INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 10, Issue 1 - V10I1-1217)

Available online at: https://www.ijariit.com

Enhancing organizational Governance: A proposal for COBIT 2019 Maturity Assessment

Taha Qureshi
qureshitaha44@gmail.com
Nangia and Co LLP, Mumbai

ABSTRACT

Background: This paper introduces a structured methodology for assigning maturity levels in accordance with The Control Objectives for Information and Related Technologies (COBIT) 2019 framework. The conventional method of evaluating an organization's COBIT Performance Management (CPM) often concentrates solely on capability levels, given the absence of a well-defined approach for assigning maturity levels in the framework.

The proposed methodology introduces an approach aligned with the principles of performance management designed to quantify the maturity of the governance and management objectives from the framework and collectively represent their impact on the overall organization.

Discussion: Maturity levels provide management with a comprehensive understanding of the current state of governance and management practices in the organization. Maturity assessment offers a holistic perspective, furnishing management with a thorough overview of the organizational landscape.

COBIT 5 released in the year 2012, followed the Process Assessment Model (PAM) model for assigning capability and maturity values. Since there is no defined PAM for COBIT 2019, The Capability Maturity Model Integration (CMMI) levels defined by the CMMI Institute can be used to represent process improvement efforts, in other words, it can measure capability levels along with other factors to give value to the organizations process for measuring maturity. Up to this point, there exists no formalized methodology for assigning or deriving maturity levels for an organization using the COBIT framework. The impetus for this paper stemmed from Luis Gorgona's, encouragement in ISACA blog for readers to explore the COBIT 2019 framework as a valuable resource for developing an approach to model, assessing maturity scores, and identifying essential factors for measuring their organization's performance.

Research Objectives: This paper aims to achieve the following objectives:

1. The Necessity and Challenges in the Assigning of Maturity Levels.
2. Proposing a Methodology for Assigning Maturity Levels for the COBIT 2019 Framework.

Conclusion: In conclusion, this paper encourages readers, auditors, and professionals to go beyond a basic evaluation of capability levels. By which organization leaders can attain an accurate comprehension of their existing Information and Technology(I&T) practices through the adoption of this systematic approach. Consequently, leading to well-informed decision-making, enhancing overall coverage of COBIT 2019 objectives.

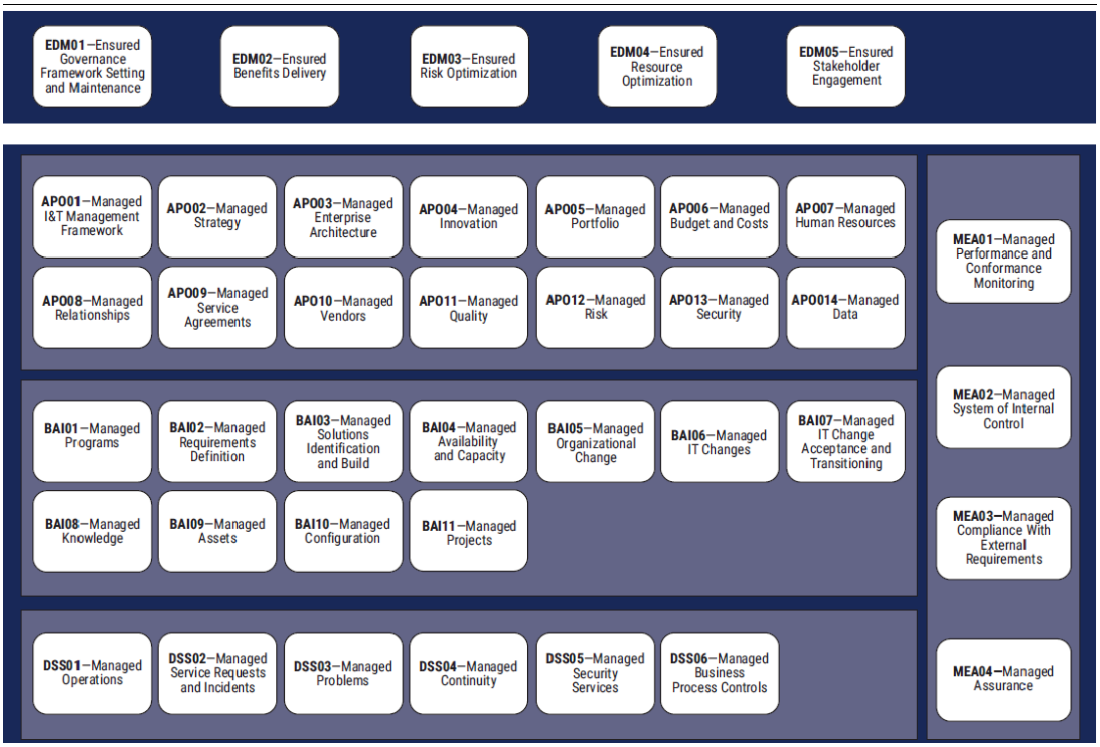
Keywords: The Control Objectives for Information and Related Technologies (COBIT), COBIT Performance Management (CPM), Capability Maturity Model Integration (CMMI), Process Assessment Model (PAM).

