Owner' (e.g. application or process owners) are responsible for maintaining their architecture artifacts within an architecture repository. For a more detailed discussion on roles and stakeholders that are typically involved, we refer to [28].

Phase 1 - Define Scope/Configure Assessment. In this phase, the scope of the Compliance Evaluation effort is defined and the principles to comply with are determined. The compliance team may choose CobiT's control objectives [11] as the prime regulation code to comply with. In a next step the meta-models of the established enterprise modeling approaches are analyzed in respect of their relevance for the Compliance Management endeavor. If relevant architecture artifacts (and underlying modeling classes) are missing, existing meta-models and approaches need to be adapted.

Subsequently, *evaluation configurations*, representing the part of the meta-model (the perspectives) stakeholders are interested in, are defined. Each of these evaluation configurations conform to a directed acyclic path $EC = (M, R)$, comprising a set M of modeling classes (consisting of architecture artifacts and principles) and a set R of relations of the underlying meta-model. Principles equate to the end nodes of this directed path. In other words, the modeling classes of the underlying meta-model are put into hierarchy. Each modeling class (architecture artifact type) represents one level in the hierarchy and the modeling class *principle* represents the bottom level. Referring to our running example (see **Fig. 2**) the modeling class *business service* might be on meta-model level *n* and the subordinated modeling class *application component* is on meta-model level *n-1*.

Phase 2 - Conduct Principle Definition and Weighing. The second phase serves a twofold purpose: First, relevant principles are defined and integrated into the model. Consider for example CobiT's control objectives for Change Management, such as *AI6.1 Change Standards and Procedures*, *AI6.2 Impact Assessment*, *Prioritization*, and *Authorization* and *AI6.3 Emergency Changes*. Together these control objectives might form the principle *Apply Change Management* which is assigned to architecture artifacts of the type *application component* or *technology component*.

Second, the defined and agreed principles are weighted according to their importance for the organization. Weighing can be done e.g. by pairwise comparison of principles. Other more sophisticated methods are the Delphi method [10] or the Analytic Hierarchy Process (AHP) [22] – both widely accepted approaches for group decision-making. In the presented method each principle is weighted from 1 (minor importance) to 5 (high importance). As there is no limit on the relevant number of principles, indifference of assigned weights is allowed. This leads to the following definition:

$$\omega(p) \in \{1, 2, 3, 4, 5\},$$

with $\omega(p)$ being the function which returns the weight which has been assigned to a principle.

Phase 3 - Conduct Data Acquisition. In this phase the model, i.e. the architecture artifacts and their relations, is defined. Ideally data acquisition and maintenance is done on a regular basis and at least once for each compliance evaluation cycle. Process patterns on how to organize the data acquisition and maintenance can be found in [20]. Referring to these patterns we advocate a decentralized approach, where architecture artifact owners are responsible for data currency and completeness,

and the compliance team conducts periodic 'verification and audit' on the enterprise model. However, as we relate to institutionalized enterprise modeling initiatives of an organization, this certainly depends on the given enterprise modeling approaches.

Phase 4 – Assess Architecture Artifacts. In phase 4, the principles are assigned to architecture artifacts and each architecture artifact is assessed respectively in the context of the related principle. Again, we use a scale from 1 to 5, where 1 stands for being *non-compliant* and 5 for being *fully compliant* to the particular principle. This leads to the following definition:

$$\rho(a, p) \in \{0,1,2,3,4,5\},$$

with ρ() being the function which returns the rating of an architecture artifact 'a' in the context of a principle 'p'. The rating value null (0) implies that the relation between a and p has not been evaluated so far. There is no standardized way for defining the compliance levels. However, to ensure enterprise-wide consistency in the ratings it is recommended to (1) have a small and concerted team of reviewers (members of the compliance team), and (2) provide detailed instructions for assessing a specific principle to ensure traceability and organizational-wide reproducibility of conducted compliance assessments.

Take the above example of the principle *Apply Change Management* which might be related to architecture artifacts of the modeling class *application component* in respect of a particular evaluation configuration defined in phase 1. Changes to an application component (where the principle has been assigned to) need to be managed in conformity with this principle. Thus, these application components are assessed against the principle, respectively against the control objectives the principle consists of. The given assessment value indicates, whether changes to a concrete application component are always made in compliance with the principle. Hence, it is evaluated whether, upfront to changes to the application component, impact assessment and priorization is conducted, and whether the changes are authorized in accordance with the organization's stipulations. The control objectives the principle consists of can be understood as the detailed instructions necessary for ensuring traceability and reproducibility of the assessments.

