2018

# Common controls driven conceptual leadership framework

Mussalo, Petteri

Finnish Journal of eHealth and eWelfare

Tieteelliset aikakauslehtiartikkelit



http://dx.doi.org/10.23996/fjhw.68821

https://erepo.uef.fi/handle/123456789/6678

FinJeHeW Finnish Journal of eHealth and eWelfare

SCIENTIFIC PAPERS

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

# Common controls driven conceptual leadership framework

Petteri Mussalo, Virpi Hotti, Anastasia Kirjanen, Henna Lauronen, Hannu Härkönen, Juho Huikari, Jukka Holopainen

School of Computing, University of Eastern Finland, Kuopio, Finland

**Virpi Hotti, School of Computing, University of Eastern Finland, 70211, Kuopio, FINLAND. Email: virpi.hotti@uef.fi**

## Abstract

The forthcoming social welfare and healthcare reform in Finland with its organizational, financing and steering changes challenges the leadership. All service systems levels of the social welfare and healthcare have to achieve performance objectives whilst at the same time also meeting conformance requirements. However, there are hundreds authority documents (e.g., best practices, guidelines, regulations and standards) the common controls of which are adapted partly manually and partly by leveraging automation in organizations. Leaders review and develop their practices around performance and conformity (i.e., conformance or compliance) within frameworks that are mainly the sets of principles. However, the common controls affect into the main tasks of the governance (i.e., direct, evaluate and monitor). Therefore, we construct a conceptual leadership framework to highlight the meaning of the common controls and the meaning of criteria for performance and conformity. The constructed framework contains the terms (e.g., a control objective, decision criteria, event, insight, and transaction) that are mainly defined in the glossaries of the authority documents. The terms are used to find out terms and definitions for the leadership framework to figure out cognitive meanings for the concepts of the common controls driven leadership.

**Keywords:** authorization, conformity, control, framework, insight, leadership, performance

## Introduction

Forthcoming reform is changing the Finnish public funded social welfare and healthcare during the next years [1]. There are 18 regions that organize the healthcare and welfare with producers such as public financed organizations, private or third part companies [2]. Despite the selected funding model - either by capitation, service compensation or personalized budgeting basis - the operators, both organizers and producers, need applicable monitoring and control methods from early preparation phases. Developing an organization network to fulfill the requirements of the reform requires a comprehensive legal, administrative and patient centric service system.

There are hundreds authority documents (e.g., best practices, guidelines, regulations and standards) that the organizations have to have “consistent follow-up, accountability, or business impact analysis” [3]. Furthermore, the authorities draw up codes of conduct intended to contribute to the proper application of the authority documents. Further, associations and other bodies may prepare codes of conduct (or amend or extend such codes) for specifying the application of the authority documents. The authorities shall collate the

approved codes of conduct in a register and make them publicly available [4] as well as monitoring the approved codes of conduct. When the codes of conduct are as regulatory concepts and expectations, then they present considerable challenges for the organizations and the conduct risks will be the most meaningful [5].

The organizations have to gather and share the authority documents as well as deciding how to adapt the authority documents. Furthermore, the mandates of the authority documents have to assign to roles for accountability and tracked to completion. Further, the organizations publish their own code of conduct. Summarily, when the organizations adapt authority documents and related codes of conduct (and measures, etc.), then they need structured accountability and oversight with workflows, tasks, and audit trails. Therefore, both conceptual and technological frameworks are needed to decrease "correlation between a preference for ambiguity and a desire to justify one's questionable behavior" [6].

The government-mandated compliance requirements have been presented, for example, in the Health Insurance Portability and Accountable Act (HIPAA), in the Sarbanes Oxley Act (SOX), and in the EU General Data Protection Regulation (GDPR). Organizations have to "held accountable for meeting their compliance obligations" [7]. Therefore, the GRC (Governance, Risk, and Compliance) tools are adapted. However, the organizations are "seeking to streamline and rationalize frameworks" [7] to reduce the diversity of the authority documents. The common control concept is used illustrate requirements or obligations that are derived from the authority documents and are controlled by the same party of parties. However, the statement of the authority documents might be ambiguous which complicates the formation of the common controls.

There are post problems if something is beyond the reach of the authority documents (e.g., HIPAA) [8]. Hence, oversight has to based on wide ranges of the common controls that are derived from authority documents (Figure 1).

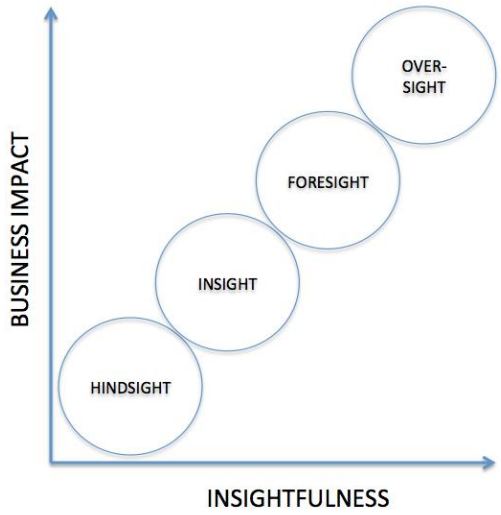


**Figure 1.** From reporting to conformity: Insight is obtained from historical data using reports, scorecards, and other methods; Foresights are created using modeling techniques; Oversight provides a standardized way to monitor the operations.

