Systematic Elaboration of Compliance Requirements Using Compliance Debt and Portfolio Theory

Bendra Ojameruaye and Rami Bahsoon

University of Birmingham, UK
{Beo136,r.bahsoon}@cs.bham.ac.uk

Abstract. [Context and motivation] Eliciting compliance requirements often results in requirements, which might not be satisfied due to uncertainty and unavailability of resources. The lack of anticipation of these factors may increase the cost of achieving compliance. **[Question/problem] M**anaging compliance is an investment activity that requires making decisions about selecting the right compliance goals under uncertainty, handling the obstacles to those goals and minimising risks. **[Principal ideas/results]** (1) We define the concept of technical debt for managing compliance and we explore its link with obstacles to compliance goals. (2) We propose goal-oriented method and obstacles handling with a portfolio-based thinking for systematically managing obstacles and refining compliance goals. **[Contribution]**We use an exemplar to illustrate and evaluate the approach. The results show that our approach can provides analysts and compliance managers with an objective tool to assess and rethink their investment decisions when elaborating compliance requirements.

Keywords: Compliance requirements, compliance debt, Economics-driven software Engineering.

1 Introduction

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications [1]. Security requirements need to be aligned with the relevant laws and other prevailing regulations to control compliance and non-compliance issues; conversely, compliance is one of the driving factors for eliciting security requirements. Though the correlation between compliance and the likelihood of security breaches is unclear, data from Verizon's PCI compliance report shows that organisations that suffered data loss, as a common example of a security breach, were much less likely to be compliant.

While compliance goals capture desired properties, obstacles to those goals capture undesirable ones, which are likely to cause situations of incompliance. The violation may place the system and the organisation at risk. Managing compliance is ultimately an investment activity that requires value-driven decision making – about selecting the right compliance goals and handling the obstacles to those goals for mitigating risks. Analysts and managers often disagree about decisions on how to invest limited resources into compliance goals that are crucial to the business sustainability as they

C. Salinesi and I. van de Weerd (Eds.): REFSQ 2014, LNCS 8396, pp. 152–167, 2014.

do not generate revenue and their value tends to be invisible. The value is usually questioned and the situation is aggravated in organisations that must balance very limited resources with requirements that have visible value chain. It has been acknowledged that the selection of requirements have an impact on the system's success [1] [2]. Consequently, the choice of requirements selected and how obstacles to those requirements are resolved will significantly determine the extent to which the compliance goals are achieved along with their cost and likely risks.

The need to prioritise and resolve obstacles for the compliance goals is necessary to manage cost, create value, sustain the solution and reduce risk. Though it could be possible to use existing requirements prioritisation techniques to prioritise obstacles, such as the Analytical Hierarchy Process (AHP) [3] [4], these techniques do not clearly include uncertainty and incomplete knowledge of the real world [5]. Factors such as minimising cost and risk generally have a higher impact on creating value [5]. The management of compliance goals and their obstacles handling shall anticipate for uncertainty, cost, incomplete knowledge, likely risks and the associated trade-offs.

The novel contribution of this paper is as follows. We introduce the concept of *Compliance Debt*. Compliance Debt is a form of a technical debt, which is result of neglected compliance when engineering requirements of software. We propose an economics-driven solution, which elaborates on the notion of obstacles handling in goal-oriented requirements engineering by using portfolio-based thinking and compliance debt analysis to systematically manage compliance goals and their obstacles. This stems from the necessity to anticipate potential hindrances that may block the fulfilment of the compliance goals and to resolve those obstacles at the best cost with minimum risk, while accounting for uncertainty. In this context, we posit that obstacles and their resolution decisions may introduce compliance debt that needs to be managed for creating value and mitigating risks. One way to reason about compliance debt in relation to goals and obstacles is to characterise it as the gap between what level of compliance can be achieved with the available resources and the hypothesised "ideal" environments, where the goals are successfully achieved. In addition, obstacles which can be temporarily tolerated can be deemed as compliance debt, which needs to be managed for risk. In finance, a portfolio denotes a collection of assets (investments) by an investor, usually used as a strategy for minimising risk and maximising returns [6]. The goal of modern portfolio theory is to select the combination of assets using a formal mathematical procedure that can minimise risk for an expected level of return on investment while accounting for uncertainty of the real world. This can be applied to the process of managing compliance goals and obstacles management, where analysts make decisions on what compliance obstacles are most critical and likely to expose the business into risk. Likely risk will also inform investment decisions in handling the obstacles for compliance. Portfolio has been cited as one of the promising techniques for predicting and managing compliance debt in software engineering. Our portfolio-based approach determines the optimum selection of obstacles that needs to be managed for risks along with the compliance debt that can be tolerated. Combining goals and obstacles analysis with portfolio-based analysis provide systematic means for elaborating compliance requirements, handling their obstacles and likely compliance debt. The approach is value driven, risk-aware, and systematic; it leverage on influential work in goal-oriented requirements and obstacles handling. It uses portfolio thinking to make the link between obstacles, risks and compliance debt explicit and transparent to compliance mangers and security requirements engineers. The approach allocates resources to resolving obstacles as well as looks at their resolution tactics and the associated compliance debts, risk and value trade-offs. The objective is to inform the decision of investment in compliance, derive more realistic compliance requirements based on their economics, risks and compliance debt.