Phase 5 – Conduct Analysis. Subsequently, in phase 5, the compliance evaluation of the organization is performed, delivering the compliance level (CL) of architecture artifacts on any level of the evaluation configuration. Compliance levels of bottom-level architecture artifacts are propagated to their superior architecture artifacts (in accordance with the evaluation configuration, defined in phase 1). Take the above example: The compliance level related to the principle *Apply Change Management* is assessed for a set of application components. As those application components are assigned to a higher-level business service, the fulfillment level of the very principle on business service level is determined by propagating the compliance levels to the higher-level business services. With the same approach compliance level of business processes can be determined (by propagation of the compliance levels of their subordinated business services). Hence, it can be stated, that a certain business process uses

business services, and the underlying application components of this business service comply with the principle *Apply Change Management* to a certain degree.

Based on the calculated compliance levels, views are generated and enriched with color coding (heat maps) to support decision-making related to compliance issues. The heat map approach can be applied to any type of viewpoint and to any architecture artifact (which is part of the evaluation configuration). We distinguish the following heat map types:

- **Status heat maps** represent the compliance status of architecture artifacts to identify weak spots and non-conformant parts of the organization at any point in time.
- **Alteration heat maps** illustrate significant improvement and worsening of compliance of architecture artifacts between two points in time.
- **Objective deviation heat maps** illustrate significant divergence between current and target compliance state of architecture artifacts. In many cases achieving compliance will be dependent on limited budgets and resources. Thus, organizations will define target values which will rise over time until reaching the required level. In exceptional cases the organization may even decide to accept non-compliance. The compliance team will be highly interested in seeing progress concerning the planned compliance level. Note: For this evaluation type, in phase 4, target values ($\rho_{\text{target}}(a, p, t)$) for compliance values need to be defined for each pair of architecture artifact and related principle. The meta-model must be extended accordingly.

Based on these heat maps the compliance team studies the enterprise in order to identify weak spots. Analysis takes place on any level of the enterprise, respectively on any meta-model level of the determined evaluation configurations. The compliance team uses drill-down functionality to clearly identify the weak spots and to set adequate measures.

Each of the three mentioned heat map types is based on mechanisms and algorithms for compliance evaluation and visualization. Each of these *compliance evaluation mechanisms* in turn builds on *basic mechanisms* which are primarily needed for putting the architecture artifacts and the principles under control. [19] discusses some of those basic mechanisms with focus on EA modeling, meant to be more generally applicable. Amongst others, mechanisms to organize version control of architecture artifacts, to establish and to maintain time-related views, and mechanisms for status management (e.g. release workflows) are defined. These mechanisms fully apply to the method at hand.

Mechanisms supporting time-related views are paramount to compliance evaluation, as compliance evaluations are performed repeatedly; this basic mechanism is briefly discussed, before we focus on the *compliance evaluation mechanisms*. Time-related views provide the capability for describing different states of architecture artifacts and their relations at different times. Hence current as well as former versions of the entire model (incl. architecture artifacts, principles and performed ratings) are traceable at any point in time. While an application component might be valid at one point in time (status 'productive'), at a later date it might become invalid (status 'retired'). This is not only true for architecture artifacts and principles, but also for relations between those architecture artifacts, as well as for their relations to principles.

[23] differentiates between two types of time versions: logical time vs. physical time. Time values used in the CE-HM method are considered as logical time – the time at which changes to architecture artifacts take place in the real world and the time a compliance rating refers to. The time at which the changes took place in the repository – physical time – will not be discussed in detail, although it is certainly relevant to keep compliance evaluations traceable. The meta-model (extension) discussed in section 3.1 considers and incorporates time-related views. Modeling classes and relation classes include the attributes 'valid from' and 'valid until' representing the timeframe during which an architecture artifact (or relation) exists (e.g. state 'productive'). The point of time at which the enterprise model is viewed, affects the visibility of architecture artifacts and their relations. It is obvious that the change of architecture artifacts comes along with the necessity for new appraisal of its conformity with the related principles. Hence, the assessment value needs to be time-related as well.

Evaluation Algorithms. In this section domain-specific evaluation algorithms for Compliance Evaluation are formalized. On modeling level, architecture artifacts are put into hierarchy in conformity with the above evaluation configurations on meta-model level, forming a directed acyclic graph with principles being the leaves (see phase 1).