In this study, we construct a conceptual leadership framework to highlight the meaning of criteria for performance and conformity to achieve the common controls based justifications. A framework has defined to be a “set of principles” or a “high level structure, identical core text, common terms and core definitions” [9]. The common controls based conceptual leadership framework (Section 3) is a construction that will be a high-level structure the terms of which are defined in the authority documents. Our construction based on terms the definitions of which are commonly used in the authority documents mainly in governance and management systems standards (Section 2).

## Material and methods

When 58 hits of the Scopus search TITLE (framework OR model OR construction) AND TITLE (compliance OR conformity OR conformance) AND TITLE ("common control" OR control) have been appraised, then non common controls framework found. However, when 259 hits of the Google search (compliance OR conformity OR conformance) AND framework AND "intitle:common control" have been appraised, then three common controls frameworks found, i.e. the Common Controls Framework (CCF) by Adobe, the Unified Compliance Framework (UCF) and the Common Security Framework (CSF) by HITRUST.

The Common Controls Framework (CCF) represents the requirements of six authority documents (e.g., ISO/IEC 27001) by 273 common controls [10]. The Common Security Framework (CSF) is built for healthcare takes into the considerations 19 authority documents (e.g., COBIT, HIPAA, ISO/IEC 27001 and NIST) by 135 control specifications [11]. The Unified Compliance Framework (UCF) represents more than 800 authority documents (e.g., COBIT, GDPR, HIPAA and ISO/IEC 27001) by tagging citations and their associated mandates (more than 200 000) for common controls [12]. There is the comparison between CSF and UCF [13]. However, we did not compare the common controls frameworks because there are differences in selected authority documents and formations of the common controls.

We exemplified the UCF common controls because UCF offers the Common Controls Hub. GDPR is mapped into 1497 common controls. The common controls (i.e., mandated, implied and implementation ones) are described as follows: the mandate controls are assigned to roles for accountability and tracked to completion, implementation controls illustrate how to carry out the mandate controls and implied controls that “are found within each mandated control's genealogy” [14]. Citations of the authority documents are mapped into the common controls that are grouped by IT impact zones (e.g., Leadership and High Level Objectives, Audits and Risk management, Monitoring and measurement, Third Party and supply chain oversight), types and classifications (e.g., corrective, detective or preventive). There are 15 top level controls (e.g., 8 - Privacy protection for information and data). For example, the common control 902 is the top level control (i.e., Records Management) and it has several implementation support controls. However, the implementation support controls of the common control 902 do not refer to any other GDPR articles (i.e., only the common control 902 is based on the cited GDPR article).

In the UCF presentation context [3] the structure of governance and compliance is presented - common controls are related within metrics and assets, assets are related within configuration items, the relationship between the common controls and assets contains roles, events, audits, functions, tasks and records (i.e., collections of fields). However, governance frameworks (e.g., ISO/IEC 38500:2015 [15] and COBIT) contain usually three main tasks of the governance: evaluate, direct and monitor. Furthermore, the main tasks are mapped into principles. For example, the tasks are all mapped into responsibility, acquisition and performance, whereas, the evaluation and monitor tasks are mapped within conformance [16]. Some governance frameworks contain some self-explanatory principles (e.g., meeting stakeholder needs [17]).

The UCF compliance dictionary [18] offers the counted definitions of the terms in citations and controls. The existing frameworks and glossaries contain definitions of the terms that can be used to construct new concep-

tual frameworks. The reasons for the selected glossaries (Figure 2) are as follows:

- Annex SL [19] contains proposals for management system standards [20]. For example, two most popular management standards for quality management (ISO 9001:2015) and for information security management (ISO/IEC 27001:2013) are based on Annex SL. Annex SL contains the terms and the definitions of them that are taken into the considerations in managements system standards.
- We research the ISO/IEC 27000:2016 [21] because it contains terms used in ISO 27004:2016 [22]. In ISO 27004:2016 the clauses or controls of ISO/IEC 27001:2013 are related within measures the descriptors of which are an ID, information need, measure, formula/scoring, target, implementation evidence, frequency, responsible parties, data source, and reporting format. According to our understanding, other governance or management standard do not have such detailed descriptions of the control related measures. Furthermore, varieties of attributes have been realized to use in metrics such as the degree to which a control reduces either the likelihood of the occurrence or consequence of the occurrence of an event.
- Glossaries from AXELOS [23] and ISACA [24] contain terms including the most famous frameworks that have been deployed, for example, into project management (e.g., Prince), service management (e.g., ITIL) and governance (e.g., COBIT).
- The TOGAF content metamodel [25] relates the control within the process entity that is further related within the entities such as an event, function, product and service. However, the TOGAF content metamodel does not have measures that are related to the codes of conduct.

