TÉCNICO LISBOA

Objectifying COBIT5 Outputs

David André Caldas Antunes

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisor: Prof. Carlos Manuel Martins Mendes

Examination Committee

Chairperson: Prof. Rui Filipe Fernandes Prada

Supervisor: Prof. Carlos Manuel Martins Mendes

Member of the Committee: Prof. Miguel Leitão Bignolas Mira da Silva

October 2018

Acknowledgments

First, I would like to thank Professor Carlos Mendes for accepting my request for being my supervisor. His availability and readiness to provide feedback, suggestions and relevant documents were critical in the realization of this thesis. I would also like to thank him for the support he provided by suggesting several contacts to me as potential experts for evaluating my research.

I would also like to thank Rafael Almeida, Bruno Soares and Professor Paulo Faroleiro for their availability and for the help they provided in evaluating my research a giving me feedback to improve my research and correct my mistakes.

Last but not least, I would like to thank my friends and family for their support and for their advice.

Resumo

Palavras-Chave: COBIT5, Outputs, PAM, Work Products, ITIL.

Esta tese tem como âmbito identificar e descrever os outputs produzidos pelos processos do COBIT5. Usando Design Science and Research Methodology como metodologia de investigação, foi identificado um problema relacionado com a forma como o COBIT5 define e descreve os outputs gerados pelos processos. A abordagem do COBIT5 como guia de boas práticas assume que os praticantes de COBIT5 tenham conhecimentos sobre o standard e sobre termos técnicos e estruturas organizacionais de diversas áreas de negócio e sejam capazes de identificar em concreto os outputs produzidos pelos processos do COBIT5 usando informação relativa à organização que é alvo da avaliação de capacidades. A forma como os outputs do COBIT5 são descritos faz com que diferentes praticantes com diferentes níveis de experiência possam ter diversas interpretações e causar impacto no resultado de uma avaliação de capacidades referentes ao COBIT5. De forma a melhorar as descrições dos outputs do COBIT5, foi feito um mapeamento dos outputs com descrições provenientes de outros standards de governança e gestão, bem como definições concretas quando estas não se encontram em standards estabelecidos.

A avaliação dos objetos produzidos nesta investigação foi realizada recorrendo a profissionais experientes em COBIT5 e process assessment e as suas opiniões e comentários foram registados de forma a obter o máximo de informação sobre a viabilidade da solução e conhecimento gerado.

Por fim foram retiradas conclusões sobre a solução proposta e o seu potencial impacto no processo de avaliação de capacidades de COBIT5 e da forma como o conhecimento gerado pode ser expandido para os restantes processos do COBIT5.

Abstract

COBIT5 is a business framework that focuses on Enterprise Governance and Management of IT, providing a list of best practices that separates governance from management, allowing an efficient management of critical business processes while also focusing on meeting the business stakeholder's needs. Due to the nature of COBIT5, the guidelines for implementing the required Enabling Processes are generic and designed to suit most organizations while not providing detailed information on how to produce their respective outputs. The outputs' description is often generic and requires the COBIT5 practitioners to be familiar with terms and definitions that often are outside the scope of IT in order to fully understand what the COBIT5's authors meant when the documentation was written. Using COBIT5 and other established standards like ITIL as a foundation, we proposed a solution that objectifies and describes the outputs produced by the COBIT5 enabling processes by providing detailed definitions of what the output is and where is should be found within the enterprise, improving the available knowledge for COBIT5 process assessment. The gathered results were evaluated using the Pries-Heje et al. framework for DSRM and expert reviews. After the evaluation we concluded that is possible to extend the descriptions of the outputs in a more objective form and how they relate to other definitions from other established standards.

Keywords: Enterprise Governance of IT, COBIT5, ITIL, Governance, Process Outputs, Work Products, Process Assessment, PAM, Self-Assessment, TOGAF, ISO.

Table of Contents

List of Figures

List of Tables

List of Acronyms

IT	Information Technology
COBIT	Control Objectives for Information and Related Technologies
TOGAF	The Open Group Architecture Framework
ISO	International Standardization for Organization
ITIL	Information Technology Infrastructure Library
SFIA	Skills Framework for the Information Age
DSRM	Design Science and Research Methodology
APO	Align, Plan and Organize
DSS	Deliver, Service and Support
PAM	Process Assessment Model
WP	Work Product
SLA	Service Level Agreement
OLA	Operational Level Agreement
RFI	Request for Information
CSI	Continual Service Improvement
EA	Enterprise Architecture

1. Introduction

In this section we will introduce the structure of the document and provide a brief overview of the several chapters and the work that was done.

1.1. Context

COBIT5 is an enterprise governance and management framework developed by ISACA (Information Systems Audit and Control Association[1] that focuses on the alignment of IT strategy with the business, meeting business stakeholder needs and separating enterprise governance from management.

Over the years, Information Technology (IT) has evolved from a small supporting department within an enterprise to become a foundation for modern enterprises.

This change and the surge in demand for more advanced IT systems led to the creation of ISACA, an international professional membership association for IT professionals and IT auditors[1], and subsequently the creation of COBIT, a standard made for IT audit.

With the everchanging world of IT and the increase in adoption of COBIT by enterprises, the standard as evolved and in its latest release IT is defined as an integral part of the business.

