ValidKI: A Method for Designing Key Indicators to Monitor the Fulfillment of Business Objectives

Olav Skjelkvåle Ligaarden*†, Atle Refsdal*, and Ketil Stølen*†

* *Department for Networked Systems and Services, SINTEF ICT, PO Box 124 Blindern, N-0314 Oslo, Norway*
E-mail: {olav.ligaarden, atle.refsdal, ketil.stolen}@sintef.no
† *Department of Informatics, University of Oslo, PO Box 1080 Blindern, N-0316 Oslo, Norway*

***Abstract*—In this paper we present our method ValidKI for designing key indicators to monitor the fulfillment of business objectives. A set of key indicators is valid with respect to a business objective if it can be used to measure the degree to which the business or relevant part thereof complies with the business objective. ValidKI consists of three main steps each of which is divided into sub-steps. We demonstrate the method on an example case focusing on the use of electronic patient records in a hospital environment.**

***Keywords*-key indicator, business objective, electronic patient record**

I. Introduction

Today's companies benefit greatly from ICT-supported business processes, as well as business intelligence and business process intelligence applications monitoring and analyzing different aspects of a business and its processes. The output from these applications may be key indicators which summarize large amounts of data into single numbers. Key indicators can be used to evaluate how successful a company is with respect to specific business objectives. For this to be possible it is important that the key indicators are valid. A set of key indicators is valid with respect to a business objective if it can be used to measure the degree to which the business or relevant part thereof complies with the business objective. Valid key indicators facilitate decision making, while invalid key indicators may lead to bad business decisions, which again may greatly harm the company.

In today's business environment, companies cooperate across company borders. Such co-operations often result in sharing or outsourcing of ICT-supported business processes. One example is the interconnected electronic patient record (EPR) infrastructure. The common goal for this infrastructure is the exchange of EPRs facilitating the treatment of the same patient at more than one hospital. In such an infrastructure, it is important to monitor the use of EPRs in order to detect and avoid misuse. This may be achieved through the use of key indicators. It may be challenging to identify and compute good key indicators that are valid. Furthermore, in an infrastructure or system stretching across many companies we often have different degrees of visibility into how the cooperating parties perform their part of the business relationship, making the calculation of key indicators particularly hard.

In this paper we present a new method *ValidKI* (Valid Key Indicators) for designing key indicators to monitor the fulfillment of business objectives. We demonstrate ValidKI by applying it on an example case targeting the use of EPRs. We have developed ValidKI with the aim of fulfilling the following characteristics:

- **Business focus:** The method should facilitate the design and assessment of key indicators for the purpose of measuring the fulfillment of business objectives.
- **Efficiency:** The method should be time and resource efficient.
- **Generality:** The method should be able to support design of key indicators for systems shared between many companies or organizations.
- **Heterogeneity:** The method should not place restrictions on how key indicators are designed.

To the best of our knowledge, there exists no other method with sole focus on design of valid key indicators to monitor the fulfillment of business objectives.

The rest of the paper is structured as follows: in Section II we introduce our basic terminology and definitions. In Section III we give an overview of ValidKI and its three main steps. In Sections IV, V, and VI we demonstrate our three-step method on an example case addressing the use of EPRs in a hospital environment. In Section VII we present related work, while in Section VIII we conclude by characterizing our contribution and discussing the suitability of our method.

II. Basic terminology and definitions

Merriam-Webster defines an "indicator" as *"one that indicates"* [1], while it defines "indicates" as *"to be a sign, symptom, or index of"* [2]. The weather forecast is a typical indicator since it gives an indication of what the weather will be like the next day.

Many companies profit considerably from the use of indicators [3] resulting from business process intelligence applications that monitor and analyze different aspects of a business and its processes. Indicators can be used to measure to what degree a company fulfills its business objectives and

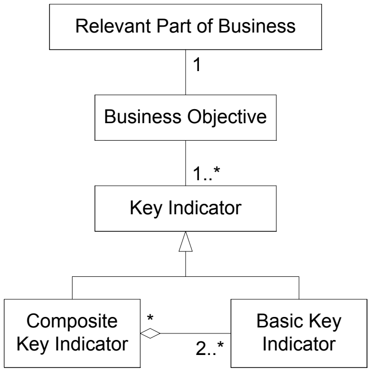

Figure 1. The artefacts addressed by ValidKI

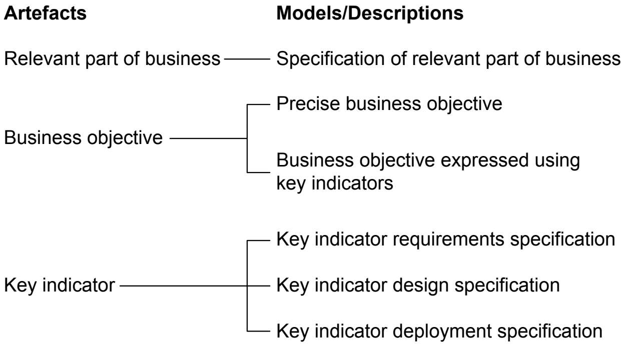
Artefacts
Models/Descriptions
Relevant part of business
Specification of relevant part of business
Precise business objective
Business objective
Business objective expressed using key indicators
Key indicator requirements specification
Key indicator
Key indicator design specification
Key indicator deployment specification

Figure 2. The models/descriptions developed by ValidKI

we then speak of key indicators. Some business objectives may focus on business performance, while others may focus on risk or compliance with laws and regulations.