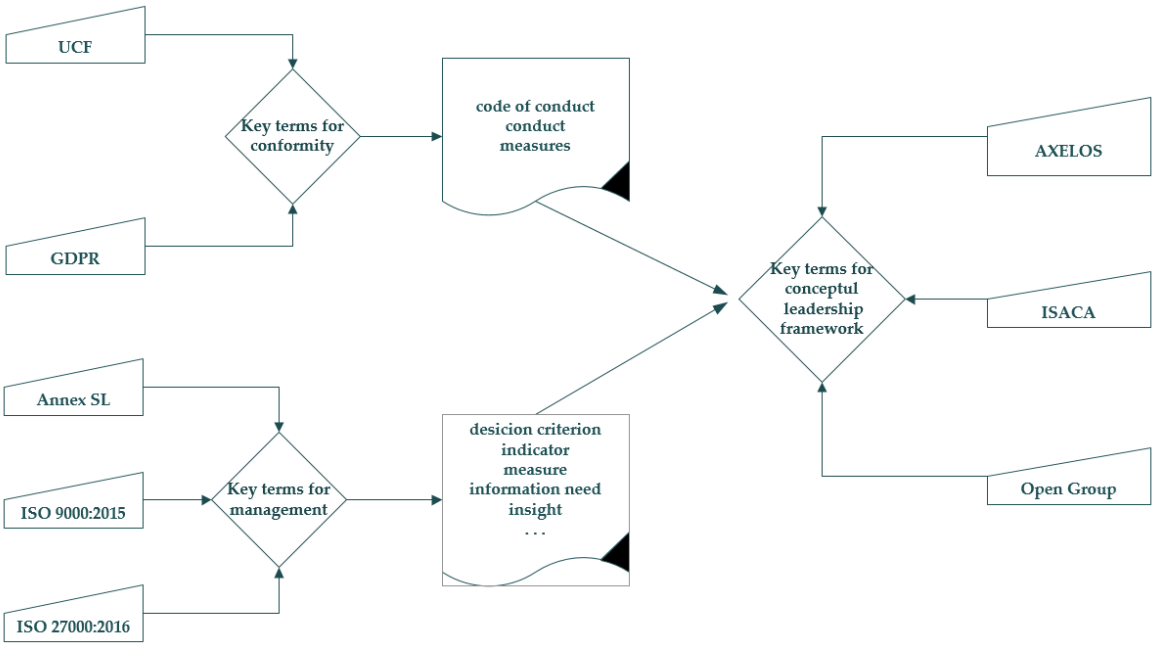


**Figure 2.** Used glossaries to find terms and definitions of the conceptual leadership framework.

There are several concepts and terms that are related within conformity and performance. First, we tabulated (Table 1) the terms from ISO/IEC 27000:2016 (2.5, 2.13, 2.15, 2.16, 2.19, 2.52, 2.56, 2.59, 2.60, 2.61, 2.68, 2.84) [26]. Second, we added terms around insights from ISO/IEC 27000:2016 (2.4, 2.20, 2.21, 2.25, 2,29, 2.30, 2.31, 2.47, 2.48) [26]. Third, we picked up more action terms as follows: a preventive action (3.12.1) from ISO 9000:2015 [27], activity [24] and transaction [24]. The rest of the selected terms include in authorization ones (i.e., code of conduct, conduct, and control) [18]. Finally, we mapped reference numbers (if any) of the selected terms into the table. We used the tabulated terms to find out terms and definitions for the leadership framework to figure out cognitive meanings for the concepts of the common controls driven leadership.

**Table 1.** Sources of terms and definitions. The numbers are references to subcategories of the standards. 'x' means that term is used in that glossary. Missing terms are marked with '-' sign. If the term or its definition need an additional explanation or remark, the numbered footnote is used.

| Term | Annex SL | ISO 9000:2015 | ISO 27000:2016 | UCF | Open Group | AXELOS | ISACA |
|---|---|---|---|---|---|---|---|
| activity | - | x[3] | - | x | - | x | x |
| attribute | - | - | 2.4 | x | - | x | - |
| audit | 3.17 | 3.13.1 | 2.5 | x | - | x | x |
| code of conduct[1] | - | - | - | x | - | - | - |
| conduct[1] | - | - | - | x | - | - | - |
| conformity | 3.18 | 3.6.11 | 2.13 | x | - | x[4] | x[4] |
| continual improvement | 3.21 | 3.3.2 | 2.15 | x | - | x | x[5] |
| control | - | - | 2.16 | x | x | x | x |
| corrective action | 3.20 | 3.12.3 | 2.19 | x | - | x | - |
| data | - | 3.8.1 | 2.20 | x | x | - | - |
| decision criteria | -. | .- | 2.21 | x[6] | - | - | - |
| event | - | - | 2.25 | x | x | x | x |
| governing body | - | - | 2.29 | x | - | - | x |
| indicator | - | - | 2.30 | - | x | - | x |
| information | - | 3.8.2 | 2.31[2] | x | - | - | x |
| insight | - | - | 2.31[2] | x | - | - | - |
| measure | - | - | 2.47 | x | x | - | x |
| measurement | 3.16 | 3.11.4 | 2.48 | x | - | - | - |
| monitoring | 3.15 | 3.11.3 | 2.52 | - | - | x | - |
| objective | 3.8 | 3.7.1 | 2.56 | x | x | x | x |
| performance | 3.13 | 3.7.8 | 2.59 | x | x | - | x |
| policy | 3.7 | 3.5.8 | 2.60 | x | - | x | x |
| preventive action | - | 3.12.1 | - | x | - | - | - |
| principle | - | - | - | x | x | - | x |
| process | 3.12 | 3.4.1 | 2.61 | x | x | x | x |
| risk | 3.9 | 3.7.9 | 2.68 | x | - | x | x |
| top management | 3.5 | 3.1.1 | 2.84 | x | - | - | x |
| transaction | - | - | - | - | - | x | x |