The remainder of this paper is organised as follows: Section 2 provides the motivation and background material on goal oriented requirement engineering, obstacles, compliance debt and portfolio management. Section 3 explores the link between compliance debt and obstacles and presents a modified obstacle analysis technique that integrates portfolio reasoning and compliance debt management. Section 4 evaluates the effectiveness of our approach using an example. Section 5 concludes the paper and explores directions for future work.

2 Motivation and Related Work

We refer to closely related work to motivate the need for our approach. We explore concepts, which are necessary for understanding our contribution.

2.1 Managing Compliance Using Goal-Driven Requirement Engineering

Organizations' heavy reliance on information systems (IS) requires them to manage the risks associated with those systems. Today, risks related to information security are a major challenge for many organizations, since these risks may have dire consequences, including corporate liability, loss of credibility, and monetary damage [7]. Ensuring information security compliance has become one of the top managerial priorities in many organizations [8]. The need for compliance arises when stakeholders establish that there is a need to operate in agreement with established laws, regulations, standards, and specifications [9] so as to protect themselves from any risk, cost or loss of value involving the consequences of non-compliance. Compliance goals express this need, describing the risk to be prevented. It is vital to elicit from these regulations and standards, prioritised information security compliance requirements that can be satisfied with the available resources. These requirements shall respond stakeholders' needs.

Compliance requirements can be considered as non-functional or quality requirements. These requirements do not have simple true or false satisfaction criteria; rather their level of satisfaction can vary [10]. Although compliance requirements are crucial to the business sustainability, they do not have clear link to revenue generation. Henceforth, the benefits and returns of compliance investments are difficult to comprehend and visualize. The value is usually questioned and the situation is intensified in projects that must balance very limited resources. Satisfying a compliance requirement can depend on the risk value attached to not complying with that requirement.

Furthermore, compliance is difficult to measure as it can crosscut many concerns within a system. This makes the measurement for compliance hard to simplify and bound the problem space. Furthermore, compliance involves a dynamic mix of changing regulations, interaction between different stakeholders in the organisation. Another challenge, which faces compliance managers is ensuring that the specified compliance requirements are neither too idealist nor too weak with respect to business goals [11] as well as finding trade-offs between achieving compliance requirements and the available resources.

Goal-orientation is a widely used approach for managing requirements [11]. *Van Lamsweerde* [12] presented a detailed study of Goal-oriented requirements engineering. A goal is an objective or a "*statement of intent that a system should satisfy*" [12] and requirements are represented in the form of goals. Goals range from high-level business objectives, to well-defined compliance properties. Agents are components, which are capable of performing operations to satisfy goal [11]. In requirement engineering, goal driven approaches focuses on why the system needed, expressing the justification for a specific requirement.

While goals capture the objectives to be satisfied, obstacles capture undesired properties that may prevent the goal from being satisfied [13] [11]. An obstacle obstructs a goal if the obstacle negates the goal in the domain [13].

There is need to apply proven requirement engineering methods and demonstrate how best to apply these methods within the context of analysing legal regulatory requirements. Requirements for compliance are derived from a variety of sources and the need to include security policies among those information sources has been recognized as important [14]. Researchers have investigated different methods for analysing security requirements using goals [15] [16], with more recent work focusing on the extraction of requirements from security policies [14] [17]. The work of Anton and Breaux [14] takes this further by systematically extracting rights and obligations from legal texts. These techniques recognise the need to manage compliance requirements; however, none of these attempts to have linked compliance to value creation under uncertainty.

An important contribution is the work of Burgemeestree et al [18], they discussed how value-based augmentation theory can be applied to formalising compliance decision. This approach models a control system and the justification for compliance decisions/choosing control in a state transition diagram. It operationalizes legislations into control objectives and identifies the control measures. This approach also takes into account the organisational context of the legislation. Although this approach helps to formalise compliance decisions, it does not present a value-based approach for managing uncertainty

2.2 Portfolio Management and Requirements

Modern Portfolio theory [19] was introduced in 1952 by Harry Markowitz. The goal of modern portfolio theory is to select the combination of assets using a formal mathematical procedure that can minimise risk for an expected level of return on investment while accounting for uncertainty of the real world. In finance, a portfolio denotes a collection of weighed compositions of assets (investments) by an investor, usually used as a strategy for minimising risk and maximising returns.

Portfolio theory attempts to show the benefits of holding a diversified portfolio of risky assets rather than assets selected individually. The theory can also assist in determining the optimal strategy for diversification of assets to minimise risk and maximise return. This is can be linked to the process of analysing compliance obstacles, where analysts make decisions on which obstacles should be resolved given a certain amount of resources for minimum risks.