1.2. Problem

COBIT5 provides a set of 37 processes that act as enablers for the IT and the business. For every enabler, COBIT includes a detailed description of the process, its activities, inputs, outputs and respective RACI chart. COBIT5 was designed to suit any organization, therefore the provided guidelines are generic, leaving the implementation of the processes and its respective outputs to the enterprise. This generic approach causes the outputs produced by the enablers to be vaguely described in the internal control documents for internal and external capabilities assessment. Since the enterprise is responsible for the implementation, documentation and monitoring of the processes, the lack of detail on the internal control can have a profound impact on the performance evaluation of the enablers when performing a process maturity assessment[2]. By leaving the descriptions of the outputs generic and vague, the COBIT5 practitioner is responsible to know what the outputs are, how they should be structured and where they are expected to be found within the enterprise's information items. This leads to a scenario where the practitioner must know what to ask when evaluating the process capability level of the enterprise and likewise, the enterprise must also know what they are being asked in order to provide the correct information to the practitioner. An incorrect capability assessment can lead to recommendations that are not suited to the current capabilities of the enterprise and the duplication of processes and resources.

1.3. Proposal

In this section we propose an extended description for the level 1 work products produced by the COBIT5 enabling processes. The proposed Work Product description uses established standards to provide a better description for specific outputs and their structure. The work product mapping has the objective of providing additional knowledge regarding the work products to facilitate the information gathering required for a process capability assessment. We will compare the COBIT5's descriptions for Level 1 Work products with descriptions from other sources and propose a definition for the work products that aims to define what the work product is, how it is usually structured and where it is expected to be found on the information items. Whenever possible, the description will be referencing an established standard in the likes of ITIL, TOGAF and ISO standards to guarantee a more accurate and correct definition of the work product.

1.4. Evaluation

Given the nature of the problem and the scope of the thesis, a real-world implementation of the solution is not feasible. Therefore, the evaluation of the proposed solution consists on evaluating the feasibility of the proposed implementation and its impact on process assessment with the help of an experienced auditor that is familiar with process assessment model, governance practices and most important, the COBIT5 framework. The evaluation will consist in presenting the proposal to the expert and asking is they agree with the proposal, where they do not agree and additional feedback on where to improve and other suggestions to increase the value and credibility of the proposal.

2. Research Methodology

The research method selected for investigation and results gathering is Design Science and Research Methodology. Design Science Research Methodology is a research and investigation methodology that adopts the principles of defining a problem and solution research from tradition Design Science while applying research methodologies used by the scientific community. DSRM is an iterative process that is comprised of a series of steps used to “create and evaluate IT artefacts intended to solve identified organizational problems” [3].

2.1. Process Model

DSRM aims to provide a standardized process model for DS research, tailored for problem identification and solution, completed by prior research on the selected research scope.

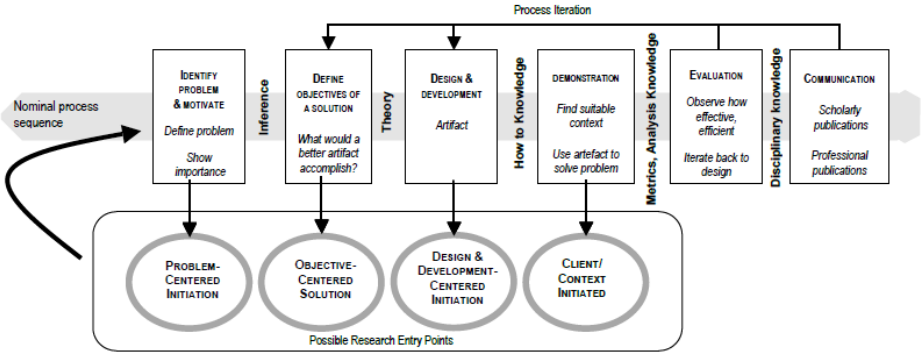

Figure 1: DSRM Process Model [4]

The process model is comprised of six steps that are used to achieve the final IS artefact that aims to solve the identified problem. The steps can be described as:

1. **Problem identification and motivation:** In this step the researcher must define the research problem. Justifying the problem is strongly encouraged as it motivates the researcher for completing the further steps and achieving the solution. This step corresponds to Section 3 of this document, where we analyze COBIT5 and the provided Process Assessment Model, identifying the problem surrounding the process outputs and level 1 work products and justifying the need for improving their descriptions in the scope of a process capability assessment.
2. **Define the objectives for a solution:** This step focuses on inferring the objectives from the problem analysis and specification as well as defining what is possible and feasible to implement. This step corresponds to Section 3 of this document, where after we define and describe the problem we define the objective that we want to achieve with the solution and the feasibility we can expect before we begin to design the solution.

3. **Design and development:** This activity focuses on researching and producing the artifact used for the solution. This step of the DSRM process corresponds to section 5 of this document. In this section we will present a proposal that solves the problem related to COBIT5's process outputs and we explain the several components that compose the solution. We will present a mapping of COBIT5's level 1 work products and the provided descriptions paired to more complete definitions from established standards and frameworks in the likes of ITIL and TOGAF. We will also provide examples of frameworks and tools can be used to create the information items that represent certain work products.
4. **Demonstration:** In this step, the researcher must test the produced artifact by demonstrating its application to one or more instances of the defined problem. The demonstration can be in the form of a simulation, case study, proof or any other type of activity that suits the problem. This step is present on section 5 of this thesis, where we provide a concrete example of a tool that can realize the work products according to the definition we provided when designing the mapping.
5. **Evaluation:** Evaluation of the gathered results from the demonstration activity. In this activity, the solution objectives must be compared with the application of the artifact in the demonstration. The means used by the researcher for evaluating the artifact should be defined according to the nature of the problem and can take the form of quantitative results, review by expert, among others. The success of this activity defines whether the artifact meets the solution objectives and the researcher proceeds to step 6 or must proceed to step 3 and revise the produced artifact. This step is present on section 6 of this document, where we consulted experts in COBIT5 and capability assessment and where we recorded their feedback on our proposed solution.
6. **Communication:** Communication of the problem and the artefact to the appropriate audience. In the case of an academic research, this step corresponds to the production of a paper. This final step of the DSRM process corresponds to the publishing of this thesis, where the problem and corresponding artifact are communicated.