For calculating the compliance levels for the status heat maps two alternative calculation methods are presented, namely the *Worst Case Rating* and the *Weighted Average Rating*.

Alternative 1 - Worst Case Rating: The values of worst rated principle are propagated to an architecture artifact (and from there to the higher-level architecture artifact).

The compliance level of an architecture artifact, which is directly related to one or more principles (architecture artifact on the bottom level of an evaluation configuration), is defined as follows:

$$\mathrm{CL}_{min}(\mathrm{a},\mathrm{t}) := \begin{cases} min_{\mathrm{p}\in\mathbb{P}}\ \rho(\mathrm{a},\mathrm{p},\mathrm{t}), & if\ \mathbb{P} \neq \emptyset\ and\ \rho(\mathrm{a},\mathrm{p},\mathrm{t}) \neq 0 \\ 0, otherwise \end{cases} \quad (1)$$

where $\mathbb{P}$ is the set of chosen principles relevant for the compliance evaluation run, and with ρ() being the function which returns the assessment value of a particular architecture artifact in the context of a particular architecture principle for the time (t) the compliance level evaluation is conducted. The compliance level for propagating the CL to the higher-level architecture artifacts is calculated as follows:

$$\mathrm{CL}_{\min}(\mathrm{a}^{\mathrm{n}},\mathrm{t}): = \begin{cases} \min_{\mathrm{a}^{\mathrm{n}-1}\in\{\mathrm{sub}(\mathrm{a}^{\mathrm{n}})\}} \mathrm{CL}_{\min}(\mathrm{a}^{\mathrm{n}-1},\mathrm{t}), & \text{if } \mathrm{sub}(\mathrm{a}^{\mathrm{n}}) \neq \emptyset \text{ and } \mathrm{CL}_{\min}(\mathrm{a}^{\mathrm{n}-1},\mathrm{t}) \neq 0 \\ 0, \text{otherwise} \end{cases} \quad (2)$$

with a^n representing an architecture artifact on level n and with sub() being the function which returns all subordinated architecture artifacts of a particular architecture artifact.

Alternative 2 - Weighted Average Rating: The ratings on each level of the evaluation method are averaged and propagated to the particular higher-level architecture artifact.

The compliance level of an architecture artifact, which is directly related to a principle (architecture artifact on the bottom level of an evaluation configuration), is defined as follows:

$$\mathrm{CL}_{\mathrm{avg}}(a,t) \coloneqq \begin{cases} \dfrac{\sum_{p\in\mathbb{P}} \rho(a,p,t) \times \omega(p)}{\sum_{p\in\mathbb{P}} \omega(p)}, & \text{if } \mathbb{P} \neq \emptyset \text{ and } \rho(a,p,t) \neq 0 \\ 0, \text{otherwise} \end{cases} \tag{3}$$

with ω() being the function which returns the weight assigned to the principle, and $\mathbb{P}$ and ρ() defined as above. The formula for propagating the CL to higher-level architecture artifacts in case of weighted average rating is defined as follows:

$$\mathrm{CL}_{\mathrm{avg}}(a^n,t) \coloneqq \begin{cases} \dfrac{\sum_{a^{n-1}\in\{\mathrm{sub}(a^n)\}} \mathrm{CL}_{\mathrm{avg}}(a^{n-1},t)}{\sigma(a^n,t)}, \text{if } \sigma(a^n,t) \neq 0 \\ 0, \text{otherwise} \end{cases} \tag{4}$$

where $\sigma(a^n,t) \coloneqq \#\left\{a^{n-1} \in \mathrm{sub}(a^n) \middle| \mathrm{CL}_{\mathrm{avg}}(a^{n-1},t) \neq 0\right\}$ with a^n representing an architecture artifact on level n of a particular evaluation configuration.