In modern portfolio theory, the risk of a portfolio R_P is determined by the individual risks associated with each asset R_1, the weight of each asset in the portfolio W_1 and the correlations between the assets P_{IJ}. These correlation coefficients range from -1 (a perfectly negative correlation between the two items) to +1 (a perfectly positive correlation and 0 indicates no relationship between the items.

$$Rp = \sqrt{\sum_{i=1} w1^2 R1^2 + \sum_{i=1}^{m} \quad \sum_{j=2}^{m} WiWjRiRjPij} \tag{1}$$

The link between selection of requirements and market value using portfolio has been first explored by [5]. They proposed market driven, systematic, and more objective approach to supplement the selection of requirements, which accounts for uncertainty and incomplete knowledge in the real world using portfolio reasoning [5]. Our use of portfolio is different: We identify an optimal portfolio of obstacles to be resolved along with their resolution tactics. We employ the analysis on the gaol and elaboration levels. We explicitly look at linking compliance goals and their resolutions to risk and compliance debt.

2.3 Technical Debt, Compliance Debt, Obstacles and Portfolio

Cunningham used the Technical debt metaphor in his 1992 report [4] to describe a situation in which long-term code quality is traded for short-term gain. The link between technical debt and financial analysis using portfolio analysis has been explored [20], Seaman et al. discussed four decision approaches to deal with Technical debt: Cost-Benefit Analysis, Analytic Hierarchical Process (AHP), Portfolio Management Model and Options. In addition, [21] proposed an approach using portfolio theory to diversify the allocation of web services in the cloud. However, none of the available work has looked at compliance debt as a type of technical debt in compliance management and goal-obstacles analysis for compliance. The concept of linking compliance debt as types of technical debt to compliance goals and their obstacles using portfolio thinking is novel. We identify an *optima*l portfolio of obstacles to be resolved. We then quantify the likely compliance debt that may be incurred by selecting different obstacle resolution tactics when elaborating compliance goals and understanding the link to value.

3 Analysing Compliance Obstacles Using Portfolio Reasoning and Compliance Debt.

Brown el al. opined that "like financial debt, compliance debt incurs interest payments in the form of increased future costs owing to earlier quick and dirty design and implementation choices" [22]. The term compliance debt has been developed broadly and has covered wider aspects associated with the overall systems development life cycle.

Unlike previous work, we introduce a new dimension of using compliance debt as a decision factor for elaborating and managing compliance goals through obstacles handling. We incorporate compliance debt analysis at the goal refinements and obstacles resolution levels. While compliance goals capture desired objectives, obstacles to those goals capture undesirable properties that may obstruct those goals, which are likely to cause situations of incompliance. The violation may place the system and the organisation at risk. Compliance debt can inform the obstacle analysis process and the decision for investing in resolving obstacles at early stages of the requirements and the goal definition and elaboration lifecycle. Our objective is to avoid inappropriate selection of obstacles resolution decisions that are not value- and risk-driven and debt-aware. The key principle here is to tackle and manage the increased and unjustified compliance debt, which can be associated with the selection and consequently the inappropriate resolution tactics of the compliance obstacles, expressed in risk, cost and value. We assume that compliance debt can vary with the different obstacle resolution tactics that can be used for realising compliance. Each tactic can deliver its own trade-offs for risk, value, cost and compliance debt reduction.

3.1 Reasoning of Compliance Debt in Handling Obstacles for Compliance

We now define relationship between obstacles and compliance debt more precisely; the integration of compliance debt and portfolio reasoning as an obstacle analysis and resolution method is then discussed. We suggest a predictive approach for anticipating and managing compliance debt at the goal refinements and obstacle analysis stages. A predictive approach can be applied during the early stages of the engineering process to predict the debt, its impact on compliance, when it will be incurred, when it will pay off, and the interest if any. Classical approaches to managing compliance debt in software development lifecycle tend to be retrospective. Unlike retrospective approaches, predictive approaches allow planning.

Compliance debt in compliance management can be traced back to requirements – the way requirements are engineered, elicited, selected, prioritised and analysed. Compliance is difficult to measure as compliance policies are often open to different interpretations and are subjective. This makes it difficult to simplify and bound the problem space. Compliance involves a dynamic mix of changing regulations and lack of insight into historical performance of security operations as well as the interaction between different stakeholders in the organisation. As a result, the solutions chosen to aid compliance may not completely meet the requirements. Fixes may be required reengineer the solution to better meet requirements or compliance will be required introducing compliance debt that needs to be managed. This particularly makes the process of goals elaboration for compliance through obstacles resolution prone to compliance debt. Compliance debt can be linked to the resolution tactics used and their appropriateness, resources used, expertise, etc. Moreover, the absence of historical performance data, metrics and benchmarks for compliance makes managing and assessing compliance, resolving obstacles for compliance a mere difficult exercise. The trial and error handling of the process can introduce unnecessary compliance debt in situations when the costs of managing compliance (capital and operational costs) tends exceed that of the generated value and the risk tends to prevail. Furthermore, compliance debt can occur accidentally when poor and quick decisions for managing and resolving obstacles for compliance may add a value in the short-term but can introduce long-term debt. Compliance debt may be intentionally incurred when corrective measures for compliance becomes unavoidable.