I. INTRODUCTION

The COBIT Framework is developed by ISACA, stands as a comprehensive and detailed model used to provides a set of guidelines and best practices that organizations can use to align their business objectives with IT goals, ensure effective risk management, and establish a framework for the implementation and monitoring of Information Technology (IT) processes. The COBIT framework is designed to help organizations address challenges related to IT governance and management by providing a systematic and holistic approach. COBIT 2019 is the latest version of the framework and builds upon its predecessor, COBIT5. COBIT serves as a comprehensive framework designed to govern and manage enterprise information and technology, catering to the entirety of the organization.

Structure: The latest iteration, COBIT 2019 released in the year 2018, is structured around five pillars known as the *COBIT Core Model* - 1. Evaluate, Direct, and Monitor (EDM), 2. Align, Plan, and Organize (APO), 3. Build, Acquire, and Implement (BAI), 4. Deliver, Service, and Support (DSS), and 5. Monitor, Evaluate, and Assess (MEA). The Governance Objective – Evaluate, Direct, and Monitor (EDM) focuses on the board level, ensuring the establishment of direction through prioritization and decision-making. They also oversee the monitoring of performance and compliance against objectives. On the other hand, Management Objectives Align, Plan, and Organize (APO), Build, Acquire, and Implement (BAI), Deliver, Service, and Support (DSS), and Monitor, Evaluate, and Assess (MEA) operate at the execution level, handling the planning, building, running, and monitoring of activities. This is done in alignment with the direction set by the governance body to achieve the enterprise objectives.

The COBIT Core (EDM, APO, BAI, DSS and MEA) pillars collectively encompass forty objectives (e.g., APO 001, APO 002, APO 003….so forth, BAI 001, BAI 002, BAI 003…. and so forth), addressing both governance and management considerations. Further these 40 Objectives contain 1202 activities, helping the organization to follow good practices in the IT domain and integrate it with the business requirements. The below figure represents the Objectives of the COBIT 2019 framework.



Reference: ISACA, COBIT® 2019 Framework: Introduction and Methodology, Chapter 4 Basic Concepts

COBIT 2019 is widely used by organizations globally to improve their IT governance and management practices. It provides a flexible framework that can be tailored to the specific needs and context of different organizations, making it a valuable tool for achieving and sustaining effective IT governance.

The COBIT 2019 framework encompasses various elements and exhibits intersections with other prominent frameworks/guidelines and standards, such as NIST, TOGAF and various ISO Standards. The COBIT 2019 framework incorporates sections that emphasize IT Processes and Resources along with their Business Requirements and focuses on areas such as Risk Management, Project Management, and Quality Management—aligning closely with ISO 9001. Additionally, it addresses IT Service Management in line with ISO 20000, Information Security Management following ISO 27001 standard, and Business Continuity in alignment with ISO 22301.These specialized sections further contribute to the framework's versatility and applicability across diverse aspects of IT governance and management.

There are many shared aspects and complementary features between COBIT 2019 and these established frameworks. Organizations have the flexibility to choose their approach towards the COBIT framework. One may opt to comply with specific sections of COBIT, i.e. Compliance with Incident and Problem Management from the framework or Implementing COBIT 2019 in its entirety as a best practice across the organization. This paper is centered on assigning Maturity Values under the assumption that the organization has fully adopted the COBIT 2019 framework.

II. THE COBIT PERFORMANCE MANAGEMENT (CPM) - CAPABILITY AND MATURITY

The *COBIT Performance Management (CPM)* pertains to the effectiveness of an enterprise's governance and management system and its components, with a focus on continuous improvement up to the desired level. CPM incorporates key concepts and methodologies, including capability levels and maturity levels.