3. Problem

In this section we will contextualize the problem and perform an analysis on the former. Finally, we will define its impact on enterprise governance.

This section corresponds to the Problem Identification and Motivation phase of DSRM. In this section we will define the problem and its context.

COBIT5 provides a generic description of the outputs (What) but does not provide a defined guideline of the structure or the location of the outputs (level 1 work products) on the information items.

3.1. Contextualizing the Problem

IT organizations are facing the transition from IT being a back office to being an integral part of the business. This transition led to the creation of several standards and best practices with the purpose of facilitating the enterprises to align their strategy to the business needs and maximizing their IT resources. Enterprises that wish to stay relevant must be able to adapt and shape their infrastructure around IT, recurring to one or more off-the-shelf solutions [1].

One of the most popular standards for IT Governance is COBIT5, a set of best practices for IT Governance and Management under a single integrated framework[5].

COBIT5 operates under 5 basic principles and a set of 37 processes, defined as COBIT Enablers in order to provide a set of best practices for corporate governance and management while ensuring benefits delivery through goal realization.

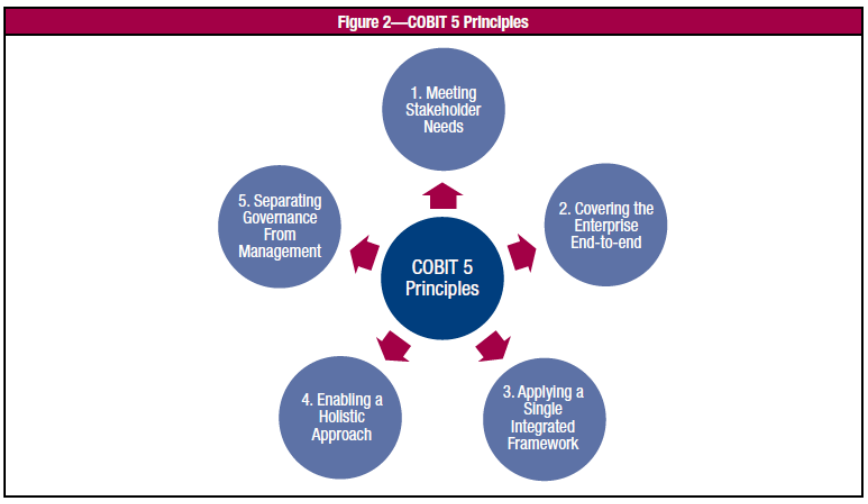

Figure 2: COBIT5's Core Principles [5]

COBIT5 defines the separation of IT Governance from IT Management with its enabling processes. The outputs of management focused enablers provide the information required by other enablers as an input for their respective implementation as well as providing the necessary feedback to the governance.

In order to provide a complete coverage of the IT, COBIT5 uses and references several domains outside IT that are critical for the design and operation of the business processes that support IT.

These domains are Finance, Accounting, Human Resources, among others, and its concepts and definitions are required to fully understand and assess the capabilities and maturity of the IT on the enterprises.

3.2. Problem Definition

Implementing and assessing COBIT5 in an organization is no easy task and requires mapping the 37 COBIT enablers using the enterprise's internal control documents. The enterprise is required to provide information regarding its processes in order to assess the state of COBIT5 implementation present in the enterprise and the capability level associated with each of the 37 COBIT5 enablers.

COBIT5 provides for each enabling process a set of associated activities that should be performed as well as a set of inputs and outputs for that specific process.

For a complete and accurate assessment of IT capabilities on an enterprise, the COBIT5 practitioner must understand what to look for and ask for and the enterprise must also know what is being asked in order to provide the required information to the practitioner.

In order for a process achieve level 2 or high capability, it should be implemented by the enterprise using its business processes and its outputs (level 1 work products) must be produced. This entails that the practitioner must know what a specific output is in order to look for its existence within the enterprise's processes.

Due to its nature as a best practices' framework and in order to fit any type of organization, the description of the outputs is generic, and its implementation is left to be decided by the organization.

The extended description that COBIT5 provides in PAM document for the process outputs (also known as level 1 work products) is inconsistent and heavily relies that the practitioner is familiar with several domains and concepts that used to describe the work products.

While some work products have a description that is easy to understand, others have a vague description or are referenced as part of a process or information item.