One way to understand compliance debt in relation to goals and obstacles is to characterise it as the gap between what can be achieved with the available resources and the hypothesised "ideal" environments, where the goals are successfully achieved. Uncertainty about whether or not a decision is appropriate or will have an associated penalty may incur a compliance debt. In this sense, compliance debt can be considered as a particular type of risk; the problem of managing compliance debt boils down to managing risk and making informed decisions [20]. Obstacles resolution decisions are examples of these decisions. Obstacles can be resolved by generating alternative resolutions and selecting one resolution among the different alternatives. Compliance debt may also occur when the obstacle is tolerated and nothing is done to completely resolve the obstacles and consequently the likely risks. If the risk materializes, the system may accumulate interest signalling debt. We can attribute compliance debt in obstacle analysis to different obstacle resolution tactics, this can also be seen as the cost of reducing or tolerating the obstacle to the cost of eliminating that obstacle. We can manage compliance debt at the obstacle level by switching from one obstacle resolution alternative to another, while considering cost, risk and value.

3.2 Portfolio-Based Approach for Managing Compliance Debt

We now examine the integration of portfolio reasoning and compliance debt in obstacle analysis and resolution. Once obstacles have been identified, they need to be assessed and prioritised. We assert that the risk value of an obstacle is the product of the likelihood of the obstacle occurring and its criticality. We describe an approach for allocating resources for resolving obstacles as well as selecting the obstacle resolution tactic by considering the amount of compliance debt that each obstacle may incur and the interest that might accumulate as the deciding factors.

Consider a compliance goal that has been specified and its obstacles have already been identified, the basic steps of our value and risk-aware approach for elaborating the compliance requirements can be stated as follows:

- **Prioritise Obstacles that Needs to be Resolved:** The fundamental component of this approach is to put the obstacles in a "list". Each item includes the obstacle, the goal it obstructs, and estimates of the *expected interest amount* and *interest probability* as well as an estimate of the *principal.* The principal refers to the cost required to completely resolve the obstacle, the interest probability refers to the likelihood that the obstacle will occur and the interest amount is the extra cost that will be required if this obstacle is not resolved as well as the cost of the consequence. Since it is uncertain that extra cost will be required, we use expected interest amount and interest probability to capture the uncertainty. Every obstacle has a risk value. We can prioritise the obstacles by quantifying the risk value of the obstacles. The value of an obstacle is the product of the likelihood of the obstacle occurring and the criticality.

$$R_O = I_P * I_A \tag{2}$$

$$V_O = P * I_P * I_A \tag{3}$$

Where R_o is the risk value of the obstacle, V_O is the value of the obstacle, P is the principal; I_P is the likelihood that the obstacle will occur and I_A the extra cost that will be needed if this obstacle is not resolved as well as the cost of the consequence. For simplicity, these (P, I_P , I_A) are assigned values of high (3), medium (2), or low (1). Initially, when a debt item is created, the principal, expected interest amount, interest standard deviation and correlations with other debt items can be estimated subjectively according to the maintainer's experience. These rough estimates can be adjusted later using historical data. Historical effort data can be used to achieve a more accurate estimation as the more accurate and detailed the data is, the more reliable the approach.

• **Determine the Weight of Each Asset in the Portfolio:** Some obstacle may be resolved to a certain degree but may not fully. In order to optimize the global risk of the portfolio and find the optimum solution, we need to find how much weight should be invested in resolving each obstacle to construct a low risk portfolio. This can be calculated using a non-linear optimisation technique or the AHP [3].

• **Determine the Correlation Coefficient:** Since we will apply the Modern Portfolio Theory model to decision making in selecting and prioritising the obstacles, we need to include "correlations with other debt items" as a property to be estimated. We use the idea of correlation coefficients to represent the correlation between two obstacles, these correlation coefficients range from -1 (a perfectly negative correlation between the two items) to +1 (a perfectly positive correlation). For simplicity, we speculate that the correlation coefficient would be either1, 0, or -1 for most pairs of the obstacles. For more accurate analysis, the correlations could be determined through dependency analysis.

•**Evaluate the Portfolio of Obstacles to be Resolved:** Since compliance requirements do not have simple true or false satisfaction criteria; but are satisfied up to a level [10], we can determine how well the obstacles to a goal needs to be resolved with the available resources. With the measurements of the value of the obstacles as described above, all input information for the portfolio approach is ready. We can start making decisions using the portfolio approach. Each obstacle O_l has a risk value R_l, a cost P_l and W_l as the weight of the obstacle. Based on these values, we can then decide on how many instances of the obstacles to the goal need to be resolved so that global risk of the goal being obstructed is reduced.

$$\sum_{i=1} \mathrm{Ep} = 1 \tag{4}$$

$$Rp = \sqrt{\sum_{i=1} w1^2 R1^2 + \sum_{i=1}^{m} \quad \sum_{j=2}^{m} WiWjRiRjPij} \tag{5}$$

• **Evaluate and Select the Best Resolution Tactic:** Evaluating and selecting the best resolution tactic is a core activity for resolving the obstacles in the compliance requirement elaboration process. We evaluate the resolution alternatives by considering the amount of compliance debt that each resolution tactic may incur as the deciding factor. We calculate and assign the compliance debt of each alternative, so that the sum of the alternatives is 1.