[1] from GDPR, [2] information need is an "insight necessary to manage objectives (2.56), goals, risks and problems", [3] in the project management context, [4] compliance, [5]countinuous improvement, [6]decision criterion, [7]top-level management

## Conceptual leadership framework

A code of conduct enforces desirable conduct and responsible behavior. It includes the policies of different kinds (e.g., behaviors policy, use policy, a sanction policy and procedure) [18]. A conduct refers to manage, control, organize or carry out something as well as behaving in a particular manner – it is "the leader of a performance" [18]. The conduct enforces measures and it is a category for analyze and quantify, as well as, the conduct of a different kind (e.g., sanctionable conduct) [18]. A measure is defined a "variable to which a value is assigned as the result of measurement" [21].

When a person or body has powers and rights to command or give a decision or permission to do something, then there is an authorization to do something [18]. The governing body focuses on a person or group of people who are accountable for the performance and conformance of the organization [18,21]. The top management is a "person or group of people who directs and controls an organization at the highest level" [19].

Conformity is "fulfilment of a requirement" where a requirement is a "need or expectation that is stated, generally implied or obligatory" [19]. Performance is a "measurable result" [19] or a "measurement of the overall time taken to carry out one or more transactions" [18]. Furthermore, continual improvement is a "recurring activity to enhance performance" [19].

In general, a risk is "an effect of uncertainty on objectives" [21] or "an uncertain event of set of events" [23]. "The purpose of a control is to modify risk" [26]. An objective is a "result to be achieved" [19]. The objective can be strategic, tactical, or operational. Furthermore, ISO/IEC 27000:2016 specify a control objective that is "statement describing what is to be achieved as a result of implementing controls" where a single control is a "measure that is modifying risk" [21] and a control objective is a "statement describing what is to be achieved as a result of implementing controls" [21]. In the framework, a control means either one or more adapted clauses or statements of the authority or policy documents. Annex SL defines a policy to be formally expressed "intentions and direction of an organization" [19]. When a principle is defined a "qualitative statement of intent that should be met by the architecture" and it "has at least a supporting rationale and a measure of importance" [25], then controls contain adapted principles. Further, we used adapted measures to illustrate that the adapted controls have corresponding measures. Further, we use adapted controls to illustrate correct, detect or prevent actions for uncertain events. We added a transaction to illustrate accountable things whereas events are occurrences.

In the framework, direct means that the top management adapts authorizations (e.g., codes of conduct, controls, and measures) as well as interpreting insights and gives justifications (e.g., to enter into a contract to do something or give the right to do something). When the top management set a decision criteria then they define their information needs (i.e., insights necessary to manage objectives, goals, risks and problems [21]). The decision criterion is "thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result" [21], which refers the possibilities to use analytics of different kinds.

In general, evaluate means "to assess or form an idea of the nature, quality, ability, amount, number, or value of something" [18]. The evaluation task is divided into three sub-tasks: indicate, extrapolate and optimize. In the framework, we want to highlight the usefulness of analytics of different kinds (e.g., retrospective, predictive and prescriptive analytics). Therefore, both aggregated and inferred insights are generated. Indicate means that there are indicators that are the aggregated insights the value of which is a "measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs" [21]. Further, analytical model algorithms or calculations combine "one or more base measures and/or derived measures with associated decision criteria" [21]. Extrapolate means that there are the inferred insights used to predict the future. Optimize means that there are insights that can be used to prescribe the options for decision-making.

In general, monitor means "determine a status" [27]. Moreover, conformance is monitored to policies and performance against plans [15]. We included the following terms in the monitor task: correction action, preventive action and monitoring. A correction action (correct something in the framework) is an "action to eliminate the cause of a nonconformity and to prevent recurrence" [19]. A preventive action (prevent something in the framework) is an "action to eliminate the cause of a potential nonconformity or other potential undesirable situation" [27]. Monitoring (detect something in the framework) is repeated observation of configuration items, systems, activities, IT services or processes to detect events and to ensure that the status is known [19,23].

We can exemplify the common controls driven conceptual leadership framework with pictorial frames (Figure 3). However, the pictorial frame without consensus between the used terms and definitions within interest parties (i.e., stakeholders) does not promote the development of the organization. Therefore, the organizations have to define concepts the cognitive meanings of which are clarified and draw pictorial frames by adapting the concepts of the presented framework. However, behaviors need justifications which can be achieved by aligning criteria for performance and conformity by insights of events and transactions.