Figure 19 - Level 1 Output Work Products *(cont.)*		
WP ID	**WP**	**Description**
EDM04-WP7	Feedback on allocation and effectiveness of resources and capabilities	Information resulting from the monitoring and reporting process for ensuring resource optimisation
EDM04-WP8	Remedial actions to address resource management deviations	Part of the monitoring and reporting process for ensuring resource optimisation
EDM05-WP1	Evaluation of enterprise reporting requirements	An evaluation of both internal and external reporting requirements including legal and regulatory and will be part of the governance framework
EDM05-WP2	Reporting and communications principles	Principles will be part of the reporting in the governance framework.
EDM05-WP3	Rules for validating and approving mandatory reports	Rules will be part of the reporting in the governance framework and could be in the form of policies, operating practices, and standards and/or procedures.
EDM05-WP4	Escalation guidelines	A part of reporting in the governance framework and could be in the form of policies, operating practices and standards and/or procedures
EDM05-WP5	Assessment of reporting effectiveness	Usually found from an annual internal audit or assessment report on the effectiveness of governance
APO01-WP1	Definition of organisational structure and functions	Part of the IT management framework related to IT organisation
APO01-WP2	Enterprise operational guidelines	Part of the IT-related policies, procedures and practices for the IT management framework
APO01-WP3	Communication ground rules	Part of a monitoring and reporting process in the IT management framework
APO01-WP4	Definition of IT-related roles and responsibilities	A RACI chart will outline these roles and responsibilities.
APO01-WP5	Definition of supervisory practices	Part of the IT-related policies, procedures and practices for the IT management framework
APO01-WP6	IT-related policies	Policies and/or operating practices/standards that reflect IT operations and accountabilities
APO01-WP7	Communication on IT objectives	Part of a monitoring and reporting process for defining an IT framework
APO01-WP8	Evaluation of options for IT organisation	Part of the IT management framework related to IT organisation
APO01-WP9	Defined operational placement of IT function	Part of the IT management framework related to IT organisation
APO01-WP10	Data classification guidelines	Part of an enterprise architecture plus data retention and risk management policy
APO01-WP11	Data security and control guidelines	Part of the IT-related policies, procedures and guidelines, but specific to data security
APO01-WP12	Data integrity procedures	Part of the IT-related policies, procedures and guidelines, but specific to data security; these are the more detailed procedures.
APO01-WP13	Process capability assessments	Part of a monitoring and reporting process for defining an IT framework such as COBIT PAM
APO01-WP14	Process improvement opportunities	Opportunities to improve arising from the use of a monitoring and reporting process for defining an IT framework
APO01-WP15	Performance goals and metrics for process improvement tracking	Part of a monitoring and reporting process for defining an IT framework

Figure 3: Level 1 Work Products[6]

Looking at the table above we can observe the inconsistency of the work product descriptions. While work products such as EDM05-WP3 and APO01-WP4 have a description that is easy to understand, other work products as APO01-WP7 and APO01-08 are vague and can have several interpretations.

Different interpretations of ambiguous descriptions can lead to different information being provided, so an objective and easy to understand description in necessary to ensure that the correct information is used on the capability assessment[1].

4. Related Work

In this section, we will describe the tools used on our proposed solution and perform an analysis on solutions that tried to solve the problem defined in section 3.

4.1. The role of Enterprise Governance of IT

In today's age of information, Information Technology (IT) plays a vital role on the structure of enterprises. IT is no longer a small segment of an enterprises, often located in a back office. Instead IT is now one of the main sources of value generation for enterprises, and as such, it requires proper measures to ensure that enterprises manage to survive in today's market.

Steven de Haes defines Enterprise Governance of IT (EGIT) as "an integral part of corporate governance, exercised by the board [..] in support of business/IT alignment and the creation of business value from IT-enabled business investments" [1].

Therefore, EGIT should set the direction of future IT related investments taken by an enterprise required to generate value, meet the stakeholder's needs and aligning the IT strategy with the Business strategy.

In order to stay competitive in today's market, enterprises now seek international certifications for their IT such as ISO and structure their IT investments and processes using best-practice frameworks such as TOGAF and COBIT5.

4.2. COBIT 5

ISACA describes COBIT5 as "comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT"[5].

COBIT5 is a generic good-practices framework developed by ISACA that focuses on Enterprise Governance of IT (EGIT) that provides a set of guidelines for enterprises to better establish IT related objectives to better manage their resources a generate value. It operates on five core principles: Meeting Stakeholder Needs; Covering the enterprise end-to end; Applying a single, integrated framework; Enabling a holistic approach; Separating Governance from Management[5]. These five principles enable enterprises to manage their resources more effectively, align the enterprise's goals with the stakeholders' and provide a governance and management framework that optimizes IT investment and benefit realization [5].

4.2.1. COBIT 5 Enabling Processes

COBIT 5 includes a reference model that describes and defines in detail a set of governance and management processes related to IT that should be found in the majority of enterprises.[5]

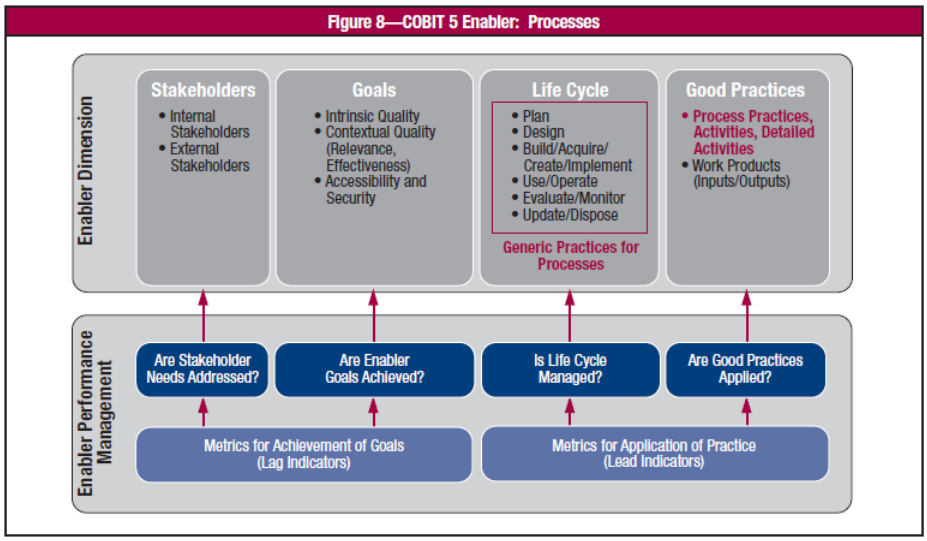

Figure 4: Anatomy of an enabling Process [5]

The set is composed by 37 core processes that enterprises need to implement and manage according to their needs in order to align their stakeholder's needs with the business' needs and provide an effective governance and management of their IT. According to the principle of separating Governance from Management, the 37 processes are separated into two categories, Governance Processes and Management Processes.