• As with selecting the obstacles, we put the resolution tactics in a "list". This contains items, each of which represents an obstacle resolution tactic for resolving a specific obstacle. Each item includes the goal, the obstacle which it is meant to resolve, the resolution tactic, an estimate of the principal, estimates of the expected interest amount and interest probability. The principal refers to the cost required by the resolution tactic; the interest is the extra cost that will be needed if this resolution tactic does not fully mitigate the risk of the obstacle as well as the cost of the consequences. For simplicity, these (principal, interest probability, and interest amount) are assigned values of high (3), medium (2), or low (1).

• We formulated the value of the resolution tactic using the following equation:

$$\mathrm{R_T} = \mathrm{P} * \mathrm{I_P} * \mathrm{I_A} \tag{6}$$

Where $\mathrm{R_T}$ is the cost of the resolution tactic, P is the principal, $\mathrm{I_P}$ is the interest probability and $\mathrm{I_A}$ is the interest amount.

• From our earlier explanation of the compliance debt metaphor in relation to goals and obstacles as the gap between what can be achieved with the available resources and the hypothesised "ideal" environments where the goals are successfully achieved. We formulate the value of the compliance debt using (6):

$$\mathrm{T_D} = \mathrm{IR_T} - \mathrm{R_T} \tag{7}$$

Where $\mathrm{T_D}$ is the compliance debt, $\mathrm{IR_T}$ is the cost of an "ideal" resolution tactic and $\mathrm{R_T}$ is the cost of the selected resolution tactic. The ideal value is context dependent. The ideal value is application and business dependent. Assuming security engineers and architects voted for Tactic *IR* as the ideal resolution tactic. $\mathrm{T_D}$ for any other tactic is calculated as the gap between value of tactic k ($\mathrm{IR_T}$) and the value of the tactic in question.

This technique provides decision makers with a metric for reasoning about compliance debt in conjunction with obstacle resolution tactics. The process of goal refinement and elaboration through obstacle analysis and handling is iterative and continuous. Our technique can inform the decision for further refinements for compliance and the need for further resolutions of the obstacles for managing debt.

The metric can also inform the desirable stopping criteria for the refinements and resolution processes. Using compliance debt and portfolio thinking, we put risk, added value and cost in the heart of refinements and elaboration process.

4 Illustrative Example

We use a hypothetical case referred to as *SmartBank* to exemplify and evaluate the approach. We describe the steps for managing compliance debt in engineering security compliance through obstacle analysis and goal refinements for *SmartBank*. We extend on the goal elaboration for *SmartBank* [23]. We describe how portfolio theory and compliance debt can assist the process of resolving obstacles and elaborating security requirements. The initial goal model is shown in Figure 1. The goal tree shows the goal tree and obstacles that may prevent the security goal from being achieved. Blue parallelograms show the goals and green parallelograms are the obstacles obstructing those goals. Hexagons represent agents. We assume OR-refinement as any of obstacles can obstruct the compliance goal. Looking at one scenario for the simplicity of exposition, SmartBank is bound by the data protection act which prohibits personal data from being stored outside its country of operation. With cloud computing, the user has very little knowledge about where the data is stored; hence this becomes a potential obstacle.

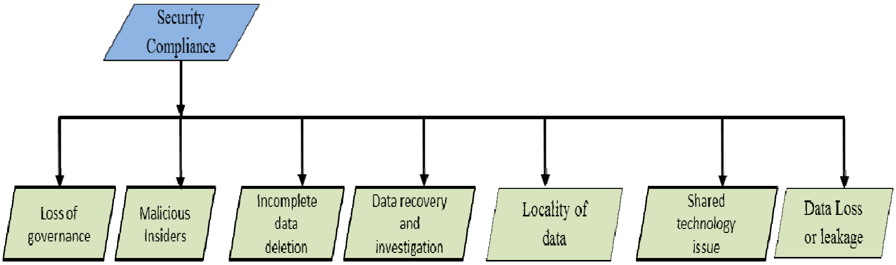

Fig. 1. Portion of the goal elaboration for Smart Bank

Identifying Compliance Obstacles: - Table 1 shows an obstacle to the "*locality of data*" goal from the goal model in figure 1

Table 1. Obstacles to Achieving Goal 1

Goal	Obstacle	Agent
Achieve [Store Personal Data in United Kingdom]	Data centre not located in the United Kingdom Subcontracting to another cloud provider as a backup plan	Cloud Provider

In this table, the cloud provider (agent) is shown to be responsible for the goal of storing data within the United Kingdom. We have thereby obtained the obstacles to this goal of storing data in the United Kingdom. In defining this obstacle, we took into consideration that cloud providers generally do not specify where the data will be stored.