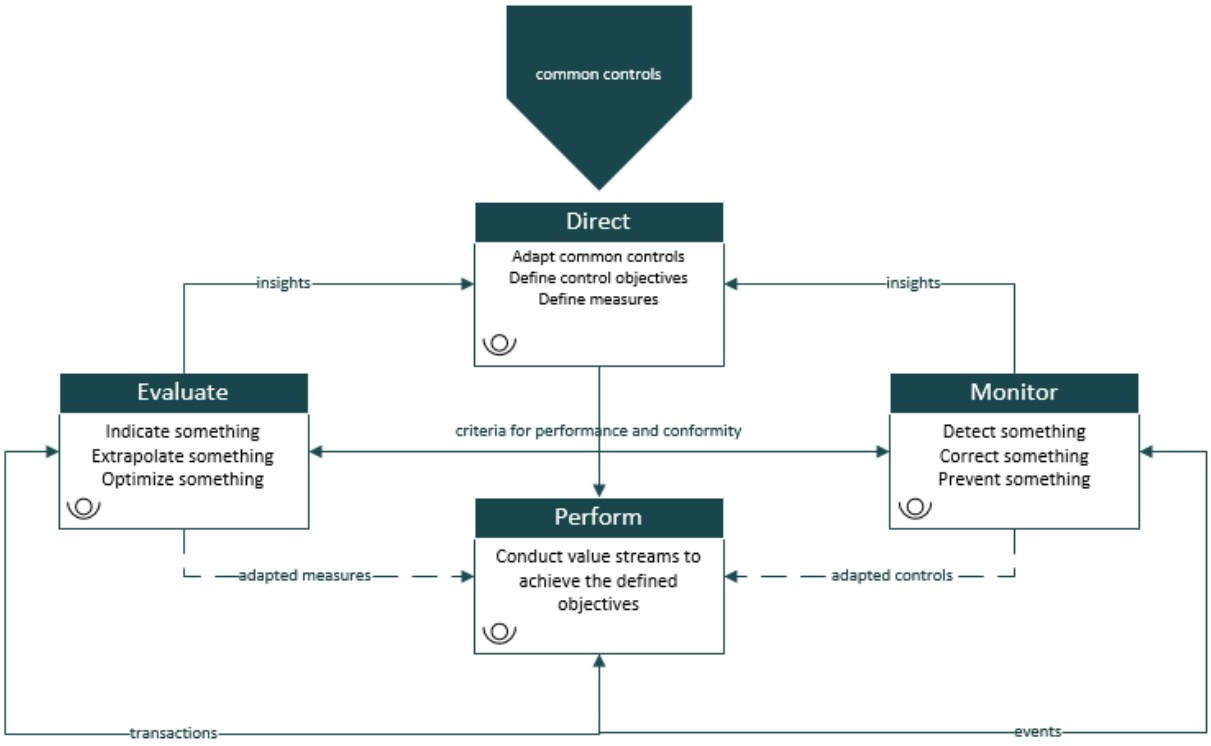


**Figure 3.** The direct task sets criteria for performance and conformity, the evaluate task adapts measures and indicates, extrapolates and optimizes transactional data, the monitor task adapts controls and corrects, detects and prevents occurrences based on event data. The direct task gets insights to fulfill an information need. Perform illustrates operational functions where value streams (e.g., series of activities) are conducted to achieve the defined objectives.

We do not explicitly highlight how criteria for performance and conformity will be achieved. There is no set of common controls that can be deployed directly. The common controls have to be adapted and supplemented, for example, by the common controls that are derived from national regulations. For example, the UCF common controls are possible to leverage within ServiceNow [28] that is a service management system where the common controls are mapped into policy statements [29]. Furthermore, there are regulatory technologies (i.e., regtech) to automate such as employee surveillance, compliance data management, fraud prevention, and audit trail capabilities [30].

## Discussion

Healthcare is globally strictly regulated business to set the rules for operations, protect individuals and individual intimacy for unintended data use [31,32]. In Europe, patient data management is regulated with the specific European Union directive and the member state legislation. Regulations regarding to person health status, genetic data and biometric data need a higher protection standard. The authority documents such as legislation [e.g., 33,34], administrative regulations [e.g., 35], national guidelines [36], and local policies [e.g., 37] instruct healthcare at all organizational and operational levels. There are also many principles and de-facto standards to standardize the healthcare operations at operational level. For example, evidence based medicine [38,39] gives recommendations for clinical practices.

During the last decades new administrative approaches (e.g., Lean [40] and Triple-Aim [41]), new treatment methodologies (e.g., a gene therapy) and new technologies are leveraged to both operational and leadership purposes [42,43]. At the same time, the outsourcing and subcontracting have increased [44] to even out the public-sector service demand and resource fluctuation. However, there is a need to reframe the wholeness to see its pervasiveness, i.e., leaders need to review and develop their practices around performance and conformity. For example, the outsourcing and subcontracting agreement monitoring (e.g., time of delivery as well quality features) is difficult and time consuming due complex organizational issues and complex information systems. In addition to administrative regulations there are also operational issues, for example purchase, delivery and outsourcing agreements. All of them need continuous attention.