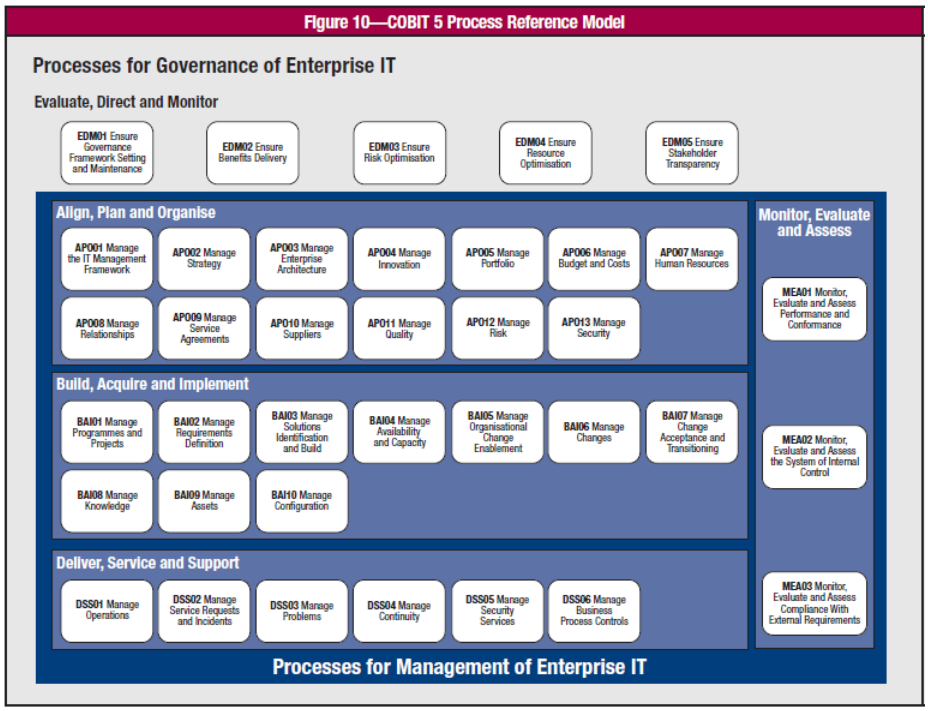

Figure 5: COBIT 5 process reference model [5]

The 37 processes are further divided into five sub-categories: Evaluate, Direct and Monitor; Align, Plan and Organize; Build, Acquire and Implement; Deliver, Service and Support; Monitor, Evaluate and Assess.

4.2.2. COBIT 5 Level 1 Work Products

The level 1 Work Products are nothing more than the work products produced by the 37 Enabling Processes as outputs. The COBIT 5 reference model for the processes states that every process should have one or more inputs required for its execution and must also generate work products as outputs. These outputs are crucial for the process maturity assessment as their creation and monitoring is a requirement for achieving maturity level 2 and higher levels. As stated in the problem section, COBIT 5 indicates what work products should be produced as process outputs but does not provide detailed guidelines for the former's format and representation, requiring additional knowledge for performing a complete assessment.

Figure 19 - Level 1 Output Work Products *(cont.)*		
WP ID	**WP**	**Description**
APO02-WP9	Value benefit statement for target environment	Part of the IT strategic plan and results from the benefits analysis process of the IT investment portfolio
APO02-WP10	Definition of strategic initiatives	Part of the strategic plan road map
APO02-WP11	Risk assessment initiatives	Part of the risk assessment process and will be included in the strategic plan road map
APO02-WP12	Strategic road map	A plan that outlines the key steps/phases in getting or achieving a strategic plan
APO02-WP13	Communication plan	Part of a reporting and monitoring process for strategic planning
APO02-WP14	Communication package	The process outline for all communication dealing with strategic planning, includes the plan, methods and delivery of communication and frequency
APO03-WP1	Defined scope of architecture	Part of the definition of a reference enterprise architecture model
APO03-WP2	Architecture principles	Part of the definition of a reference enterprise architecture model
APO03-WP3	Architecture concept business case and value proposition	Business case proposal for an architecture concept
APO03-WP4	Baseline domain descriptions and architecture definition	Part of an enterprise architecture model
APO03-WP5	Process architecture model	A typical process architecture model organises the logic for business process and IT infrastructure, which reflects the integration and standardisation requirements of the enterprise operating model.
APO03-WP6	Information architecture model	Part of an enterprise architecture model, but will specifically relate to how information is organised
APO03-WP7	High-level implementation and migration strategy	Implementation and migration strategy for architecture
APO03-WP8	Transition architectures	Part of the implementation and migration strategy for architecture
APO03-WP9	Resource requirements	Part of the implementation plan for enterprise architecture
APO03-WP10	Implementation phase descriptions	Part of the implementation plan for enterprise architecture
APO03-WP11	Architecture governance requirements	Part of the enterprise architecture model or framework governance requirements
APO03-WP12	Solution development guidance	Part of the implementation plan for enterprise architecture
APO04-WP1	Innovation plan	Innovation plan with the summary of approved and evaluated opportunities, business benefits and risk articulated
APO04-WP2	Recognition and reward programme	Part of the strategic IT plan
APO04-WP3	Innovation opportunities linked to business drivers	Part of an innovation plan for applications and IT infrastructure articulated in a strategic IT plan
APO04-WP4	Research analyses of innovation possibilities	Found in an innovation planning process and will form part of a strategic IT plan
APO04-WP5	Evaluations of innovation ideas	Found in an innovation planning process and will form part of a strategic IT plan
APO04-WP6	Proof-of-concept scope and outline business case	Validation of assumptions for a proof of concept and will be part of the business case
APO04-WP7	Test results from proof-of-concept initiatives	Part of a pilot or test found in an evaluation report