A. The artefacts addressed by ValidKI

The UML [4] class diagram in Fig. 1 relates the main artefacts addressed by ValidKI. The associations between the different concepts have cardinalities that specify how many instances of one concept that may be associated to an instance of the other concept. The hollow diamond specifies aggregation.

As characterized by the diagram, a key indicator is either basic or composite. By basic key indicator we mean a measure such as the number of times a specific event generated by the ICT infrastructure has been observed within a given time interval, the average time between each generation of a specific event, the load on the network at a particular point in time, or similar. A composite key indicator is the aggregation of two or more basic key indicators. One or more key indicators are used to measure to what extent a business objective is fulfilled with respect to a relevant part of the business.

B. The models/descriptions developed by ValidKI

As illustrated by Fig. 2, performing the steps of ValidKI results in six different models/descriptions each of which describes one of the artefacts of Fig. 1 from a certain perspective.

A specification, at a suitable level of abstraction, documents the relevant part of the business in question.

Business objectives are typically expressed at an enterprise level and in such a way that they can easily be understood by for example shareholders, board members, partners, etc. It is therefore often not completely clear what it means to fulfill them. This motivates the need to capture each business objective more precisely. The degree of fulfillment of a precise business objective is measured by a set of key indicators. To measure its degree of fulfillment there is a need to express each business objective in terms of key indicators.

For each key indicator we distinguish between three specifications; the key indicator requirements specification, the key indicator design specification, and the key indicator deployment specification. The first captures the expectations to the key indicator, the second defines how the indicator is calculated, while the third documents how the calculation is embedded in the business or relevant part thereof that ValidKI is used to help monitor. In other words the deployment specification describes how the data on which the key indicator calculation is based is extracted and transmitted within the business in question. We often refer to the pair of the design specification and the deployment specification as the key indicator's realization.

C. External and internal validity

We distinguish between external and internal validity. External validity may be understood as a relation between a business objective and a set of key indicators.

Definition 1. ***External validity*** *A set of key indicators is externally valid with respect to a business objective if it can be used to measure the degree to which the business objective is fulfilled.*

Internal validity may be understood as a relation between the requirements specification of a key indicator and its realization as captured by its design and deployment specifications.

Definition 2. ***Internal validity*** *A key indicator is internally valid if its realization as captured by its design and deployment specifications fulfills its requirements specification.*

If each element of a set of key indicators is internally valid we may evaluate its external validity by considering only the requirements specifications of its elements.

III. Overview of ValidKI

Fig. 3 provides an overview of the ValidKI method. It takes as input a business objective and delivers a set of key indicators and a report arguing its external validity with

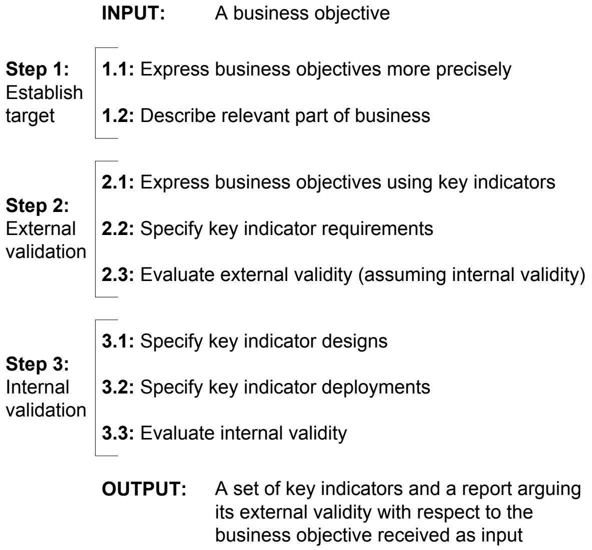
INPUT: A business objective
Step 1: Establish target
1.1: Express business objectives more precisely
1.2: Describe relevant part of business
Step 2: External validation
2.1: Express business objectives using key indicators
2.2: Specify key indicator requirements
2.3: Evaluate external validity (assuming internal validity)
Step 3: Internal validation
3.1: Specify key indicator designs
3.2: Specify key indicator deployments
3.3: Evaluate internal validity
OUTPUT: A set of key indicators and a report arguing its external validity with respect to the business objective received as input

Figure 3. Overview of ValidKI

respect to the business objective received as input[1]. In the following we offer additional explanations for each of the three main steps.

A. Establish target

The first main step of ValidKI is all about understanding the target, i.e. understanding exactly what the business objective means and acquiring the necessary understanding of the relevant part of business for which the business objective has been formulated. In the first sub-step we help the client to characterize the business objective in a more precise manner leading to a precise business objective, while in the second sub-step we specify the relevant part of the business.

B. External validation

The second main step of ValidKI is concerned with establishing a set of key indicators that is externally valid with respect to the business objective considering only their requirements specifications.