Based on the calculations for status heat maps, evaluation values for *alteration heat maps* and *objective deviation heat maps* (introduced in phase 5) are calculated. **Alteration heat maps** are calculated as follows:

$$\mathrm{CL}_{\Delta\mathrm{Alteration}}(a,t_1,t_2) \coloneqq \mathrm{CL}(a,t_1) - \mathrm{CL}(a,t_2) \tag{5}$$

For calculating the evaluation values for **objective deviation heat maps** compliance levels of the architecture artifacts at some point in time need to be compared with the actual planned target values. The following function applies:

$$\mathrm{CL}_{\Delta\mathrm{DEVIATION}}(a,t) \coloneqq \mathrm{CL}_{\mathrm{plan}}(a,t) - \mathrm{CL}_{\mathrm{as-is}}(a,t) \tag{6}$$

where $\mathrm{CL}_{\mathrm{as-is}}(a,t)$ represents the actual compliance level at some point in time and $\mathrm{CL}_{\mathrm{plan}}(a,t)$ represents the planned compliance level at some point in time, and the calculation of $\mathrm{CL}_{\mathrm{plan}}(a,t)$ is done analogous to $\mathrm{CL}_{\mathrm{as-is}}(a,t)$.

Algorithms for Color Coding. In order to visualize the calculated compliance levels (status, alteration and deviation) the given shapes of the architecture artifacts (defined in the modeling language) are colored using specific color progressions. We use bipolar color progressions, which are, according to [21], typically used for mapping temperatures. A color progression from dark red (indicating non-compliant architecture artifacts) to dark green (indicating fully compliant architecture artifacts) with yellow in the center is used. Following the recommendation of [21] five hue categories are used, as the authors state that the human eye can easily distinguish at maximum seven hues.

The algorithms for applying the colors considers this recommendation by putting evaluation results into intervals, with each interval assigned to a color of the color progression from red to green. In the following status heat maps including color codes evaluated via weighted average method are defined exemplarily. In this case the possible range for compliance level values is defined from 1 to 5. With the span width of 5 – 1 = 4, and with five planned intervals the required interval size is 4/5 (= 0.8). The following function specifies the color of the graphical representation of the architecture artifacts at a given point in time:

$$\text{colour}(a,t) := \begin{cases} \text{red, if } 1 \le \text{CL}(a,t) < 1.8 \\ \text{organge, if } 1.8 \le \text{CL}(a,t) < 2.6 \\ \text{yellow, if } 2.6 \le \text{CL}(a,t) < 3.4 \\ \text{lightgreen, if } 3.4 \le \text{CL}(a,t) < 4.2 \\ \text{green, if } 4.2 \le \text{CL}(a,t) \le 5 \\ \text{grey, if } \text{CL}(a,t) = 0 \end{cases} \tag{7}$$

View Generation. For illustration purposes, we apply the heat maps to any viewpoint available in the method at hand. For automatic generation of views layout algorithms (see specific mechanisms and algorithms) are used. In conformance to the running example at hand heat maps are assigned to the three main viewpoints defined in TOGAF: (1) diagrams (supporting presentation of architecture artifacts and relations in a visual way suitable for stakeholder communication), (2) matrices (supporting presentation of relationships between architecture artifacts), and (3) catalogues (lists of architecture artifacts). An illustrative example is given in **Fig. 3**. However, the discussed mechanisms work for any other viewpoint like those defined in [3].

4 A CE-HM Prototype Based on ADO*xx*

This section presents the prototypical implementation of the CE-HM method based on the meta-modeling platform ADO*xx*. Based on its meta-modeling capabilities, ADO*xx* allows for implementing any enterprise modeling framework. It incorporates collaboration features for data acquisition and on-going data maintenance, a central repository, and mechanisms for controlling relevant architecture artifacts. By utilizing the platform's open APIs the discussed evaluation mechanisms, and heat maps for compliance evaluation have been prototypically implemented.

Fig. 3 depicts a screenshot of the tool. The user interface is subdivided into three areas: (1) The modeling surface presenting graphical viewpoints, such as diagrams and matrices (diagram and matrix viewpoints), (2) the object catalogue (catalogue viewpoints), and the panels for choosing (3a) evaluation configurations (including relevant principles) as well as (3b) a time-slider for choosing the relevant point in time. On the modeling surface an automatically generated cluster map – as one example of a viewpoint in ADOxx - is shown. The visualized clusters (rectangles) are colored automatically in accordance with the underlying evaluation mechanism.