The common controls are essential drivers when even efficiency and quality issues of the clinical operations are evaluated and monitored. Social welfare and healthcare are complex areas of business. Comprehensive operation monitoring at all service system levels is necessary for efficiency and quality. Without common controlling guidelines, the monitoring of the service system will become easily time consuming, inefficient and expensive. The well-defined leadership framework with comprehensive common controls as well shared definitions will relieve the organizations to control definition, metric definition and metric development. Using the common controls and shared definitions of the leadership concepts will enable extensive monitoring. In addition, the shared definitions will enable comparable scores to be calculated. Quality issues have been topical since Donabedian's pioneering article at 1978 [45]. The following examples are the quality assessment ones:

- Pioneering hospital in Finland was Kuopio University Hospital certifying first ISO 9000 based quality system at the beginning of 1990's [37]. Specialty based quality programs became more common at the beginning of 2000's [46]. During implementation of the Kuopio University Hospital (KUH) quality system it was self-clear to control the quality - data have been collected from hospital information systems at early stages, the responsible statistician analyzed data and produced the monthly statistics and results were published for all staff within KUH.
- In Finland, intensive care units (ICU) have together carried out the benchmarking project since 1994. Outcome measurement, quality assessment and benchmarking are based on scientifically validated metrics, shared dataset and sophisticated data collection tools. It is possible to say that because of the project the intensive care results have smoothly improved. [43]

- In Sweden, the clinical quality assessment is advanced. The government administrates the national quality registries (QRs) of individual clinical data to review, analyze and improve the healthcare delivery. QR's autonomy is high, which has led to overlapping data sets and lack of cooperation between the QRs [47]. Therefore, the QRs need systematical development, a strategic plan and willingness to overcome the isolationism [48]. However, the QRs are seen valuable source for quality improvement - QRs advantage the operation efficiency and they help in standardizing the operations.

In Finland, the forthcoming social welfare and healthcare reform aims are quite the same they were in Norway and in Sweden. The reform will meet the requirements to decrease costs, improve service availability, improve service integration and improve population equal possibilities to get the services. Despite the current tight schedule, the reform effectiveness should be monitored. Common controls, common metrics and standardized methodologies enable the monitoring success. The presented leadership framework encourages to adapt the controls and corresponding metrics at all service system levels, which makes the monitoring at different levels easier and more reliable. Irrespective on the financing model fulfilling the reform targets in primary care the operations require more attention. The presented framework encourages to solve the controlling and monitoring needs during the early stages of the reform.

Already at 2005 World Health Organization (WHO) emphasized the importance of performance analysis and improvement [49]. Hence, National Health Services (NHS) leadership model calls for looking new perspectives, creating data driven insights and developing new concepts based on data, insights and perceptive analysis [50]. The presented framework supports government-mandated approach and the usefulness of analytics of different kinds (e.g., retrospective, predictive and prescriptive analytics).

Conformity is achieved via standards, or other non-legal authority documents, that are directly or indirectly legally enforceable [51]. Sometimes authority documents might be vague. Therefore, there are common controls, codes of conduct and metrics such as defined in ISO/IEC 27004:2016. Specific instructions do not crowd motivation and harm performance [7]. However, governance (the main tasks of which are to evaluate, to direct and to monitor) guarantees conformity as well as liberating opportunities [52]. When we have ability to adapt and audit common controls, then we will achieve a pervasive level where oversights promote both conformity and performance. Pervasive business intelligence refers "capturing the business data and getting the right information to the right people, at the right time, through the right channel" [53]. By analogy, pervasive conformity refers capturing both controls and data and getting the right insights to the right people, at the right time, through the right channel. "If the user cannot fully understand data, she cannot perceive the utility of the information provided" [53] and by analogy, if the user cannot fully understand common controls, she cannot detect, correct or prevent something based on the insights of the events, or she cannot indicate, extrapolate or optimize something based on the insights of the transactions.

## Conclusion

In this study, we proposed the conceptual leadership framework that can be used to highlight the meaning of the common controls and the meaning of criteria for performance and conformity. We figured out the usable terms the definitions of which are commonly used in authority documents (e.g., management systems standards). Furthermore, we reviewed three common controls frameworks and we realized that the Unified Compliance Framework (UCF) provides concreteness around the common controls based on several authority documents. However, the leaders have to have abilities to adapt common controls, codes of conduct and metrics as well as defining objectives and controls. Further, each adapted metrics (or measures) has to be related within an insight that can be the required indicator (or the accountable thing) or combination of the insights. Therefore, the leadership has to based on the

define concepts the cognitive meanings of which are clarified by with whom the leading model affects.

We assess the accuracy of the results by the three aspects of the validity. Construct validity based on 28 terms and their definitions that are used to define concepts the explanations of which are mainly cited statements (i.e., terms and definitions) from the selected glossaries of the authority documents. Internal validity based on the factors (i.e., the terms and definitions from ANNEX SL, ISO 9000:2015, ISO/IEC 27000:2016, AXENOS, and ISACA) that affect directly the studied factor (i.e., the concepts in the conceptual leadership framework). External validity of the used terms and definitions is obvious because of the glossaries.

The presented common controls based conceptual leadership framework promises to support organizations to improve the understanding overall governance status in light of controls and insights. Continuous control as well awareness of the organization governance status will improve organization performance and release resources to organization development tasks. More research is required to find out the reasonable use cases (e.g., clinical practice assessment and outsourced service level assessment) and related common controls, especially for healthcare and welfare. Furthermore, there are two main steps within tools such as ServiceNow instruct the selected common controls are adapted within criteria for performance and conformity, as well as, for monitorable controls of events and evaluable metrics of transactions. The top management or governing body has to have abilities to reduce conduct risks, i.e., the leaders have to have abilities to assess impacts of different kinds based on analytics and other decision-making tools. Moreover, the most important duty of the top management or governing body is to guarantee a sense of security, especially, for them who add value into value streams by the defined criteria of performance and conformity.