As per *COBIT 2019: Framework and Methodology*, CPM has the following principles:
1. Simplicity in understanding and use.
2. Alignment with and support for the COBIT conceptual model.
3. Provision of dependable, repeatable, and pertinent results.
4. Flexibility to accommodate varying needs.
5. Support for diverse types of assessments.

The CPM model closely aligns with the concepts from CMMI® Development V2.0201 from CMMI Institute. This alignment is integrated into the *COBIT 2019 Framework: Governance and Management Objectives Guide*, where process activities are linked to capability levels. There are two metrics which are used to represent compliance-state for COBIT framework: Capability levels and Maturity levels.

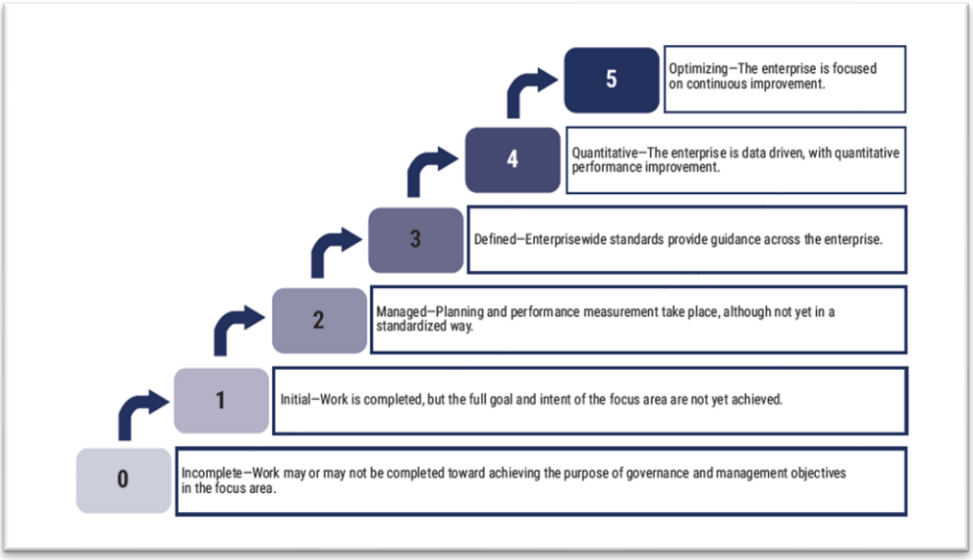
Capability Assessment

The capability level is a measure for how well a process is implemented within the organization. Each process activity is associated with a capability level. COBIT 2019 supports a CMMI-based process capability scheme. The process within each governance and management objective can operate at capability levels, between 0 to 5.

In order to assign capability levels, the *COBIT 2019 Framework: Governance & Management Objectives* can be leveraged for assigning capability values. However, it is crucial to understand how the organization and auditors intend to obtain these values and how they plan to address any gaps identified in the assessment. There also exists another proposed way to assign capability levels from ISACA in the year 2019 mentioned in ISACA Blog *"Defining Target Capability Levels in COBIT 2019: A Proposal for Refinement."*

Maturity Assessment

Maturity Level refers to the overall capability of an organization to manage and govern its IT processes effectively. This paper centers its attention on a vital aspect—the assignment of Maturity values. The decision to spotlight this particular area stems from the noticeable scarcity of methodologies when it comes to the comprehensive evaluation and assignment of Maturity Levels within organizations. It is important to note that in an assessment, maturity levels may serve as a secondary component/rating, offering a broader overview of organizational practices. A higher level is needed to convey performance without the *granularity* associated with individual process capability ratings, making maturity levels suitable for this purpose. In essence, maturity levels can be derived from the assigned capability levels and are interrelated. COBIT 2019 defines maturity levels as a performance measure at the focus area level, as shown in figure below-



Reference: COBIT 2019 Framework: Introduction and Methodology, Chapter 6 Performance Management in COBIT, Maturity Levels for Focus Areas

Our further discussion is grounded in the facts and insights highlighted in the COBIT framework, their supporting guides, the COBIT 2019 pillars, and the ISACA blogs for proposing a methodology towards maturity levels. These sources provide valuable expressions and perspectives from ISACA members regarding COBIT 2019.

