Available online at: https://proceeding.researchsynergypress.com/index.php/rsfconferenceseries1
RSF Conference Series: Business, Management and Social Sciences
e-ISSN 2807-5803/p-ISSN 2807-6699
Volume 1 Number 5 (2021):116-124

Comparative Review of the Latest Concept in Compliance Management & The Compliance Management Maturity Models

Ridwan Hendra
Institute of Compliance Professionals Indonesia,
Parahyangan Catholic University

Abstract

Like many other management systems, the compliance management system needs to be measured to know how exemplary the implementation is. The Compliance management maturity model (CMMM) is one measurement method that can help the organization assess the degree of Compliance Management implementation and the effectiveness of compliance management practices to help the organization achieve its objectives. To determine and identify the state-of-the-art CMMM, this study will enumerate and synthesize current CMMM and map their similarities and differences. Furthermore, to determine if the existing enterprise CMMM can measure the current Compliance Management practices by using the ISO 37301 international Standard as a proxy for a state-of-the-art Compliance Management system. The synthesizing process of the enterprise CMMM uses the literature review approach on the existing CMMM and ISO 37301 as the primary benchmark reference. The findings show that despite organizations facing increasing complexity and organizational characteristics of internal and external regulations, the CMMM as Compliance Management measurement tools are very few. The result also shows that the existing CMMM cannot cover all the current CMMM requirements needed from the International Standard.

Keywords: Compliance Management, Maturity Model, ISO 37301

INTRODUCTION

The dynamic, turbulent, and complex business environment has compelled regulators and decision-makers to update or stipulate new laws, standards, and policies. Likewise, the situation forced the present-day organizations to update and make sure their business process always complies with the requirements. Compliance management is a difficult task requiring monitoring and reporting against a constantly changing and seemingly limitless set of rules, agreements, standards, regulations, and laws. Each area of compliance has its own set of rules. In many circumstances, it necessitates an in-depth understanding of esoteric technical subject matter as well as a comprehensive database for compliance requirements, measurement, and reporting. Regrettably, in many organizations, compliance management has formed and maintained a collection of silos, each serving its own purposes but not being coordinated across organizational levels. This tendency to "silo" often duplicates planning, redundant reporting systems, and misplaced priorities. As a result, it can waste the scarcest resource in business: management attention (Society of Corporate Compliance and Ethics, 2018).

International Organization for Standardization has established ISO 19600:2014 Compliance Management System – Guidelines and revised by ISO 37301:2021 - Compliance management systems — Requirements with guidance for use. Hopefully, the establishment of Compliance Management standards helps the organization support the diffusion of compliance management into the organization system because standards could provide comprehensive scientific and practical knowledge for everyone at a low cost (Anna Pohle, 2018). However, as with other management systems, the effectiveness of the system needs

Corresponding author
ridwan.npradja@gmail.com
DOI: https://doi.org/10.31098/bmss.v1i5.457

to be systematically measured. The measurement will help the organization to check how well their compliance management system as a reference for further corrective action to continuously improve their compliance management system as mentioned by Deming's PDCA Concept

At the organization level, the ineffectiveness of the Compliance system and inadequate maturity level may jeopardize the whole organization's value. Webster defines effectiveness as "producing a decisive or desired effect. We can identify what effectiveness means for an organization by (1) defining the program's goals, (2) determining how to measure whether the goals are met, and (3) measuring whether the goals are met using these definitions.

The current maturity model is heavily oriented in the disciplines of software development and software engineering. However, because software development is frequently managed as a project, its impact on information technology also has an impact on the maturity models used in project management. Furthermore, during the "quality revolution," product quality concepts became the foundation of most maturity models. (Alijoyo, Hendra, & Sirait).

Following the introduction above, the purpose of this research is to present the existing CMMM to uncover its state-of-the-art status and mapping the models' similarities and differences. Furthermore, the review of the CMMM is also to determine if the existing models are still relevant to the current dynamics of rules and regulations changes faced by the firms at the enterprise level within the aspect of practicality. Therefore, this study aims to comprehensively analyze the CMMM and its implications to compliance practitioners and researchers.

Compliance Framework

Obedience is not the same as compliance. When an individual alters his or her conduct as a member of an organization in response to another person's explicit or implicit request, this is known as compliance. Compliance is frequently referred to as an active form of social influence because it is usually begun by an individual. However, because it focuses on a change in overt conduct, it is sometimes thought of as an exterior form of social influence. Although internal changes in people's views or feelings can sometimes lead to compliance, they are not the primary purpose of compliance, nor are they necessary for the request to be effective.