Figure 6: COBIT5 APO Level 1 Work Products [5]

4.2.3. COBIT5 Process Assessment Model

COBIT5 provides a process assessment model for its 37 enabling processes that is compliant with ISO/IEC 15504. This process model uses a measurement framework that assesses the maturity level of each one of the 37 enablers according to the state of implementation and work product generation.

The COBIT5 PAM (Process Assessment Model) is composed of two dimensions – The Process Reference Model that describes enterprise governance and management of IT and the Capability Dimension that provides a measure of a process's capability to meet an enterprise's current or project goals for the specific process [6].

4.3. ITIL

ITIL is a framework designed for IT service management and operation. It provides a set of best practices and guidelines for service design, service strategy, service operation and service transition. Due to its principles, ITIL provides detailed descriptions for service and IT related concepts[7]. ITIL has the same purpose of the COBIT5's DSS family of enablers, providing a set of operational level practices. ITIL is structured around an iterative cycle, ITIL Continual Service Improvement, that gathers information from the enterprise's stakeholders and operational indicators and provides a process to design and optimize its processes according to the enterprise's needs and its vision. The complete ITIL model is represented on the image below.

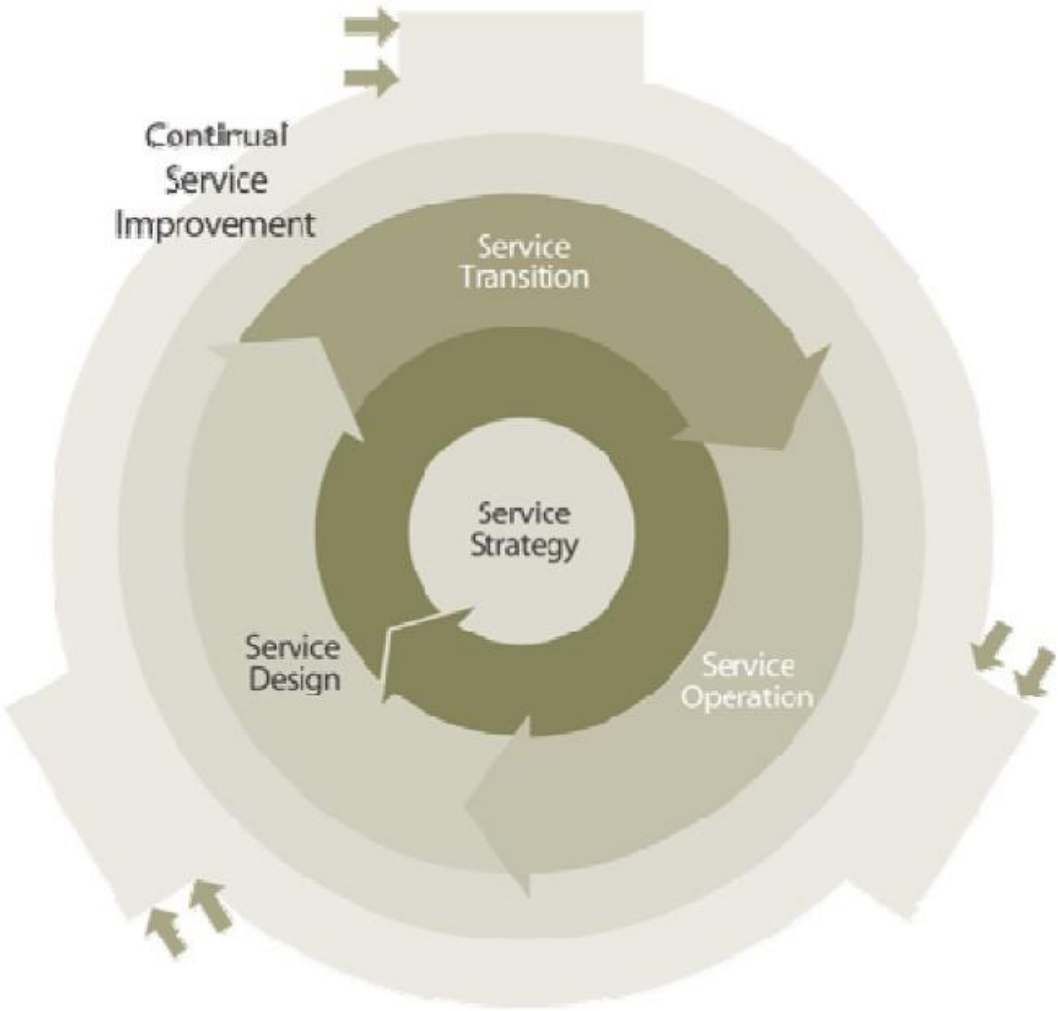

Figure 7: The ITIL Core[7]

To fully support the ITIL cycle, ITIL is divided into five main publications: Service Strategy, Service Design, Service Transition and Service Operation and Continual Service Improvement. Each one of the five fully details the processes and activities necessary for their realization.