In order to argue external validity we reformulate the precise business objective in terms of key indicators. Furthermore, we specify our requirements to each key indicator referred to in the reformulated precise business objective. These two sub-steps are typically conducted in parallel. Based on this we evaluate external validity assuming internal validity of each key indicator. If we are not able to establish external validity the reformulated business objective and/or requirements specifications must be changed.

C. Internal validation

In the third main step we do an internal validation of each key indicator of the externally valid key indicator set. In the first two sub-steps we specify the design and deployment of each key indicator. Then, we evaluate whether this realization fulfills its requirements specification. If this is the case we have established internal validity and thereby external validity; if not we iterate.

IV. Establish target

In the following we assume that we have been hired to help the public hospital Client H design key indicators to monitor their compliance with Article 8 in the European Convention on Human Rights [5]. The article states the following:

Article 8 – Right to respect for private and family life

1) Everyone has the right to respect for his private and family life, his home and his correspondence.
2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Client H needs to comply with Article 8 since it is a public authority. The consequence for Client H of not complying with Article 8 may be economic loss and damaged reputation. One example [6] of violation of Article 8 is from Finland. A Finnish woman was first treated for HIV at a hospital, before she later started working there as a nurse. While working there she suspected that her co-workers had unlawfully gained access to her medical data. She brought the case to the European Court of Human Rights in Strasbourg which unanimously held that the district health authority, responsible for the hospital, had violated Article 8 by not protecting the medical data of the woman properly. The district health authority was held liable to pay damages to the woman. Client H has therefore established the following business objective:

Business objective BO-A8: Client H complies with Article 8 in the European Convention on Human Rights.

Client H wants to make use of key indicators to monitor the degree of fulfillment of BO-A8, and now they have hired us to use ValidKI for designing them. In the rest of this section we conduct Step 1 of ValidKI on behalf of Client H with respect to BO-A8.

[1] When using ValidKI in practice we will typically develop key indicators for a set of business objectives, and not just one which we without loss of generality restrict our attention to here.

A. Express business objectives more precisely (Step 1.1 of ValidKI)

Article 8 states under which circumstances a public authority can interfere with someone's right to privacy. One of these circumstances is *"for the protection of health"*, which is what Client H wants us to focus on. In the context of Client H this means to provide medical assistance to patients. The ones who provide this assistance are the health-care professionals of Client H.

The medical history of a patient is regarded as both sensitive and private. At Client H, the medical history of a patient is stored in an electronic patient record (EPR). An EPR is *"an electronically managed and stored collection or collocation of recorded/registered information on a patient in connection with medical assistance"* [7]. The main purpose of an EPR is to communicate information between health-care professionals that provide medical care to a patient. To protect the privacy of its patients, Client H restricts the use of EPRs. In order to comply with Article 8, Client H allows a health-care professional to interfere with the privacy of a patient only when providing medical assistance to this patient. Hence, the dealing with the EPRs within the realms of Client H is essential.

For Client H it is important that every access to information in an EPR is in accordance with Article 8. A health-care professional can only access a patient's EPR if he/she provides medical assistance to that patient, and he/she can only access information that is necessary for the medical assistance provided to the patient. The information accessed can not be used for any other purpose than providing medical assistance to patients. Accesses to information in EPRs not needed for providing medical assistance would not be in accordance with Article 8. Also, employees that are not health-care professionals and that work within the jurisdiction of Client H are not allowed to access EPRs. Based on the constraints provided by Client H, we decide to express BO-A8 more precisely as follows:

Precise business objective PBO-A8: $C_1 \;\wedge\; C_2 \;\wedge\; C_3$

- **Constraint** C_1**:** Health-care professionals acting on behalf of Client H access:
  - a patient's EPR only when providing medical assistance to that patient
  - only the information in a patient's EPR that is necessary for providing medical assistance to that patient
- **Constraint** C_2**:** Health-care professionals acting on behalf of Client H do not use the information obtained from a patient's EPR for any other purpose than providing medical assistance to that patient.
- **Constraint** C_3**:** Employees that are not health-care professionals and that work within the jurisdiction of Client H do not access EPRs.

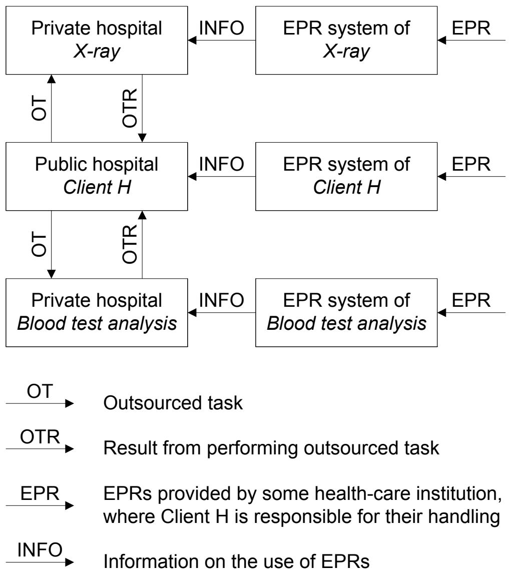

Figure 4. Specification of relevant part of business

As indicated by PBO-A8's definition, all three constraints must be fulfilled in order for PBO-A8 to be fulfilled.