Assessing and Selecting the Obstacles Using Portfolio Theory: Once obstacles have been identified, they need to be assessed, prioritised and be allocated with resources for resolving them. We can prioritise the obstacles by quantifying the risk value of the obstacles. The value of an obstacle is the product of the likelihood of the obstacle occurring and the criticality. In order to optimize the global risk of the portfolio and find the optimum solution, we calculated how much weight should be invested in resolving each obstacle to construct a low risk portfolio. This is calculated using their relative risk value in an optimisation algorithm. These weights imply that we will be able to construct the minimum risk portfolio for resolving the obstacles by allocation x-unit of resources. For this example, we assume no correlations between the obstacles.

$$Rp = \sqrt{\sum_{i=1} W1R1} \tag{8}$$

Table 2. Obstacle Analysis

Obstacle	Likelihood	Criticality	Risk Value	R1 (%)	Cost / Principal	Optimum Weights % (W1) (AHP)	Amount to be invested
Loss of governance	1	3	3	9.09	1	0.06	0.54
Malicious Insiders	1	3	3	9.09	2	0.06	0.54
Incomplete data deletion	3	2	6	18.18	1	0.16	1.45
Locality of data	3	3	9	27.27	2	0.40	3.59
Shared technology issue	3	2	6	18.18	3	0.16	1.45
Data Loss or leakage	2	3	6	18.18	3	0.16	1.45
Portfolio Risk Value	**12.01%**						

Assuming we have 9 units of resources available for resolving the obstacle, we can either decide to resolve the obstacles based on their priority using AHP (3) or their cost. If the obstacles to be resolved are selected based on their AHP priority, we will allocate the 9 units of resources to the resources with the highest priorities. Using this approach, we will be left with a combined risk of ***18.2%*** for the obstacles not resolved (i.e. we resolved the obstacle by doing nothing).

On the other hand, if the obstacles to be resolved are selected based on their cost, we will allocate the 9 units of resources to the cheapest obstacles to resolve. Using this approach, we will be left with a risk of ***18.2%*** for the obstacle not resolved.

From the results allocation process in table 2, It can be concluded that portfolio based approach has the minimum risk profile ***(12.01%)*** because it utilizes the concept portfolio to diversify the allocation of resources to resolving the obstacles instead of resolving just some of the obstacles based on priority alone.

Instead of focusing the investment on resolving some of the obstacles, the approach spreads the investment into a portfolio of multiple obstacles. The diversifying process is a risk mitigating strategy. This is believed to be a powerful risk mitigating strategy in situations where analysts and compliance managers lack the experience and make ad hoc decisions, which fail to justify the choice of obstacles to be resolved under uncertainty. In such context, the conclusion would have been different if portfolio was not in use: the analyst may have focused the investment on prioritised obstacles that may be driven by cost, time, risk profile and resources. The result from the portfolio analysis process shows that the new global risk of portfolio is 12.01% when resolving the obstacles based on the optimal weight of the available resources.

Resolving the Obstacles: To resolve the *"locality of data"* obstacle, we have catalogued different obstacle resolution tactics. We have explored some potential resolutions to this obstacle. We have listed different resolution in order to guide the selection of the preferred resolution tactic as illustrated in Table 3. Once a resolution tactic has been selected, we probed further for possible obstacles and new resolution tactics for this obstacle. We report on an iteration of this process.

Table 3. Resolving the Compliance Obstacle Data-centre not located in the United Kingdom

Goal: Achieve [Store Personal Data in United Kingdom]	
Obstacles: Data-centre not located in the United Kingdom The cloud provider subcontracting to another provider as a backup plan	
Resolution Strategies	
Goal Substitution	None because the obstructed goal is essential
Agent Substitution	Store and process personal data in-house Assign the responsibility of obstructed goal to trusted cloud platform
Obstacle Prevention	Avoid the obstacle by negotiating terms and conditions with cloud provider
Obstacle Reduction	Reduce the obstacle by getting a US-EU safe harbor certification that will allow data to be stored in a wider area
Goal Weakening	Relaxing the requirements to include storing of data in the EU as this is covered by the Data Protection Act.
Goal Restoration and Obstacle Mitigation	These include the requirement to alert the organization when that won't be able to store the data in the United Kingdom.
Obstacle Tolerance – Do Nothing	Do nothing

Our objective is to use compliance debt as risk metric for informing the resolution process for this obstacle. We calculate and assign the compliance debt of each alternative, so that the sum of the alternatives is equal 100%. P is the relative cost of the resolution tactics. For this example, we assume that ideal value is the tactic with the least risk value.