## References

[1] Finnish Government. Health, social services and regional government reform to enter into force on 1 January 2020, county elections in October 2018. Available at: http://alueuudistus.fi/en/artikkeli/-/asset_publisher/10616/sote-ja-maakuntauudistus-voimaan-1-1-2020-maakuntavaalit-lokakuussa-2018?p_p_auth=lhkTtpwi.

[2] Finnish Government. Services and freedom of choice. Available at: http://alueuudistus.fi/en/services-and-freedom-of-choice/language-rights.

[3] GRC 20/20 Research, LLC. Common Controls Hub Innovations Break New Ground – Innovation in Regulatory Intelligence for Compliance Management, October 2015.

[4] The European Parliament or the Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[5] English S, Hammond S. Cost of compliance 2016. Thomas Reuters; 2016. Available at: https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/report/cost-compliance-2016.pdf.

[6] Boussalis C, Feldman Y, Smith HE. Experimental analysis of the effect of standards on compliance and performance. Regulation and Governance, 2017;1–11. https://doi.org/10.1111/rego.12140

[7] Hayden L. Designing common control frameworks: A model for evaluating information technology governance, risk, and compliance control rationalization strategies. Information Security Journal 2009;18(6):297–305. https://doi.org/10.1080/19393550903324936

[8] Terry N. Existential challenges for healthcare data protection in the United States. [Des défis existentiels pour la protection des données de santé aux États-Unis] Ethics, Medicine and Public Health, 2017;3(1):19–27. https://doi.org/10.1016/j.jemep.2017.02.007

[9] ISO. Glossary – Guidance on selected words used in the ISO 9000 family of standards. 2016. Available at:

https://www.iso.org/files/live/sites/isoorg/files/standards/docs/en/terminology-ISO9000-family.pdf.

[10] Adobe. Compliance overview. Available at: https://www.adobe.com/content/dam/acom/en/security/pdfs/AdobeCloudServices_ComplianceOverview.pdf.

[11] HITRUST. The HITRUST Common Security Framework: A revolutionary way to protect electronic health information. Available at: https://hitrustalliance.net/content/uploads/2014/01/HITRUST-CSF-Brochure.pdf

[12] Unified Compliance. How the UCF Works. Available at: https://support.commoncontrolshub.com/hc/en-us/articles/211837123-How-the-UCF-Works.

[13] HITRUST. Comparing the CSF and the Unified Compliance Framework. Available at: https://hitrustalliance.net/documents/csf_rmf_related/HiTrustUCFDatasheet.pdf.

[14] Unified Compliance. What is the difference between an Implied, Mandated, and an Implementation Control? Available at: https://support.commoncontrolshub.com/hc/en-us/articles/204278525-What-is-the-difference-between-an-Implied-and-a-Mandated-Control-.

[15] ISO/IEC. ISO/IEC 38500:2015 (en) Information technology — Governance of IT for the organization. Available at: https://www.iso.org/standard/62816.html

[16] SFSedu. Available at: http://www.sfsedu.fi/files/122/ISO-38500.ppt.

[17] ISACA. COBIT 5 Principles. Available at: http://www.isaca.org/Knowledge-Center/Academia/Pages/cobit-5-principles.aspx.

[18] Unified Compliance. Compliance Dictionary. Available at: https://compliancedictionary.com/.

[19] ISO/IEC. Annex SL (normative) - Proposals for management system standards. ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2016. Available at: http://isotc.iso.org/livelink/livelink/fetch/-10469877/10469901/16474137/Annex_SL__ISO_Directives_2016_7th_edition.pdf?nodeid=17859835&vernum=-2.

[20] ISO. ISO Management System Standards. Available at: https://www.iso.org/management-system-standards-list.html.

[21] ISO/IEC. ISO/IEC 27000:2016(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

[22] ISO. ISO/IEC 27004:2016 Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation.

[23] AXELOS. Best Management Practice portfolio: common glossary of terms and definitions. Version 1, October 2012. Available at: https://www.axelos.com/glossaries-of-terms.aspx.

[24] ISACA. Glossary. Available at: https://www.isaca.org/Pages/Glossary.aspx.

[25] The Open Group. 34. Content Metamodel. Available at: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap34.html.

[26] ISO. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements.

[27] ISO. ISO 9000:2015(en) Quality management systems — Fundamentals and vocabulary. Available at: https://www.iso.org/obp/ui#iso:std:iso:9000:ed-4:v1:en.

[28] ServiceNow. Preparing for the General Data Protecting Regulation (GDPR). ServiceNow Governance, Risk and Compliance. Available at: https://www.servicenow.com/content/dam/servicenow/documents/whitepapers/wp-preparing-for-the-gdpr.pdf.

[29] ServiceNow. Use the Unified Compliance Framework (UCF) with Policy and Compliance Management. Available at: https://docs.servicenow.com/bundle/helsinki-governance-risk-compliance/page/product/grc-ucf-import/concept/c_UCF-cch.html.