B. Describe relevant part of business (Step 1.2 of ValidKI)

To design key indicators to monitor BO-A8 we need to understand the part of business that is to comply with BO-A8 and therefore is to be monitored. Client H has outsourced some of its medical services to two private hospitals. These two are referred to as *X-ray* and *Blood test analysis* in Fig. 4. The first hospital does all the X-ray work for Client H, while the second hospital does all the blood test analyses. Client H is not only responsible for its own handling of EPRs, but also the outsourcing partners' handling of EPRs, when they act on behalf of Client H. As shown in Fig. 4, Client H outsources tasks to the two private hospitals, and gets in return the results from performing these tasks. All three health-care institutions use some kind of EPR system for handling the EPRs. An EPR system is *"an electronic system with the necessary functionality to record, retrieve, present, communicate, edit, correct, and delete information in electronic patient records"* [7]. These systems use EPRs provided by several different health-care institutions. As shown in Fig. 4, these systems are only of interest when they handle EPRs where Client H is responsible for their handling. These systems will provide their institutions with information on the use of EPRs. This information can later be used in the monitoring. It should be noticed that the model in Fig. 4 only provides a small overview of the modeling that is performed.

V. External validation

In this step we establish a set of key indicators that is externally valid with respect to the business objective BO-

A8 by only considering their requirements specifications. In order to argue external validity we reformulate the precise business objective PBO-A8 in terms of key indicators. Due to lack of space, we only show how we reformulate constraint C_1.

A. *Express business objectives using key indicators (Step 2.1 of ValidKI)*

At the three health-care institutions, most of the medical tasks that a health-care professional conducts during a working day are known in advance. It is known which patients the professional will treat and what kind of information the professional will need access to in order to treat the different patients. When a health-care professional accesses information in a patient's EPR it is then possible to check whether the professional really needs this information. Client H and the two outsourcing partners have a list for each health-care professional documenting which patients the professional is treating and what kind of information the professional needs for this purpose. These lists are updated on a daily basis. Many of these updates are automatic. For instance, when Client H is assigned a new patient, then this patient is added to the lists of the health-care professionals that will be treating this patient.

The EPR systems classify an access to information in an EPR as *authorized* if the professional needs the information to do a planned task. Otherwise, the access is classified as *unauthorized*. If it is classified as unauthorized then it is possible to check in retrospect whether the access was necessary. In an emergency situation, for instance when a patient is having a heart attack, a health-care professional often needs access to information in an EPR that he/she was not supposed to access. By checking in retrospect whether unauthorized accesses were necessary it is possible to classify the unauthorized accesses into two groups; one for accesses that were necessary, and for those that were not. The first group is called *approved* unauthorized accesses, while the second group is called *not approved* unauthorized accesses. All accesses that are classified as not approved unauthorized accesses are considered as *illegal* accesses.

At Client H and the two outsourcing partners, health-care professionals use smart cards for accessing information in EPRs. If a card is lost or stolen, the owner must report it as missing, since missing cards may be used by other health-care professionals to access EPRs illegally[2]. When the card has been registered as missing it can no longer be used. When reporting it as missing, the last time the card owner used it before noticing that it was missing is recorded. All accesses to EPRs that have occurred between this time and the time it was registered as missing are considered as illegal accesses.

It seems reasonable to monitor different types of violations of constraint C_1 in order to measure its degree of fulfillment. The violations of interest, for this particular constraint, are the different types of illegal accesses that may be performed by health-care professionals. These are as follows:

1) Not approved unauthorized accesses to EPRs where the owners of the EPRs are patients of the accessors
2) Not approved unauthorized accesses to EPRs where the owners of the EPRs are not patients of the accessors
3) Accesses to EPRs from missing or stolen smart cards

It should be noticed that each EPR is owned by a patient, which is natural since the information stored in the EPR is about the patient in question.

For each of the types 1, 2, and 3 of illegal accesses we identify the key indicators K_1, K_2, and K_3, respectively, where each key indicator measures the ratio of one type of illegal accesses to all accesses to information in EPRs. In (1) these key indicators have been used to express C_1. Ideally, Client H would have liked all three ratios to be zero in order for the constraint to be fulfilled. However, in real life things are not perfect; EPRs may for example be accessed by accident or a health-care professional may not have a perfect recollection of when he/she used the smart card the last time before losing it. After some hesitation, Client H came up with the intervals documented in (1).

$$\begin{aligned}&0 \leq K_1 \leq 0.005 \ \wedge \ 0 \leq K_2 \leq 0.001 \ \wedge \\ &0 \leq K_3 \leq 0.0001\end{aligned} \tag{1}$$

The formula in (1) expresses for what key indicator values constraint C_1 is fulfilled. By inserting key indicator values into this formula we get the degree of fulfillment of C_1. For instance, if K_1 equals 0.006 while the values of K_2 and K_3 are less than their upper thresholds, then C_1 is close to being fulfilled. On the other hand, if K_1 equals 0.05 instead, then C_1 is far from being fulfilled.