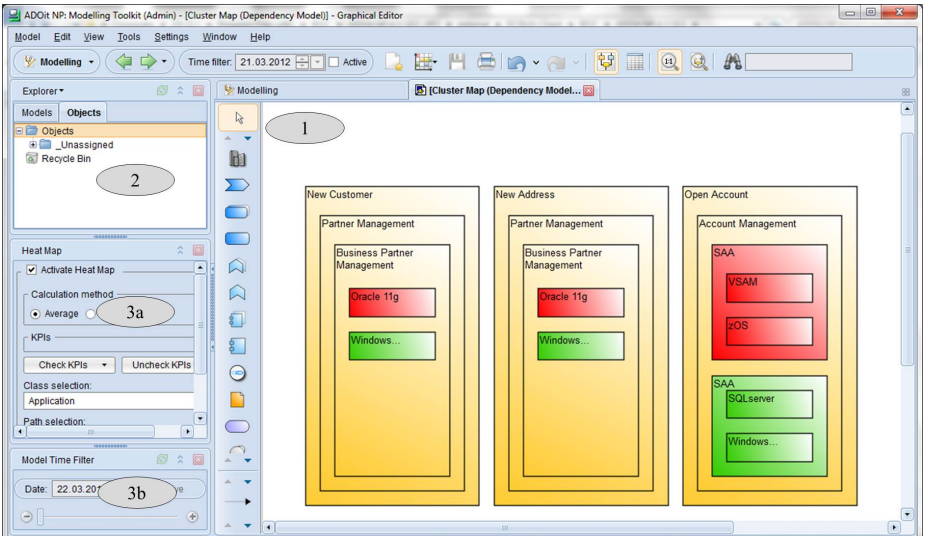

Fig. 3. Reference Implementation based on ADO*xx*

5 Conclusion

The CE-HM method and its prototypical implementation based on a meta-modeling platform are presented. The method supports compliance evaluation in an effective and efficient manner, by building on established enterprise modeling initiatives of an organization. For illustration of the compliance degree of architecture artifacts a sophisticated heat mapping approach is applied. The presented mechanisms evolved step by step during compliance evaluation and enterprise modeling projects.

The suitability of the presented method certainly needs to be proven in a structured manner. We are working on the evaluation of the CE-HM method in an application domain, namely the banking area. The method will be used for measuring and planning compliance of enterprise architectures based on self-imposed architecture principles comparable with those of TOGAF [27]. First evaluation results show the importance of a consistently maintained architecture repository. An approach planned to be evaluated in the next step is the integration of further information bases, e.g. of the organization's configuration management system (CMS). Maintenance procedures of the entire architecture repository and the Compliance Management need to be aligned. This might be followed by resistance of the different stakeholders, not willing to provide transparency in their domains. It needs to be evaluated, whether the presented scoring approach and the propagation rules prove reasonable in terms of (1) expressiveness of the gained heat maps, (2) efforts related, e.g. for weighing principles and grading compliance degrees, and (3) most importantly, acceptance within the organization. Our evaluation approach will define and evaluate key performance indicators (KPIs), e.g. the 'reduction in time/effort for performing compliance evaluation', and indicators evaluating the reduction in workload regarding compliance

evaluation efforts. Soft indicators, such as improved communication means by reusing viewpoints familiar to the stakeholders, as they are part of existing enterprise modeling initiatives, will be collected and evaluated via structured interviews.

Acknowledgements. Many thanks to the reviewers for providing us with constructive criticism, all of which have been carefully considered.