Compliance is a continuous process that occurs when a business fulfills its commitments. Compliance is made durable by integrating it into the culture of the organization as well as the conduct and attitude of its employees. While maintaining its independence, compliance management integration with the organization's other management processes, operational requirements, and procedures is a must (International Organization for Standardization, 2021). On the other hand, obedience is a change in behavior prompted by direct instruction from a higher authority figure. As a result, obedience is a sort of active influence. It is frequently launched by an authority figure and is typically external in that directives are usually directed at overt conduct.

An organization can demonstrate its commitment to comply with relevant laws, regulatory requirements, industry codes, organizational standards, and standards of good governance, generally accepted best practices, ethics, and community expectations by implementing a practical, organization-wide compliance management system.

By using core values and commonly acknowledged good governance, ethical, and community norms, the leadership shapes the organization's approach to compliance. As a result, embedding compliance in the conduct of employees requires leadership at all levels, as well as acknowledging and implementing strategies to encourage compliant behavior. There is a risk of non-compliance if this is not the case at all levels of an organization.

Organizations can protect their reputation by avoiding or minimizing non-compliance with their compliance duties. By using binding values and adequate compliance management, integrity and successful compliance become key parts of good and active management. Organizations' socially responsible behavior is also aided by compliance. When it comes to shaping compliance culture within important constituencies inside a business, it's useful to look at the triggers. Senior leaders are typically affected by different compliance culture issues than middle managers and line staff. There must be a tone at the top, a mood in the middle, and a buzz at the bottom of the company.

When deciding the appropriate penalty to be imposed for violations of relevant legislation, courts in some jurisdictions have taken into account an organization's commitment to compliance through its compliance management system.

The ISO 37301:2021 - Compliance management systems — Requirements with guidance for use now contain requirements, with additional guidance based on those requirements. The standards also follow ISO's requirements for a harmonized structure for management system standards. The main difference between these ISO 19600 and ISO 37301 is that organizations can get certified against ISO 37301 by undergoing a conformity assessment via an independent third party.

Compliance Management Maturity Models (CMMM)

The maturity level measurement is not precisely the same as the conformity level measurement—the conformity level measure how an organization obeys authority figures, regulations, or standards. On the other hand, the maturity level measurement is beyond the conformity level measurement. Maturity level is not gained with age or time but by learning, understanding, and thinking. A maturity model is a forward-looking approach that measures the conformity to the standards and the capabilities and capacities of the organization to support the effectiveness of management system implementation. The maturity model assesses the creation of values, ethics, beliefs, and conduct across an organization, interacting with the organization's structures and control mechanisms to produce compliance-friendly behavioral norms.

There are challenges, however, in adapting maturity models to compliance. Some are maturity models initially developed and most often applied to software architecture and engineering development processes that present clear process metrics. Another challenge relates to the danger of defining a final maturity state, such as "optimization." That would raise the question of what happens when an organization defines itself as reaching the final level of a maturity model (Kusserow, 2020). Finally, to be fully useful for compliance, the factors and characteristics measured to support findings regarding the maturity level need to be detailed, precise, and exact. Too few factors and the maturity level decisions will rely too much upon the subjective judgment of reviewers.

To avoid subjective judgment as minimum as possible, a reference like a standard can be helpful. The ISO 37301 standard lays out standards as well as guidelines for compliance management systems and best practices. ISO 37301's requirements and advice are adaptable. As a result, depending on the size and maturity of an organization's compliance management system, as well as the context, nature, and complexity of its operations and objectives, its implementation may vary.

RESEARCH METHOD

The goal of this study is to present existing compliance maturity models, determine their state-of-the-art status, map model similarities, and differences, and determine whether existing compliance maturity models are still relevant to the current dynamics of rules and regulations faced by businesses at the enterprise level. A literature review is being used in this study.

The research design adapts from the approach used in the research conducted by (Alijoyo, Hendra, & Sirait). The variables employed in the analysis are the structure's perspective and the maturity models' assessment criteria.

It focuses on the model composition under the variables of the CMMM framework. The critical parts of the CMMM, as well as its maturity levels, were chosen to reveal a broad range of company compliance management maturity. As a result, the variables used to examine the model are (1) the number of essential parts or criteria in the model, (2) the number of maturity levels, (3) the lowest maturity level, and (4) the maximum maturity level.

When it comes to analyzing the CMMM assessment technique, it focuses on the model's application. As a result, the variables chosen focus on the CMMM's implementation and use in enterprises. As a consequence, it considers the variables of (1) assessment method availability, (2) identification of strong and weak spots, (3) continual improvement, (4) quantitative findings, and (5) qualitative outcomes.