4.3.1. ITIL Service Strategy

ITIL defines Service Strategy as a means to provide guidance to enterprises on how to design, develop and implement Service Management both as an organizational capability and as a strategy asset[7]. Service Strategy defines a set of principles and structures that allows the enterprises to structure their processes and services to better suit their needs. Being at the core of ITIL, Service Strategy as a publication covers the pillars of strategy and development such as value creation, market analysis and portfolio management. This publication contains most of the detailed concepts and definitions that are necessary for the proposal of this thesis.

4.3.2. ITIL Service Design

ITIL defines its Service Design publication as a guidance for the design and development of IT services and processes[8]. This publication covers Service Management as a practice and includes service design fundamentals and organizational considerations that help implement service design in the form of roles, activities, skills and responsibilities. This publication also includes on its appendix several templates that serve as a reference for information items useful for IT services. These templates and definitions can also serve as additional references for the proposal of this thesis.

4.3.3. ITIL Service Operation

ITIL defines Service Operation as a publication that contains practices for achieving effective and efficient delivery of it services [9]. This publication covers a variety of concepts related to service operation principles and service operation management, from functions and activities required for service operation to communication principles that ensure operational communication and reporting.

4.3.4. ITIL Continual Service Improvement

This ITIL publication focuses on practical guidance for applying a 7-step improvement process for IT services. The main purpose of CSI is to cover topics and concepts found on the other ITIL publications and applying the former in a practice that allows for a constant assessment of the services and service management processes[10].

4.4. TOGAF

TOGAF is an enterprise architecture framework. It provides the enterprises with a set of guidelines and a framework for designing and improving the IT architectures. TOGAF adopts a high-level approach to the design of enterprise architectures and it is flexible by design, allowing the enterprises to develop a broad range of architectures using the provided framework [18]. The framework is an iterative framework that is composed of 7 key phases that allows enterprises to define in a AS-IS state its current architectures and define a roadmap to achieve the desired TO-BE architecture. The TOGAF framework is represented on the figure below.

Figure 8: TOGAF ADM phases [18]

TOGAF also provides detailed descriptions for enterprise architecture concepts that are present on several COBIT5 enablers. These concepts can be found throughout the seven phases of TOGAF.

4.5. Mapping and Integration of Enterprise Governance of IT Practices.

Renato Jacob Lourinho [11] on his master thesis recognizes COBIT5 as a powerful IT framework for implementing governance of information technology. Lourinho recognizes that there is no single complete and off-the-shelf best practice framework, and therefore an enterprise must choose the adoption of the frameworks according to its needs. The variety of off-the-shelf solutions makes enterprises adopt one or more frameworks and standards in order to ensure alignment between service management and the organization's artifacts (Gama, Sousa, & Mira da Silva, 2012).

Lourinho proposes to model COBIT5 and ISO 27001 standard using the ArchiMate EA language and join both metamodels on a single unified model that captures the strong points of both standards. Lourinho states that when a COBIT5 process matches one or more ISO 27001 control categories, all the controls from that specific ISO category are relevant to the COBIT5 process and therefore is possible to create a direct structural association between ISO 27001 controls and COBIT 5 processes [11].

Due to this structural alignment between ISO 27001 and COBIT 5, the COBIT 5 process inputs and outputs can be modelled as Information Items using the ISO TS 330XX family of standards.

The mapping provides a top-down view of the alignment between COBIT5 and ISO standards, but does not detail the focus of our research, the COBIT5 Outputs.