[30] Investopedia. Regtech. Available at: https://www.investopedia.com/terms/r/regtech.asp (accessed on 8 November 2017).

[31] Pelayo S, Bras Da Costa S, Leroy N, Loiseau S, MacKeon D, Trancard D, Beuscart-Zéphir M. Application of the medical device directive to software: methodological challenges. Studies in heal technology and informatics 2013;(192):437–441. DOI: 10.3233/978-1-61499-289-9-437.

[32] Bolognini L, Bistolfi C. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law & Security Review 2016;33(2):171–181. https://doi.org/10.1016/j.clsr.2016.11.002

[33] FINLEX ®. Terveydenhuoltolaki 1326 / 2010. Available at: https://www.finlex.fi/fi/laki/ajantasa/2010/20101326.

[34] FINLEX ®. Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016. Available at: https://www.finlex.fi/fi/laki/ajantasa/2016/20161397?search%5Btype%5D=pika&search%5Bpika%5D=hankintalaki.

[35] EUR-Lex. Ensuring medical devices are safe for patients 31993L0042. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0042.

[36] Duodecim. Käypähoito. Available at: http://www.kaypahoito.fi/web/english/home.

[37] Rissanen V. Quality system based on the standard SFS-EN ISO 9002 in Kuopio University Hospital. Int J Health Care Qual Assur Inc Leadersh Health Serv. 2000;13(6-7):266-72.

[38] Sackett DL, Rosenberg WMC, Gray JAM, Haynes RB, Richardson WS. Evidence based medicine: what it is and what it isn't. It's about integrating individual clinical expertise and the best external evidence. British Medical Journal (BMJ) 1996;312(7023):71–72. https://doi.org/10.1136/bmj.312.7023.71

[39] Beckmann JS, Lew D. Reconciling evidence-based medicine and precision medicine in the era of big data: challenges and opportunities. Genome Med 2016;8:134 https://doi.org/10.1186/s13073-016-0388-7

[40] Fournier P-L, Jobin M-H. Understanding before implementing: the context of Lean in public healthcare organizations. Public Money Manage 2018;38(1):37–44. https://doi.org/10.1080/09540962.2018.1389505

[41] Swarthout M, Bishop MA. Population health management: Review of concepts and definitions. Am J Health Syst Pharm. 2017 Sep 15;74(18):1405-1411. https://doi.org/10.2146/ajhp170025

[42] Grossglauser M, Saner H. Data-driven healthcare: from patterns to actions. Eur J Prev Cardiol. 2014;21(2 Suppl):14-7. https://doi.org/10.1177/2047487314552755

[43] Reinikainen M, Mussalo P, Hovilehto S, Uusaro A, Varpula T, Kari A, et al. Association of automated data collection and data completeness with outcomes of intensive care. A new customised model for outcome prediction. Acta Anaesthesiologica Scandinavica 2012;56(9):1114–1122. https://doi.org/10.1111/j.1399-6576.2012.02669.x

[44] Junnila ML, Fredriksson S. Palvelujen ulkoistus. Terveyden ja hyvinvoinnin laitos, 2012. Available at: http://urn.fi/URN:ISBN:978-952-245-720-2.

[45] Donabedian A. The quality of medical care. Science 1978;200(4344):856–864. https://doi.org/10.1126/science.417400

[46] van der Veer, S N, de Keizer NF, Ravelli ACJ, Tenkink S, Jager KJ. Improving quality of care. A systematic review on how medical registries provide information feedback to health care providers. Int J Med Informatics 2010;79(5):305-323. https://doi.org/10.1016/j.ijmedinf.2010.01.011

[47] Emilsson L, Lindahl B, Köster M, Lambe M, Ludvigsson JF. Review of 103 Swedish Healthcare Quality Registries. J Intern Med. 2015 Jan;277(1):94-136. https://doi.org/10.1111/joim.12303

[48] Adami HO, Hernán MA. Learning how to improve healthcare delivery: The Swedish Quality Registers. J Intern Med. 2015 Jan;277(1):87-9. https://doi.org/10.1111/joim.12315

[49] NHS Leadership Academy. Healthcare Leadership Model. Available at: https://www.leadershipacademy.nhs.uk/resources/healthcare-leadership-model/.

[50] World Health Organization (WHO). Strengthened health systems save more lives (2005). Available at: http://www.euro.who.int/en/health-topics/Health-systems/health-systems-financing/publications/2006/strengthened-health-systems-save-more-lives-2005.

[51] Bhimani A, Soonawalla K. From conformance to performance: The corporate responsibilities continuum. Journal of Accounting and Public Policy 2005;24(3):165–174. https://doi.org/10.1016/j.jaccpubpol.2005.03.001

[52] Ransbotham S, Kiron D. Analytics as a Source of Business Innovation. MIT Sloan Management Review 2017, Available at: http://sloanreview.mit.edu/projects/analytics-as-a-source-of-business-innovation/.

[53] Turricchia E. Pervasive Business Intelligence. PhD in Electronics, Computer Science and Telecommunication, Alma Mater Studiorum - University of Bologna; 2013. Available at: http://amsdottorato.unibo.it/5232/1/TURRICCHIA_ELISA_TESI.pdf.