Maturity models are now a universal language that brings together business and IT functions, making collaboration and improvement more seamless. These maturity levels act as straightforward benchmarks, especially for board directors, where level 0 signals lack of approach towards the objective and level 5 represents a fully implemented and followed status, making it easy to communicate about the organization's maturity. In Volume 6 of the ISACA Journal, Luis Gorgona's blog encourages creative exploration, emphasizing that every vertical can establish its own set of expected levels based on distinct IT department processes and value creation methods. Unlike Capability levels there is no established method/guidance for assigning Maturity Levels to an organization's IT Governance and Management objectives. Additionally, there is a lack of clarity regarding the appropriate level at which maturity levels should be assigned—whether it should be at the activity level, objective levels, or within the COBIT Core model, which comprises the five pillars: APO, EDM, BAI, DSS, and MEA.

III. THE CHALLENGES OF ASSIGNING MATURITY LEVELS:

I. Assessing Maturity for Activities: COBIT 2019 encompasses a total of 1202 activities, making the task of assigning Maturity levels to each control a considerable challenge. This becomes especially intricate when IT teams and executive management seek capability values as their primary focus for improvement. Furthermore, the primary objective of presenting Maturity Levels to the Board of Directors could prove time-consuming for the board, focusing extensively on granularity. Hence, assigning Maturity levels onto activities of the framework cannot be considered a viable task for the Board of any organization to investigate and understand the gaps in COBIT 2019 Implementation.

II. Assessing Maturity for COBIT Core Model: The COBIT 2019 framework consists of five pillars - 1. Evaluate, Direct, and Monitor (EDM), 2. Align, Plan, and Organize (APO), 3. Build, Acquire, and Implement (BAI), 4. Deliver, Service, and Support (DSS), and 5. Monitor, Evaluate, and Assess (MEA). While this approach identifies areas of gaps, assigning Maturity Levels to the pillars does not provide clear direction for the governance function to address gaps or non-compliance. Moreover, this would not provide an effective approach to address I&T practices within the organization. However, this method can effectively demonstrate year-over-year growth within the organization when presenting it to the board discussed in the below in this paper.

IV. PROPOSED APPROACH AND METHODOLOGY

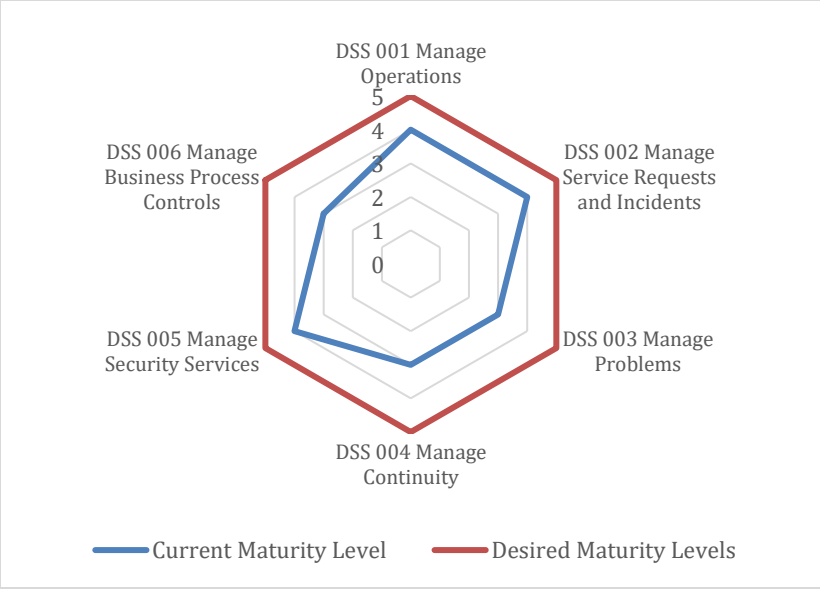
Maturity levels are aimed at helping the Management (Board of Directors, Senior Managers) to understand the organization at a higher level. This implies that when assessing maturity levels, we should not focus solely on specific details but rather consider achieving the overall objectives of COBIT 2019. According to the *COBIT 2019 Framework: Introduction and Methodology*, "Maturity levels are associated with focus areas (i.e., a collection of governance and management objectives and underlying components) and a certain

maturity level is achieved if all the processes contained in the focus area achieve that particular capability level." The above statement implies that capability and maturity levels are interrelated, with capability levels (primary rating) serving as a basis for deriving maturity levels. While COBIT 2019 emphasizes assigning maturity levels between 0 to 5, it falls short in providing clear guidance on the decision-making process for these levels and the specific criteria for assigning these values. Below are the considerations we have taken into consideration for assigning Maturity levels:

- Compliance Percentage: Utilizing a familiar maturity levels scale of 0 to 5, where 5 represents the desired state, and 0 indicates non-compliance or insufficient coverage for the objective. These Maturity levels are defined by the CMMI Institute for effective Capability Maturity Model Integration (CMMI). Each Governance or Management Objective is assigned a *compliance percentage*, illustrating the collective impact of grouped activities to the COBIT objective. See calculation method for deriving compliance percentage below in this paper. Higher compliance percentage correlates with higher capability values for activities associated with each COBIT Objective. This relationship implies that maturity levels are influenced by capability levels. Furthermore, for ensuring consistent outcomes and upholding uniformity in our rating methodologies, a standard similar to CMMI, such as ISO/IEC 55041 (Information technology — Process assessment) can be used for representing *compliance percentage* and thereby assigning Maturity values.

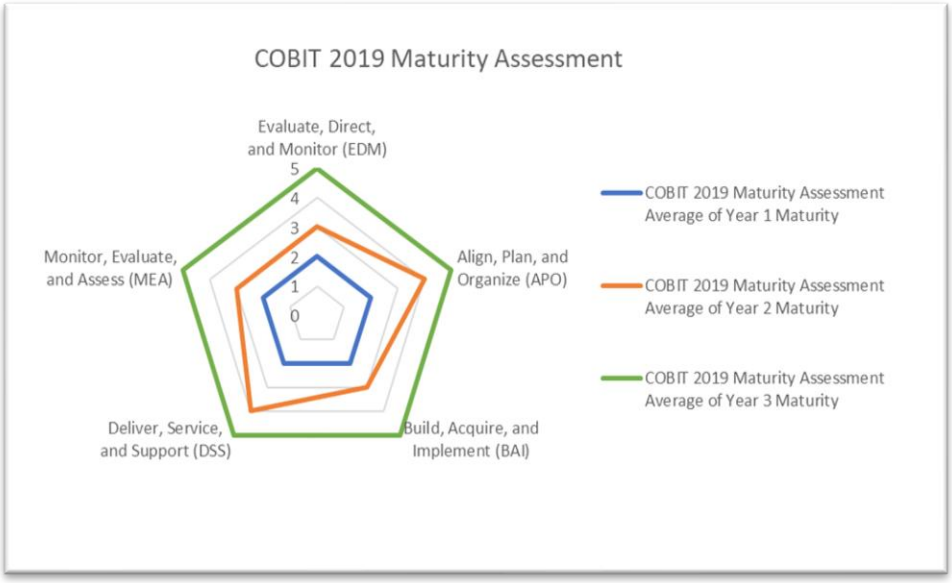
- Flexibility: The COBIT framework offers flexibility accommodating organizations with diverse needs and priorities. For organizations seeking alignment with specific processes within the framework, e.g. IT Service Management (ITSM) under DSS (Delivery, Service, and Support), or certain sections of the COBIT framework a tailored approach to assigning Maturity values can be used. For instance, when assessing maturity levels for ITSM, organizations can use a methodology that calculates *compliance percentages* based on the total number of controls relevant to IT-Service. By focusing solely on the maturity assessment of IT- Service, organizations can streamline their efforts and resources while still benefiting from COBIT governance framework. This approach allows organizations to gauge their compliance with COBIT standards specifically related to IT-Service practices. Moreover, organizations have the flexibility to remove certain controls or activities from the assessment if they are excluded upon management's decision or not applicable to their ITSM processes. The diagram below illustrates an example of an organization that has implemented ITSM practices from the COBIT framework, showcasing how flexibility in approach allows organizations to tailor their maturity assessments to specific areas of focus.

Domain	Activities
DSS 001	Manage Operations
DSS 002	Manage Service Requests and Incidents
DSS 003	Manage Problems
DSS 004	Manage Continuity
DSS 005	Manage Security Services
DSS 006	Manage Business Process Controls



Graph of a DSS (Delivery, Service, and Support) process Maturity level – IT Service

- Dependable, repeatable, and pertinent results: Organizations should regularly conduct audits and assessments to uphold their commitment to attaining the desired maturity level. It is crucial to recognize that organizations do not typically achieve all Maturity levels as 5 (Desired Level) at the outset of implementing the framework, as COBIT is structured for continual improvement. Adopting a mindset that embraces the current state of assessment and actively working towards the desired level of maturity, particularly level 5, aligns with COBIT's ethos.