In order to review whether the existing CMMMs are still relevant to the current dynamics of rules and regulations faced by the organization at the enterprise level, this research uses ISO 37301 clauses as a proxy benchmark for comparative review on how the implementation of the Compliance Management in today organization. This research use ISO 37301 because of several reasons:

1. The ISO 37301 is an international standard developed by compliance experts from various countries.
2. The ISO 37301 is the most recent generic standard in Compliance Management.

Furthermore, the research tries to uncover the gaps between the existing CMMMs measurements with the ISO 37301 requirements and recommendations by directly mapping the ISO 37301 clauses with the existing CMMMs measurements.

FINDINGS AND DISCUSSIONS

There is only a few existing concept or research around CMMM, especially in academic papers or research. In that regard, this paper use the CMMM from (Jackman, 2015) (Otte, Karen, Mudler, & Potter, 2018), (RSA Security LLC, 2020), and (Society of Corporate Compliance and Ethics, 2018), and (OCEG, 2016) as references. In addition, this paper uses ISO 37301 to analyze the models mentioned above to map and uncover the gap between the clauses in ISO 37301 that do not exist in the CMMM models or the other way around.

The research adopts the approach used in the research conducted by (Alijoyo, Hendra, & Sirait) to synthesis existing CMMM, as depicted in Table 1 below

Table 1. The Result of the Compliance Management Maturity Model

Variables	Jackman - 2015	Otte, Karen, Mudler, Potter - 2018	Society of Corporate Compliance & Ethics - 2018	RSA - 2020	OCEG - 2016
Number of key elements	5	8	7	4	4
Maturity levels	5	5	5	5	5
Highest maturity	Values-led	Basic	Excellent	Advantaged	Advantage
Lowest maturity	Non-compliance	Leading	Non-existent/ Poor	Siloed	Siloed
Assessment method availability	Yes	Yes	Unspecified	Unspecified	Unspecified
Strong or weak point identification	Yes	Yes	Unspecified	Yes	Yes
Continuous improvement	Unspecified	Yes	Unspecified	Yes	Yes
Qualitative results	Yes	Yes	Yes	Yes	Yes
Quantitative results	Unspecified	Yes	Unspecified	Yes	Yes

The table shows that all current maturity levels consist of 5 levels despite having a different name and different measurement elements. To know how relevant the measurement elements of the existing CMMM today are, this research use clauses in ISO 37301 Compliance Management International Standards as a proxy for Compliance Management system implementation requirements in today's organization. This research does not include (Society of Corporate Compliance and Ethics, 2018) because the model does not inform the information needed in the comparative review.

Table 2 and Table 3 below show that none of the existing CMMM could cover all the requirements from of ISO 37301 clauses. The highest percentage comes from (RSA Security LLC, 2020) and (OCEG, 2016). The root cause of these phenomena is because the CMMM from RSA just updated in 2020. The maturity model from OCEG is supposed to measure the integration of Governance, Risk Management, and Compliance Management (GRC) implementation. In that regard, the integrated measurement of GRC makes the OCEG maturity more comprehensive.

Regarding risks and opportunities, all the existing CMMM do not address opportunities in their measurements. All current observed CMMM focus on the negative side of the legal and compliance risks and how to manage the negative effect impact and likelihood to happen. In the high uncertainties' era, the organization not only built their resilience, but they also needed to build their agility. Agility and resilience are not the same things. Resilience is defined as the ability to resist, absorb, and respond to quick and/or disruptive changes, including recreating oneself if necessary. On the other hand, agility is the ability to move rapidly, flexibly, and decisively in predicting, initiating, and seizing opportunities while avoiding the adverse effects of change.

All the observed CMMM do not mention the investigation process in their measurement. However, according to the ISO 37301, the organization shall develop, establish, implement and maintain processes to assess, evaluate, investigate and close reports on suspected or actual instances of non-compliance. These investigation processes are needed for exemplary compliance management implementation to ensure fair and impartial decision-making.

(RSA Security LLC, 2020) CMMM includes management review in its measurement and is the only observed CMMM that includes continuous improvement. However, the (RSA Security LLC, 2020) CMMM did not include Leadership and Commitment in their measurement, while it stated clearly in other observed CMMM.

In order to make sure the observed CMMM in this research does not misinterpret as conformity check with the ISO 37301, the research also analyzed what characteristics or elements measured in the observed CMMM but obscure in the ISO 37301 clauses. The research found that the observed CMMM considers the readiness and organization capabilities level in managing compliance using technological advancement. Implementation and integration of technology into an organization's business activities, as well as exploiting its advantage to give risk-based information that the firm may utilize to develop effective plans, are among the models' qualities. In addition, the current CMMM tends to evaluate the firm's maturity in terms of its ability to forecast regulatory and compliance concerns in the future.