References

1. van Bommel, P., et al.: Architecture Principles - A Regulative Perspective on Enterprise Architecture, vol. P-119 GI, pp. 47–60 (2007)
2. Buckl, S., et al.: A Pattern based Approach for constructing Enterprise Architecture Management Information Models, Universitaetsverlag Karlsruhe, pp. 145–162 (2007)
3. Buckl, S., et al.: Enterprise Architecture Management Pattern Catalog. Release 1.0, Garching b. München, Germany (2008), http://srvmatthes8.informatik.tu-muenchen.de:8083/file/EAMPatternCatalogV1.0.pdf (access: October 15, 2008)
4. Campbell, P.L.: An Introduction to Information Control Models. Sandia National Laboratories report SAND2002-0131, Albuquerque, New Mexico (2003)
5. US Department of the Treasury - Chief Information Officer Council: Treasury Enterprise Architecture Framework (TEAF). Version 1 (2000)
6. FEA Working Group: E-Gov Enterprise Architecture Guidance (Common Reference Model) Version 2.0 (2002)
7. Fischer, C., et al.: What Is an Enterprise Architecture Design Principle? - Towards a Consolidated Definition. In: Proceedings of the 2nd International Workshop on Enterprise Architecture Challenges and Responses, Yonezawa, Japan (2010)
8. Frank, U.: The MEMO Meta Modelling Language (MML) and Language Architecture. In: ICB Research Report 24, Institute for Computer Science and Business Information Systems (ICB), Germany (2008), http://www.icb.unidue.de/fileadmin/ICB/research/research_reports/ICBReport24.pdf (access: November 12, 2010)
9. Ghanavati, S., et al.: Comparative Analysis between Document-based and Model-based Compliance Management Approaches. In: RELAW 2008, Barcelona, Catalunya, pp. 35–39 (2008)
10. Helmer, I., Rescher, N.: On the Epistemology of the Inexact Sciences. Management Science 6(1) (1959)
11. IT Governance Institute: COBIT. Version 4.1, IT Governance Institute, http://www.isaca.org/downloads (access: December 31, 2010)
12. IT Governance Institute: Mapping of Togaf 8.1 with CobiT 4.0, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Mapping-Mapping-of-TOGAF-8-1-With-COBIT-4-0.aspx (access: August 15, 2011)
13. Karagiannis, D., et al.: Open Models Initiative Feasibility Study, http://cms.dke.univie.ac.at/uploads/media/Open_Models_Feasibility_Study_SEPT_2008.pdf (access: January 23, 2011)
14. Keller, W.: Using Capabilities in Enterprise Architecture Management, Version of 2009-12-18, http://www.objectarchitects.biz/ResourcesDontDelete/CapabilityBasedEAMWhitepaper.pdf (access: April 20, 2010)

15. Karagiannis, D., Kühn, H.: Metamodelling Platforms. In: Bauknecht, K., Tjoa, A.M., Quirchmayr, G. (eds.) EC-Web 2002. LNCS, vol. 2455, p. 182. Springer, Heidelberg (2002)
16. Lankhorst, M.: Enterprise Architecture at Work: Modelling, Communication and Analysis. Springer, Berlin (2005)
17. Microsoft Services: Microsoft Motion Heat Mapping Tool, http://blogs.microsoft.co.il/files/folders/2034/download.aspx (access: December 23, 2010)
18. McCarthy, W.E.: An entity-relationship view of accounting models. The Accounting Review 54(4), 667–686 (1979)
19. Moser, C., et al.: Business Objectives Compliance Framework. Mechanisms for Controlling Enterprise Artifacts, vol. 127, pp. 73–88. GI (2008)
20. Moser, C., et al.: Some Process Patterns for Enterprise Architecture Management, vol. 150, pp. 19-30. GI (2009)
21. Robinson, et al.: Elements of Cartography, 6th edn. John Wiley & Sons, New York (1995)
22. Saaty, T.L.: Decision Making for Leaders – The Analytic Hierarchy Process for Decisions in a Complex World, 3rd edn. RWS Publishing, Pittsburgh (2001)
23. Sciore, E.: Versioning and Configuration Management in an Object-Oriented Data Model. VLDB Journal (3), 77–106 (1994)
24. Silveira, P., et al.: On the design of compliance governance dashboards for effective compliance and audit management. In: Proc. of the 3rd Workshop on Non-Functional Properties and SLA Management in SOC, NFPSLAM-SOC 2009, pp. 208–217 (2009)
25. Shneiderman, B.: The eyes have it: A task by data type taxonomy for information visualizations. In: Proc. IEEE Symposium on Visual Languages, Boulder, Colorado, pp. 336–343 (1996)
26. Strecker, S.: Toward modeling constructs for audit risk assessment: Reflections on internal controls modeling, vol. 171, pp. 131–148. GI (2010)
27. TOGAF: The Open Group Architecture Framework, Enterprise Edition. Version 8.1.1, http://www.opengroup.org/architecture/togaf8-doc/arch/ (access: August 15, 2007)
28. Vicente, P., Mira da Silva, M.: A Business Viewpoint for Integrated IT Governance, Risk and Compliance. In: Services, 2011 IEEE World Congress on Services, Washington, DC, USA, pp. 422–428 (2011)
29. El Kharbili, M., et al.: Towards a Framework for Semantic Business Process Compliance Management. In: The Impact of Governance, Risk, and Compliance on Information Systems (GRCIS), Montpellier, France. CEUR Workshop Proceedings, vol. 339, pp. 1–15 (2008)
30. Popova, V., Sharpanskykh, A.: Formal Modelling of Organisational Goals Based on Performance Indicators. Data & Knowledge Engineering 70(4), 335–364 (2011)