B. *Specify key indicator requirements (Step 2.2 of ValidKI)*

The key indicators identified in the previous step only provide a high-level specification of what they should measure. In Table I a more refined specification has been given for each key indicator. As we can see, each of the three identified key indicators is composed of basic key indicators. The expectation to each basic key indicator is that it is measured every week and that it measures the total number for all three health-care institutions. This is necessary since Client H is responsible for the handling of EPRs not only at its own premises but also within its two outsourcing partners when they act on behalf of Client H. In addition, we specify for each key indicator used in (1) the required level of trust in the correctness of its values. Together with Client H we

[2] Missing smart cards may of course also be misused by other people that are not health-care professionals, but in the case of constraint C_1 we only focus on health-care professionals.

Table I
KEY INDICATOR REQUIREMENTS SPECIFICATIONS

The composite key indicator K_1 is the ratio of

the basic key indicator K_{B1} = "the total number of not approved unauthorized accesses at Client H, Blood test analysis, and X-ray, in the period of one week, where the owners of the EPRs are patients of the accessors"

to

the basic key indicator K_{B2} = "the total number of accesses to EPRs at Client H, Blood test analysis, and X-ray in the period of one week".

Required level of trust in the correctness of the values of K_1: 0.9

The composite key indicator K_2 is the ratio of

the basic key indicator K_{B3} = "the total number of not approved unauthorized accesses at Client H, Blood test analysis, and X-ray, in the period of one week, where the owners of the EPRs are not patients of the accessors"

to

the basic key indicator K_{B2}.

Required level of trust in the correctness of the values of K_2: 0.9

The composite key indicator K_3 is the ratio of

the basic key indicator K_{B4} = "the total number of accesses at Client H, Blood test analysis, and X-ray, in the period of one week, from smart cards registered as missing"

to

the basic key indicator K_{B2}.

Required level of trust in the correctness of the values of K_3: 0.9

Table II
ADDITIONAL KEY INDICATOR REQUIREMENTS SPECIFICATION

The composite key indicator K_4 is the ratio of

the basic key indicator K_{B5} = "the total number of smart cards at Client H, Blood test analysis, and X-ray, in the period of one week, left in terminals used to access information EPRs and where the terminal eventually timed out"

to

the basic key indicator K_{B6} = "the total number of smart cards used at Client H, Blood test analysis, and X-ray in the period of one week".

Required level of trust in the correctness of the values of K_4: 0.9

assign a trust level of 0.9 to each composite key indicator. This means that for each composite key indicator we need to believe that the probability of its values being correct is at least 0.9, in order for the composite key indicator to be useful.

C. Evaluate external validity (Step 2.3 of ValidKI)

To evaluate external validity we try in collaboration with Client H to construct an argument for external validity based on the reformulated precise business objective and the requirements specifications of the key indicators. At this stage we assume for each key indicator that it is possible to come up with a realization that is internally valid. We agree that the identified key indicators can be used to monitor possible violations of constraint C_1, but we are a bit uncertain whether we have managed to capture all the types of illegal accesses that are relevant when measuring the degree of fulfillment of C_1. After some discussion, we conclude that there is fourth type of illegal accesses that we should also monitor. This type of illegal access may occur if a health-care professional forgets his/hers smart card in a terminal used to access information in EPRs. Other health-care professionals may then use this terminal to access information in EPRs. An indication of the number of forgotten smart cards is the number of terminals that timed out with a smart card inserted.

We update the models created in Step 2.1 and 2.2 in order to include the new type of illegal accesses. The Boolean expression in (1) is updated as shown in (2). The key indicator K_4 is the ratio of the number of forgotten smart cards to the number of smart cards used by all health-care professionals. The interval that Client H came up with for K_4 is documented in (2). In Table II, Client H's expectations to K_4 has been documented.

$$\begin{aligned} &0 \leq K_1 \leq 0.005 \ \wedge \ 0 \leq K_2 \leq 0.001 \ \wedge \\ &0 \leq K_3 \leq 0.0001 \ \wedge 0 \leq K_4 \leq 0.002 \end{aligned} \tag{2}$$

VI. INTERNAL VALIDATION

Due to lack of space, we only show how the internal validity of the key indicator K_1 is established.

A. Specify key indicator designs (Step 3.1 of ValidKI)

Together with Client H we specify the designs of the key indicators $K_{B1}(X)$, $K_{B2}(X)$, and K_1 in the form of algorithms, as shown in Table III. $K_{B1}(X)$ and $K_{B2}(X)$ are computed at each of the three health-care institutions. The total sum of the three variants of $K_{B1}(X)$ is denoted by K_{B1}, while the total sum of the three variants of $K_{B2}(X)$ is denoted by K_{B2}. The algorithms for $K_{B1}(X)$, $K_{B2}(X)$ are used by all three health-care institutions, while the algorithm for K_1 is only used by Client H. This algorithm takes the three variants of both $K_{B1}(X)$ and $K_{B2}(X)$ as input.