Representation of Year-on-Year Progress in Maturity Assessment of COBIT Core

As ISACA aptly states, "Efficiency, effectiveness, and continuous improvement drive success." The journey towards maturity is represented in the above figure, illustrating year-on-year progress. By consistently conducting maturity assessments and striving for the desired results, organizations can effectively communicate their progress and status to management and the board. This representation serves as a valuable tool for transparency and informed decision-making.

Understanding Compliance Percentage in Relation to ISO/IEC 55041 Standard

The maturity levels outlined in the ISO/IEC 55041 Standard, range from 0 to 5, which closely resemble those defined by the CMMI Institute, each indicating a distinct level of process maturity:

- Level 0 - Incomplete Process (Not Performed): At this stage, the process lacks systematic execution, and basic practices may be overlooked.
- Level 1 - Performed Process (Initial): Processes are executed somewhat systematically but may lack consistency and full integration.
- Level 2 - Managed Process: Processes are defined, documented, and integrated into standard organizational practices, with management and control measures in place.
- Level 3 - Established Process (Defined): Processes are standardized across the organization, leading to predictable outcomes.
- Level 4 - Predictable Process (Quantitatively Managed): Processes are quantitatively managed and measured, offering a higher level of control and performance understanding.
- Level 5 - Optimizing Process: Organizations continuously refine processes based on quantitative feedback and innovative ideas, aiming for optimal results.

A higher *compliance percentage* indicates greater capability levels within the COBIT objective. The ISO/IEC 15504-7 rules can be applied to get an estimation on the maturity levels based on capability values. The maturity level is determined by the compliance percentage and process capability level ratings, following these rules:

1) To reach maturity level 1, all processes assigned to level 1 must achieve a capability level of 1 or higher.
2) For maturity level 2, all processes assigned to levels 1 and 2 must achieve a capability level of 2 or higher.
3) Attaining maturity level 3 requires all processes assigned to levels 1, 2, and 3 to achieve a capability level of 3 or higher.
4) To achieve maturity level 4, all processes assigned to levels 1, 2, 3, and 4 must achieve a capability level of 3 or higher. Additionally, one or more processes in the basic set must achieve a capability level of 4 or higher.

5) For maturity level 5, all processes must achieve a capability level of 3 or higher, with at least one process in the basic set reaching a capability level of 5.

The above rules can be used to get an idea of whether the Maturity levels being assigned are correct and are correlated with the assigned capability values. Regular assessments and enhancements play a vital role in enhancing the organization's maturity and effectiveness. When assigning maturity levels, it's essential to focus on the coverage of COBIT objectives. In the 2022 ISACA Blog titled "Exploring Innovative Approaches with Maturity Models and COBIT 2019," Luis Gorgona underscores the importance of several factors when assigning maturity levels, including coverage of control objectives, automation, and associated metrics. The approach we propose guarantees thorough coverage of objectives through the utilization of *compliance percentages*, which are directly correlated with capability values (primary rating). It's noteworthy that higher capability values invariably result in elevated maturity levels.

Assigning Maturity Levels Based on Compliance Percentage

Considering the limitations addressed in this paper above, it is crucial to take a holistic approach. Therefore, our proposed methodology involves assigning Maturity Levels at the objective level of the COBIT 2019 Framework. Below, an example is provided to illustrate how compliance percentage can be derived, leading to the determination of Maturity values.

$$\text{Compliance Percentage (\%)} = \frac{\text{Complaint Controls}}{\text{Total controls in the Governance/Management Objective}} \times 100$$

The Domain ALIGN, PLAN, AND ORGANIZE (APO) comprises of 14 Objectives (APO 001, APO 002, APO 003….) and so on, out of which APO 001 Objective has 46 Activities in total.

Total Controls (Activities) in APO 001 = 46.

Out of 46 Total Controls, Compliant Controls are 45.