Table 2: Comparative review between existing CMMM with ISO 37301

No	ISO 37301	Jackman - 2015	Otte, Karen, Mudler, Potter - 2018	RSA - 2020	OCEG - 2016
	Context of the organization	67%	67%	83%	83%
1	Understanding the organization and its context	-	√	√	√
2	Understanding the needs and expectations of interested parties	-	-	√	√
3	Determining the scope of the compliance management system	√	√	-	-
4	Compliance management system	√	√	√	√
5	Compliance obligations	√	-	√	√
6	Compliance risk assessment	√	√	√	√
	Compliance leadership	100%	100%	67%	100%
7	Leadership and commitment	√	√	-	√
8	Compliance policy	√	√	√	√
9	Roles, responsibilities, and authorities	√	√	√	√
	Compliance management Planning	17%	17%	83%	83%
10	Actions to address risks and opportunities	1/2	1/2	1/2	1/2
11	Compliance objectives and planning to achieve them	-	-	√	√
12	Planning of changes	-	-	√	√

Table 3: Comparative review between existing CMMM with ISO 37301 (continued)

No	ISO 37301	Jackman - 2015	Otte, Karen, Mudler, Potter - 2018	RSA - 2020	OCEG - 2016
	Compliance management Support	20%	80%	80%	100%
13	Resources	√	√	√	√
14	Competence	-	-	√	√
15	Awareness	-	√	-	√
16	Communication	-	√	√	√
17	Documented information	-	√	√	√
	Operation of compliance management	25%	75%	75%	50%
18	Operational planning and control	√	√	√	√
19	Establishing controls and procedures	-	√	√	√
20	Raising concerns	-	√	√	-
21	Investigation processes	-	-	-	-
	Compliance management performance evaluation	0%	33%	100%	67%
22	Monitoring, measurement, analysis, and evaluation	-	√	√	√
23	Internal audit	-	-	√	√
24	Management review	-	-	√	-
	Continuous Improvement	0%	50%	100%	50%
25	Continual improvement		√	√	√
26	Nonconformity and corrective action		-	√	-
	Overall	37%	63%	79%	75%

CONCLUSIONS

The goals of this paper were to discover the similarities and differences among the CMMM as well as their current state-of-the-art status. The findings from the review suggest that there are similarities among the model, such as the number of levels of the reviewed compliance management maturity models to the absence of investigation process and opportunities aspect in their measurement. These two variables are critical measurements when included in the CMMM because the organization needs to specifically address opportunities to build its resilience and agility to survive in this rapidly changing environment. In addition, the effectiveness of the investigation process could help ensure the decision-making process in the organization from conflict of interests. This situation is very critical when organizations today become more interconnected and transparent. The current edition of CMMM takes into account the impact of technological innovation on businesses and their capabilities, as well as the possibility for new context changes and risks.

Following the findings of this research, it has its practical implication. The complexity and rapid change in today's environment make some CMMM unsuitable for today's organization. To a certain extent, the compliance practitioners have to regularly reassess the firm's maturity level and capability in practicing compliance management. The compliance professionals and academicians could also provide more accurate and practical steps to help the compliance management become more mature by using a suitable measurement.

Although the findings meet the research's objectives, they are not without flaws. The number of models utilized in this study may be insufficient to capture all of the differences and similarities. The research on CMMM is minimal, and it can be an opportunity for future research, to expand the scope of the CMMM by expanding the sample of Compliance management maturity models in order to provide a more thorough examination of the aspect that is appropriate for both a generic and specific organization.

REFERENCES

Society of Corporate Compliance and Ethics. (2018). *The Complete Compliance and Ethics Manual.* Minneapolis: Society of Corporate Compliance and Ethics.

Anna Pohle, K. B. (2018). The Impact of International Management Standards on Academic Research. *MDPI Sustainability Journal*.

Alijoyo, F. A., Hendra, R., & Sirait, K. (n.d.). The State-of-The-Art of Enterprise Risk Management Maturity Models: A Review.

International Organization for Standardization. (2021). ISO 37301:2021 Compliance Management System - Requirements with guidance for use.

Kusserow, R. P. (2020). Compliance Program Maturity Models. *Journal of Health Care Compliance*, 23-24, 61-62.

Jackman, D. (2015). *The Compliance Revolution.* Singapore: John Wiley & Sons.

Otte, K. K., Karen, H. A., Mudler, L. M., & Potter, J. H. (2018). Compliance Program Maturity and Effectiveness: Developing a Common Measure. *Journal of Health Care Compliance*, 5-16, 61.

RSA Security LLC. (2020). RSA Archer Regulatory & Corporate Compliance Management. Bedford, Massachusetts, Middlesex.

OCEG. (2016). *A Maturity Model for Integrated GRC.* Phoenix: Open Compliance and Ethics Group (OCEG).