B. Specify key indicator deployments (Step 3.2 of ValidKI)

Together with Client H we create deployment specifications for each of the three health-care institutions. Each specification describes how data on which the calculation of K_1 is based is extracted and transmitted. The deployment specification for X-ray in Table IV specifies how different data is extracted, how often, and by whom; how the data is transmitted internally at X-ray; and how the data is transmitted to Client H, to who, by whom, and how often. The

Table III
KEY INDICATOR DESIGN SPECIFICATIONS FOR $K_{B1}(X)$, $K_{B2}(X)$, AND K_1 IN THE FORM OF ALGORITHMS

Algorithm for $K_{B1}(X)$
Input: $L_{B1}(X) =$ "list of all the unauthorized accesses to EPRs in the period of one week at X, where the owners of the EPRs are patients of the accessors", where $X \in \{\text{Client H}, \text{Blood test analysis}, \text{X-ray}\}$ **Step 1:** At X a manual inspection of the elements in $L_{B1}(X)$ is done. The list elements are partioned into two lists; one list containing the approved unauthorized accesses and one list containing the not approved unauthorized accesses. The employee at X partioning $L_{B1}(X)$ decides whether an unauthorized access should be classified as approved or not approved. **Step 2:** $K_{B1}(X)$ is calculated by counting the number of list elements in the list of not approved unauthorized accesses. **Output:** $K_{B1}(X) =$ "number of not approved unauthorized accesses at X in the period of one week, where the owners of the EPRs are patients of the accessors"
Algorithm for $K_{B2}(X)$
Input: $L_{B2}(X) =$ "list of all the accesses to EPRs in the period of one week at X", where $X \in \{\text{Client H}, \text{Blood test analysis}, \text{X-ray}\}$ **Step 1:** An employee at X calculates $K_{B2}(X)$ by counting the number of list elements in $L_{B2}(X)$. **Output:** $K_{B2}(X) =$ "number of accesses to EPRs at X in the period of one week"
Algorithm for K_1
Input: K_{B1}(Client H), K_{B1}(Blood test analysis), K_{B1}(X-ray), K_{B2}(Client H), K_{B2}(Blood test analysis), and K_{B2}(X-ray) **Step 1:** Calculate K_{B1} as follows: $K_{B1} = K_{B1}(\text{Client H}) + K_{B1}(\text{Blood test analysis}) + K_{B1}(\text{X-ray})$ **Step 2:** Calculate K_{B2} as follows: $K_{B2} = K_{B2}(\text{Client H}) + K_{B2}(\text{Blood test analysis}) + K_{B2}(\text{X-ray})$ **Step 3:** Calculate K_1 as follows: $K_1 = \frac{K_{B1}}{K_{B2}}$ **Output:** K_1

Table IV
KEY INDICATOR DEPLOYMENT SPECIFICATION FOR X-RAY THAT DESCRIBES THE EXTRACTION AND TRANSMISSION OF DATA USED TO CALCULATE K_1

Extraction and transmission of L_{B1}(**X-ray**)
The EPR system administrator at X-ray creates the list L_{B1}(X-ray) every week, based on the access log of the EPR system at X-ray, which contains information on all accesses to information in EPRs at X-ray. The list is created by extracting all list elements in the access log that represents an unauthorized access where the owner of the EPR is a patient of the accessor and where the access occurred during the past seven days. The list is sent by encrypted email to the EPR monitoring officer at X-ray for further processing.
Extraction and transmission of L_{B2}(**X-ray**)
The EPR system administrator at X-ray creates the list L_{B1}(X-ray) every week, based on the access log of the EPR system at X-ray. The list is created by extracting all list elements in the access log that represents an access that occurred during the past seven days. The list is sent by encrypted email to the EPR monitoring officer at X-ray for further processing.
Transmission of K_{B1}(**X-ray**) **and** K_{B2}(**X-ray**)
The EPR monitoring officer at X-ray transmits K_{B1}(X-ray) and K_{B2}(X-ray) every week to the EPR monitoring officer at Client H by the use of an encrypted email.

deployment specification of Blood test analysis is similar, while the deployment specification of Client H differs from the other two with respect to how data is transmitted. Client H's deployment specification describes only internal data transmission.

C. Evaluate internal validity (Step 3.3 of ValidKI)

To evaluate the internal validity of K_1 we construct together with Client H an argument that its design and deployment specifications fulfills its requirements specification. After consulting both the requirements specification, in Table I, and the realization of K_1 we conclude that this is the case. The algorithm for K_1, in Table III, calculates the composite key indicator exactly as stated in its requirements specification. Also, all the data needed to calculate K_1 is specified to be extracted and transmitted every week at all three institutions. This is also in accordance with the requirements specification since it specifies that K_1 must be computed every week and with data from all three institutions. In addition, we discuss with Client H how much trust we can have in the correctness of the different kinds of data used to compute K_1. During this discussion, Client H tells us that they have more trust in the correctness of the values of K_{B1}(X-ray) than in the values of K_{B1}(Blood test analysis), since they believe that the employees at X-ray are more competent than the employees at Blood test analysis in classifying unauthorized accesses. Also, Client H finds it unlikely that X-ray or Blood test analysis would provide them with manipulated data. Based on the discussion, we assign high trust levels to the different kinds of data used to compute K_1 and we combine the individual trust levels into a single trust level for K_1. We conclude that our trust in the correctness of the values of K_1 is at least 0.9.