Table 4. TD for Resolving the Compliance Obstacle

Resolution Tactic	P	I_P	I_A	Value	Risk Value	Risk %	TD%
Store and process personal data in-house	2	1	2	4	2	7%	4%
Assign the responsibility of obstructed goal to trusted cloud platform	3	1	1	3	1	3%	0%
Avoid the obstacle by negotiating terms and conditions with cloud provider	2	1	3	6	3	10%	13%
Reduce the obstacle by getting a US-EU safe harbour certification that will allow data to be stored in a wider area	2	2	2	8	4	14%	22%
Relaxing the requirements to include storing of data in the EU as this is covered by the Data Protection Act.	2	2	2	8	4	14%	22%
The requirement to alert the organisation when that won't be able to store the data in the United Kingdom.	1	3	2	6	6	21%	13%
Do nothing	1	3	3	9	9	31%	26%

In table 4, we can see that the ideal solution with the lowest risk has the highest principal. If we decide that we only have 2units of resources to spend on resolving this obstacle, the next best resolution tactic will be ***tactic 1*** has it incurs the lowest compliance debt of 4% for using 2units. Likewise if we decide that we only have 1 unit of resources to spend on resolving this obstacle, the next best resolution tactic will be ***tactic 6*** has it incurs the lowest compliance debt of 13% for using 1 unit.

We have now applied the technique described in the previous section. The main objective of the approach is to improve compliance by reducing the risks associated with goals obstruction through a diversified portfolio. The compliance debt metric provides better insights on the significance of a tactic in mitigating risks given the resources in hand. This is calculated as the gap between the values of tactic in question relative to the ideal tactic for resolving this obstacle. As investing in the ideal tactic is not always affordable, the metric is an expression for the risks tolerated if *this* tactic is chosen. It also expresses the likely consequences if the risk materialises. This analysis provides analysts and compliance managers with a powerful and objective tool to assess and rethink their investment decisions in elaborating compliance requirements. The use of compliance debt metric had made both the short term and long term risk visible in the selection and allocation process.

5 Discussion and Limitations

Reflecting on the application of the method, we discuss its limitations and threats to validity of what has been observed in section 4. The main objective of the approach is to improve compliance by reducing the risks associated with goals obstruction through a diversified portfolio. The compliance debt metric provides better insights on the significance of a tactic in mitigating risks given the resources in hand. This is calculated as the gap between the values of tactic in question relative to the ideal tactic for resolving this obstacle. As investing in the ideal tactic is not always affordable, the metric is an expression for the risks tolerated if *this* tactic is chosen. It also expresses the likely consequences if the risk materialises. This analysis provides analysts and compliance managers with a powerful and objective tool to assess and rethink their investment decisions in elaborating compliance requirements. The use of compliance debt metric had made both the short term and long term risks visible in the selection and allocation process. Further empirical investigation and application of the method to an extended real case is required to confirm the validity of these claims.

Portfolio theory is a well-accepted concept for diversifying risk; it is well grounded in theory. The framework presented here although useful, has its limitations. Analysing the portfolio depends on identifying threats and estimating their likelihood. This approach assumes sufficient awareness and experience of compliance standards which are related to the case. Furthermore it assumes that stakeholders are confident enough to anticipate the probabilities and the likely risks involved. Nevertheless, anticipating risks is rather a subjective exercise, which can be biased to the perspective and the experience of the stakeholders involved. Consequently, due to the different variables that might be estimated in a subjective way; this approach can only provide a best-case portfolio rather optimal portfolio.

The exemplar has looked at an aspect of security compliance, its goals and subgoals to illustrate the feasibility of the approach. In the practice, the modelling tends to be complex involving many security goals and inter-dependencies between the goals. Though the goal modelling is inherently scalable to accommodate for such, completeness of the refinements process and the number of iterations tend to vary with the expertise and knowledge of the domain experts involved. Consequently, the mode of application and the quality of the results tends to vary. This is subject for future investigation.

Standards tend to change by time. Though the current exemplar does not explicitly cater for change and evolution of compliance, the prioritisation process assumes the considered requirements provide baseline for realising compliance at that specific time. However, the same process can be reiterated with any incoming requirements and changes in compliance standards.

In this example, the correlation between the obstacles was assumed to be zero. This does not cater for the dependencies and how resolving an obstacle will affect the resolution of other obstacles and the constructed portfolio.

In practice, software like any other system shall be subject to continual review and audit for compliance. Though it is not widely adopted practice for periodically auditing software for compliance, the compliance debt metric and the approach can provide useful input and support to the process. Beyond what we have reported in the exemplar, it would be interesting to see how real life scenarios can leverage on the reported approach to motivate and inform the auditing process.

6 Conclusion

Our working hypothesis is that goal refinement and obstacle resolution for compliance may introduce compliance debt that needs to be managed for mitigating risks. We have explored the link between obstacles and compliance debt when managing compliance. We have proposed a portfolio-based approach to quantify the compliance debt and risk for compliance. The approach can determine the candidate obstacles that need to be managed along with the compliance debt and risks that can be tolerated. Our technique is integrated into existing methods for handling obstacles in goal-oriented requirements engineering with the aim of managing trade-offs and deriving more realistic compliance requirements based on their economics, risks and compliance debt. We have illustrated the approach using an example. The process goal refinement and elaboration through obstacle analysis and handling is iterative and continuous. Our future work will look at how compliance debt can be further estimated and used as a metric to inform stopping criteria and further refinements, elaborations and resolution of obstacles hindering compliance. We will also look at including correlation coefficient as a property to be estimated for the portfolio and determining the correlations between the obstacles through dependency analysis.