Hence, *Compliance Percentage* (%) for the Objective APO 001 = (45 /46) * 100 = 97.8 %

Compliance % (> 95) = Level 5 Maturity Level

Hence, APO 001 = Level 5

The following table illustrates the assignment of maturity levels based on compliance percentage:

Level 0	Incomplete	Not Performed (0%)
Level 1	Initial	< 20%
Level 2	Managed	20 % to <= 50%
Level 3	Defined	50 % to <= 80%
Level 4	Quantitative (Measurable)	80 % to <= 95%
Level 5	Optimizing	> 95%

Objectives	Domain	Total Controls	Compliant	Complaince %	Desired Maturity Level	Current Maturity Level	
APO01	APO - Align Plan Organise	46	45	97.8	Level 5	Level 5	5
APO02		28	20	71.4	Level 5	Level 3	3
APO03		40	20	50.0	Level 5	Level 2	2
APO04		24	18	75.0	Level 5	Level 3	3
APO05		23	21	91.3	Level 5	Level 4	4
APO06		32	15	46.9	Level 5	Level 2	2
APO07		34	19	55.9	Level 5	Level 3	3
APO08		21	16	76.2	Level 5	Level 3	3
APO09		21	17	81.0	Level 5	Level 4	4
APO10		29	20	69.0	Level 5	Level 3	3
APO11		26	20	76.9	Level 5	Level 3	3
APO12		36	15	41.7	Level 5	Level 2	2
APO13		19	18	94.7	Level 5	Level 4	4
APO14		59	57	96.6	Level 5	Level 5	5
EDM01	EDM - Evaluate, Direct and Monitor	21	20	95.2	Level 5	Level 5	5
EDM02		25	25	100.0	Level 5	Level 5	5
EDM03		16	15	93.8	Level 5	Level 4	4
EDM04		13	13	100.0	Level 5	Level 5	5
EDM05		11	11	100.0	Level 5	Level 5	5
DSS01	DSS - Deliver, Service and Support	33	33	100.0	Level 5	Level 5	5
DSS02		25	22	88.0	Level 5	Level 4	4
DSS03		23	20	87.0	Level 5	Level 4	4
DSS04		41	20	48.8	Level 5	Level 2	2
DSS05		50	27	54.0	Level 5	Level 3	3
DSS06		34	30	88.2	Level 5	Level 4	4

Representation of Maturity Assessment

Determining if an objective like APO 001, APO 002, APO 003, and so on, has reached Maturity Level 5 involves considering various factors. Factors including the organization's size, management processes, scope of site coverage, business risks, compliance with other frameworks, and year-on-year maturity progress. Also, the sample size, type and amount of objective evidence should be sufficient to match the scope of the assessment on which the capability levels are assigned. It is important to note that there might be gaps at the activity/control levels. If the activities/controls within the objectives don't comply or fail to meet the criteria, reaching the desired Capability levels and Maturity Level becomes difficult.

V. CONCLUSION

In conclusion, the significance of maturity levels lies in their ability to provide a comprehensive overview of an organization's governance and management practices. The exploration of maturity levels within the context of the research paper has shed light on the intricate dynamics of assessing and assigning these levels, particularly within the framework of COBIT 2019. The significance of maturity models as a common language bridging the gap between business and IT functions has been emphasized. The evolution from COBIT 5 to COBIT 2019 has brought about a paradigm shift, necessitating the development of customized maturity models to align with the updated framework.

This paper has aimed to emphasize the significance of taking into account different factors, including coverage of control objectives and relevant metrics, when creating a customized maturity model. It has underscored the flexibility inherent in developing unique approaches based on organizational differences. In essence, this paper advocates for a thoughtful and adaptable approach to maturity levels, urging organizations to move beyond simplistic evaluations and embrace a continuous improvement mindset. The idea to explore, be creative, and adjust maturity models to fit each organization's unique needs stands out as an important point, highlighting how IT governance and management are always evolving.

VI. REFERENCES

[1] COBIT® 2019 Framework: Governance and Management Objectives, ISACA 2018
[2] COBIT® 2019 Framework: Introduction & Methodology, ISACA 2018
[3] The ISO/IEC 55041 Standard (Information technology — Process assessment)

[4] Defining Target Capability Levels in COBIT 2019: A Proposal for Refinement, ISACA, Joao Souza Neto, 2019.
[5] Getting Creative with Maturity Models, ISACA, Luis Gorgona,2022
[6] Building a Maturity Model for COBIT 2019 Based on CMMI, ISACA, Luis Gorgona, 2021
[7] Effective Capability and Maturity Assessment Using COBIT 2019, ISACA, Emeka Elue, 2020
[8] ISO/IEC Information technology — Process assessment —Part 7: Assessment of organizational maturity, International Organization for Standardization and International Electrotechnical Commission Std. 2008.