VII. RELATED WORK

To the best of our knowledge, there exists no other method with sole focus on design of externally valid key indicators to monitor the fulfillment of business objectives. There is a tool framework called Mozart [8] that uses a model driven approach to create monitoring applications that uses key performance indicators. We do not focus on the implementation of key indicators, but we specify what is needed for implementing them. The work in [8] also differs from our work by not designing indicators from scratch, but by mining them from a data repository during the design cycle.

An important part of our method is the assessment of external validity of the key indicators we design. There exist other approaches that assess the validity of indicators in other contexts. For instance, in [9] measurement theory is used to validate the meaningfulness of IT security risk indicators. There are also examples of approaches that assess the validity of specific sets of key indicators. For instance, in [10] the validity of indicators of firm technological capability is assessed, while the validity of indicators of patent value is assessed in [11].

There are several approaches that focus on measuring the achievement of goals. One example is COBIT [12], which is a framework for IT management and IT governance. The framework provides a IT governance model that helps in delivering value from IT and understanding and managing the risks associated with IT. In the governance model, business goals are aligned with IT goals, while metrics, in the form of leading and lagging indicators [13], and maturity models are used to measure the achievement of the IT goals. In our approach we do not focus on the value and risk that the use of IT has with respect to the business objectives. In our context, IT is relevant in the sense of providing the infrastructure necessary for monitoring the part of business that needs to comply with the business objectives.

Another way to measure the achievement of goals, is by the use of the Goal-Question-Metric [14], [15] (GQM) approach. Even though GQM originated as an approach for measuring achievement in software development, it can also be used in other contexts where the purpose is to measure achievement of goals. In GQM, business goals are used to drive the identification of measurement goals. These goals do not necessarily measure the fulfillment of the business goals, but they should always measure something that is of interest to the business. Each measurement goal is refined into questions, while metrics are defined for answering each question. No specific method, beyond reviews, is specified for validating whether the correct questions and metrics have been identified. The data provided by the metrics are interpreted and analyzed with respect to the measurement goal, to conclude whether it is achieved or not. One of the main differences between our method and GQM is that we characterize completely what it means to achieve a goal/objective. In GQM, however, this may be a question of interpretation.

In the literature, key indicators are mostly referred to in the context of measuring business performance. There exist numerous approaches for performance measurement. Some of these are presented in [16]. Regardless of the approach being used, the organization must translate their business objectives/goals into a set of key performance indicators in order to measure performance. An approach that is widely used [17] is balanced scorecard [3]. This approach translates the company's vision into four financial and non-financial perspectives. For each perspective a set of business objectives (strategic goals) and their corresponding key performance indicators are identified. However, the implementation of a balanced scorecard is not necessarily straight forward. In [18], Neely and Bourne identify several reasons for the failure of measurement initiatives such as balanced scorecards. One problem is that the identified measures do not measure fulfillment of the business objectives, while another problem is that measures are identified without putting much thought into how the data must be extracted in order to compute the measures. The first problem can be addressed in the external validation step of our method, while the second problem can be addressed in the internal validation step.

Much research has been done in the field of data quality. The problem of data quality is also recognized within the field of key indicators [19], [20]. In [21] a survey on how data quality initiatives are linked with organizational key performance indicators in Australian organizations is presented. This survey shows, amongst other things, that a number of organizations do not have data quality initiatives linked to their key indicators. Data quality should be taken into account when designing key indicators, since the use of key indicators based on poor quality data may lead to bad business decisions, which again may greatly harm the organization.

In [22], [23] the problem of key indicators computed from uncertain events is investigated. The motivation for this work is to understand the uncertainty of individual key indicators used in business intelligence. The authors use key indicators computed from data from multiple domains as examples. In the papers a model for expressing uncertainty is proposed, and a tool for visualizing the uncertain key indicators is presented.

VIII. Conclusion

The contribution of this paper is the new method *ValidKI* (Valid Key Indicators) for designing key indicators to monitor the fulfillment of business objectives. ValidKI facilitates the design of a set of key indicators that is externally valid with respect to a business objective, i.e. measures the degree to which the business or relevant part thereof complies with the business objective. To the best of our knowledge, there exists no other method with sole focus on design of externally valid key indicators to monitor the fulfillment of business objectives. The applicability of our method has been demonstrated by applying it on an example case addressing the use of electronic patient records in a hospital environment.

The demonstration of our method on the example case shows that the method facilitates the design and assessment of key indicators for the purpose of measuring the degree of fulfillment of business objectives. Even though ValidKI has been demonstrated on a realistic example case there is still a need to apply ValidKI in a real-world industrial setting in order to evaluate properly to what extent it has the characteristic mentioned above and to what extent it can be used to design key indicators for systems shared between many companies or organizations. By applying ValidKI in such a setting we will also determine to some extent whether it is time and resource efficient.

ValidKI is not restrictive when it comes to designing key indicators. The only restriction that ValidKI place on the design of key indicators is that it should be possible to realize them. This is a necessary restriction since a key indicator is of no value if it cannot be realized.

In the example case we have used trust levels to specify how much trust we need to have in the correctness of the different key indicators in order for them to be useful. In ValidKI it is up to the analysts to decide how to assess whether a key indicator has the necessary trust level or not. Thus, different approaches for reasoning about and aggregating trust can be applied for coming up with the trust level of a key indicator. As future work we will investigate the use of different approaches for reasoning about and aggregating trust in ValidKI.