References

1. Jansen, W., Grance, T.: Guidelines on Security and Privacy in Public Cloud Computing. In: National Institute of Standards and Technology (2011)
2. Lubars, M., Potts, C., Richter, C.: A Review of the State of the Practice in Requirements Modelling. In: IEEE International Symposium on Requirements Engineering, pp. 2–14 (1993)
3. Nuseibeh, B., Easterbrook, S.: Requirements Engineering: A Roadmap. In: Proceedings of the Conference on the Future of Software Engineering, pp. 4–11 (2000)
4. Saaty, L.: The Analytical Hierarchy Process. McGraw-Hill (1980)
5. Karlsson, J., Olsson, S., Ryan, K.: Improved Practical Support for Large-scale Requirements Prioritising. Requirements Engineering 2(1), 51–60 (1997)
6. Sivzattian, S., Nuseibe, B.: Linking the Selection of Requirements to Market Value: A Portfolio-Based Approach. In: Proceedings of 7th International Workshop on Requirements Engineering: Foundation for Software Quality (2001)
7. Seaman, C., Guo, Y., Izurieta, C., Cai, Y., Zazworka, N., Shull, F., Vetro, A.: Using technical debt data in decision making: Potential decision approaches. In: 2012 Third International Workshop on Managing Technical Debt (MTD), pp. 45–48 (2012)
8. Benbasat, I., Cavusoglu, H., Bulgurcu, B.: Information Security compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 523–548 (2010)

9. Ransbotham, S., Mitra, S.: Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. Information Systems Research 20, 121–139 (2009)
10. Haley, C., Laney, R., Moffett, J., Nuseibeh: Security Requirements Engineering: A Framework for Representation and Analysis. IEEE Transactions on Software Engineering 34, 133–151 (2008)
11. Duboc, L., Letier, E., Rosenblum, D.: Systematic Elaboration of Scalability Requirements through Goal-Obstacle Analysis. IEEE Transactions on Software Engineering 39, 119–140 (2013)
12. van Lamsweerde, A.: Goal-Oriented Requirements Engineering: A Guided Tour. In: Proceedings of 5th IEEE International Symposium on Requirements Engineering, pp. 249–263 (2001)
13. Letier, E., Lamsweerde, A.: Handling Obstacles in Goal-Oriented Requirements Engineering. IEEE Transactions on Software Engineering, Special Issue on Exception Handling 26(10), 978–1005 (2000)
14. Breaux, T., Anton, A., Vail, M.: Towards Compliance: Extracting Rights and Obligations to Align Requirements with Regulations. In: 14th IEEE International Conference on Requirements Engineering, pp. 49–58, 11–15 (2006)
15. Giorgini, P., Mylopoulos, J., Massacci, F.: Modelling Security Requirements through Ownership, Permission and Delegation. In: Proceedings of the 13th IEEE International Conference on Requirements Engineering, pp. 167–176 (2005)
16. Van Lamsweerde, A.: Elaborating security requirements by construction of intentional anti-models. In: Proceedings of 26th International Conference on Software Engineering, pp. 148–157 (2004)
17. May, M., Gunter, C., Lee, I.: Privacy APIs: Access Control Techniques to Analyse and Verify Legal Privacy Policies. In: 19th IEEE Computer Security Foundations Workshop, pp. 13–97 (2006)
18. Burgemeestre, B., Hulstijn, J., Tan, Y.: Value-Based Argumentation for Justifying Compliance. In: Governatori, G., Sartor, G. (eds.) Deontic Logic in Computer Science, pp. 214–228. Guido Governatori (2010)
19. Markowitz, H.M.: Portfolio Selection: Efficient Diversification of Investments. John Wiley & Sons, New York (1957)
20. Guo, Y., Seaman, C.: A Portfolio Approach to Technical Debt Management. In: Proceedings of the 2nd Workshop on Managing Technical Debt, MTD 2011, pp. 31–34 (2011)
21. ALRebeish, F., Bahsoon, R.: Risk-Aware Web Service Allocation in the Cloud Using Portfolio Theory. In: Proceedings of the 2013 IEEE International Conference on Services Computing, pp. 675–682 (2013)
22. Brown, N., Cai, Y., Guo, Y., Kazman, R., Kim, M., Kruchten, P., Lim, E., MacCormack, A., Nord, R., Ozkaya, I., Sangwan, R., Seaman, C., Sullivan, K.: Zazworka. N.: Managing technical debt in software-reliant systems. In: Proceedings of the FSE/SDP Workshop on Future of Software Engineering Research, FoSER 2010, pp. 47–52 (2010)
23. Zardari, S., Faniyi, F., Bahsoon, R.: Using Obstacles for Systematically Modelling, Analysing and Mitigating Risks in Cloud Adoption. In: Aligning Enterprise, System and Software Architectures, pp. 275–296. IGI Global (2013)