ACKNOWLEDGMENTS

The research on which this paper reports has been carried out within the DIGIT project (180052/S10), funded by the Research Council of Norway, and the MASTER and NESSoS projects, both funded from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreements FP7-216917 and FP7-256980, respectively.

REFERENCES

[1] Merriam-Webster Online Dictionary, "Definition of Indicator," http://www.merriam-webster.com/dictionary/indicator, 2008, Accessed: 2011-04-27 11:00AM CEST.

[2] Merriam-Webster Online Dictionary, "Definition of Indicates," http://www.merriam-webster.com/dictionary/indicates, 2008, Accessed: 2011-04-27 11:00AM CEST.

[3] R. S. Kaplan and D. P. Norton, "The Balanced Scorecard – Measures That Drive Performance," *Harvard Business Review*, vol. 70, no. 1, pp. 71–79, 1992.

[4] Object Management Group, "Unified Modeling Language Specification, version 2.0," 2004.

[5] Council of Europe, "Convention for the Protection of Human Rights and Fundamental Freedoms," 1954.

[6] European Court of Human Rights, "Press Release – Chamber Judgments 17.07.08," 17. July 2008.

[7] Helsedirektoratet, "Code of Conduct for Information Security – The Healthcare, Care, and Social Services Sector," http://www.helsedirektoratet.no/vp/multimedia/archive/00278/The_Code_of_conduct_278829a.pdf, 2. June 2010, Accessed: 2011-04-27 11:00AM CEST.

[8] M. Abe, J. Jeng, and Y. Li, "A Tool Framework for KPI Application Development," in *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'07)*. IEEE Computer Society, 2007, pp. 22–29.

[9] A. Morali and R. Wieringa, "Towards Validating Risk Indicators Based on Measurement Theory," in *Proceedings of First International Workshop on Risk and Trust in Extended Enterprises*. IEEE Computer Society, 2010, pp. 443–447.

[10] T. Schoenecker and L. Swanson, "Indicators of Firm Technological Capability: Validity and Performance Implications," *IEEE Transactions on Engineering Management*, vol. 49, no. 1, pp. 36–44, 2002.

[11] M. Reitzig, "Improving Patent Valuations for Management Purposes – Validating New Indicators by Analyzing Application Rationales," *Research Policy*, vol. 33, no. 6-7, pp. 939–957, 2004.

[12] IT Governance Institute, "COBIT 4.1," 2007.

[13] W. Jansen, *Directions in Security Metrics Research*. DIANE Publishing, 2010.

[14] V. R. Basili and D. M. Weiss, "A Methodology for Collecting Valid Software Engineering Data," *IEEE Transactions on Software Engineering*, vol. SE-10, no. 6, pp. 728–738, 1984.

[15] R. V. Solingen and E. Berghout, *The Goal/Question/Metric method: A Practical Guide for Quality Improvement of Software Development*. McGraw-Hill International, 1999.

[16] A. Neely, J. Mills, K. Platts, H. Richards, M. Gregory, M. Bourne, and M. Kennerley, "Performance Measurement System Design: Developing and Testing a Process-based Approach," *International Journal of Operation & Production Management*, vol. 20, no. 10, pp. 1119–1145, 2000.

[17] T. Lester, "Measure for Measure," http://www.ft.com/cms/s/2/31e6b750-16e9-11d9-a89a-00000e2511c8.html#axzz1ImHJOLmg, 5. October 2004, Accessed: 2011-04-27 11:00AM CEST.

[18] A. Neely and M. Bourne, "Why Measurement Initiatives Fail," *Measuring Business Excellence*, vol. 4, no. 4, pp. 3–6, 2000.

[19] S. M. Bird, D. Cox, V. T. Farewell, H. Goldstein, T. Holt, and P. C. Smith, "Performance Indicators: Good, Bad, and Ugly," *Journal Of The Royal Statistical Society. Series A (Statistics in Society)*, vol. 168, no. 1, pp. 1–27, 2005.

[20] D. M. Eddy, "Performance Measurement: Problems and Solutions," *Health Affairs*, vol. 17, no. 4, pp. 7–25, 1998.

[21] V. Masayna, A. Koronios, J. Gao, "A Framework for the Development of the Business Case for the Introduction of Data Quality Program Linked to Corporate KPIs & Governance," in *Proceedings of the 2009 Fourth International Conference on Cooperation and Promotion of Information Resources in Science and Technology (COINFO'09)*. IEEE Computer Society, 2009, pp. 230–235.

[22] C. Rodríguez, F. Daniel, F. Casati, and C. Cappiello, "Computing Uncertain Key Indicators from Uncertain Data," in *Proceedings of 14th International Conference on Information Quality (ICIQ'09)*. HPI/MIT, 2009, pp. 106–120.

[23] C. Rodríguez, F. Daniel, F. Casati, and C. Cappiello, "Toward Uncertain Business Intelligence: the Case of Key Indicators," *Internet Computing*, vol. 14, no. 4, pp. 32–40, 2010.