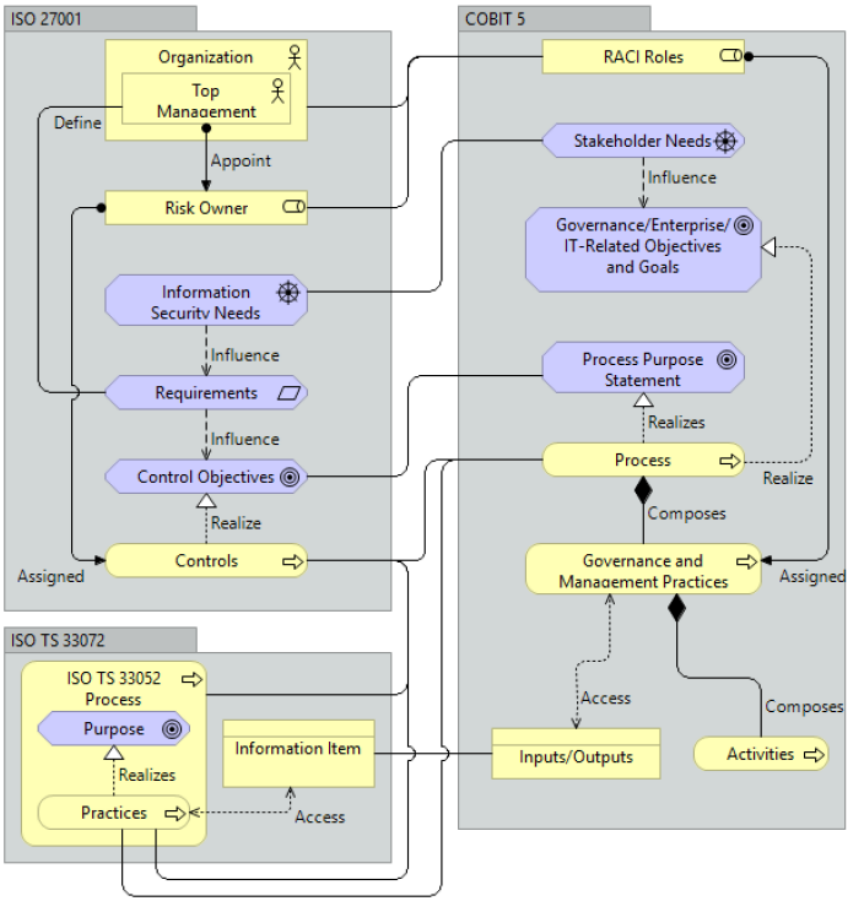

Figure 9: ISO 27001 - ISO TS 33052/3307 - COBIT5 Metamodel [10]

4.6. Using Enterprise Architecture for COBIT 5 Process Assessment and Process Improvement

Gonçalo Cadete on his master thesis provides a valuable research on the deficiencies of the process assessment model of COBIT5. Cadete recognizes that most enterprises possess a low self-awareness of the importance of documentation regarding its business processes and as a consequence need to allocate significate amounts of resources to the auditing and consulting activities for process capabilities [12]. Cadete focused his research on providing a better solution for evidence collection when gathering the evidence required for a COBIT5 capability assessment. His proposal focuses on mapping COBIT5's Process Assessment concepts using Enterprise Architecture notation in order to provide a fast and easy to read notation that helps both stakeholders and auditors to communicate what is required and reduce the amount of resources that the enterprise needs to allocate for the auditing processes. Cadete mapped the COBIT5's concepts to ArchiMate's concepts and proceeded to create viewpoints of COBIT5's process assessment model and metamodels for processes using ArchiMate as a proof-of-concept, as it can be shown in the figure below.

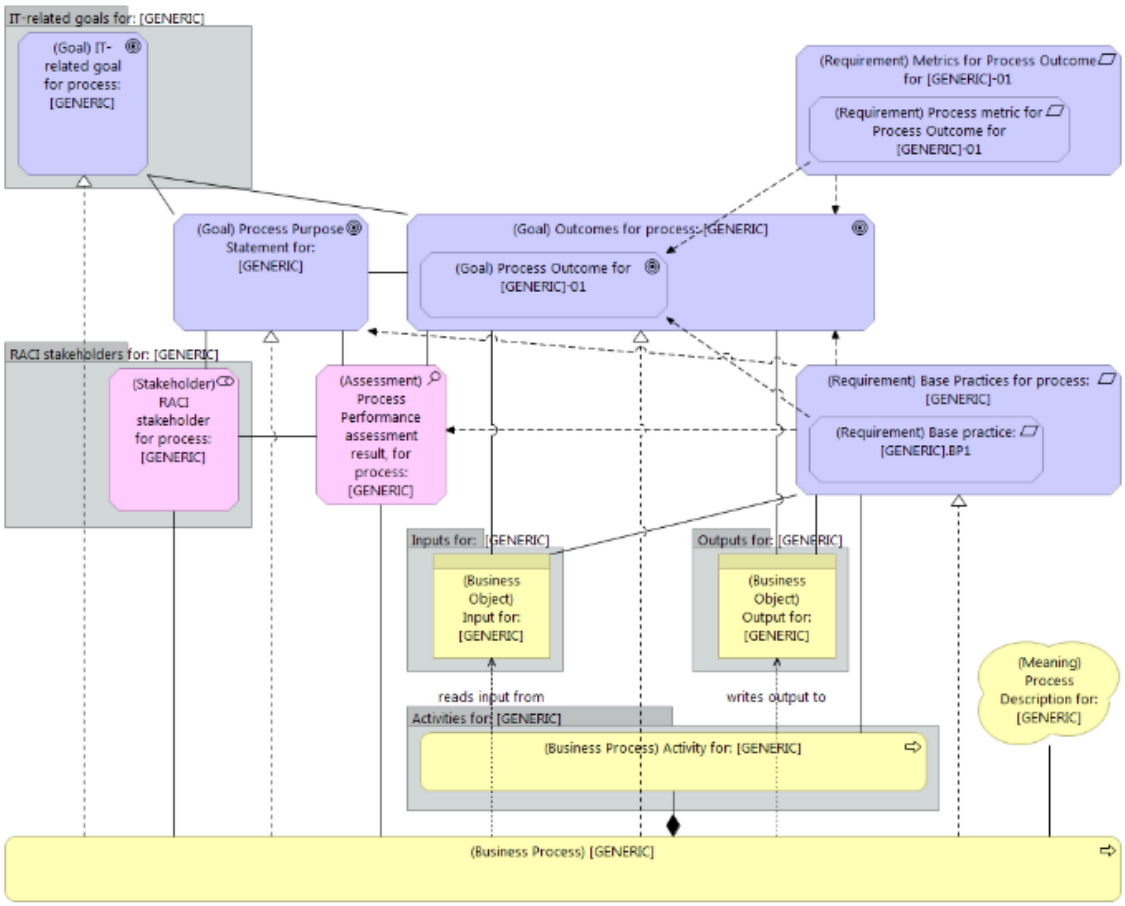

Figure 10: Generic ArchiMate template, for viewpoints used in COBIT 5 Process Performance Assessments [12].

He then proceeded to model viewpoints for each capability level transition for the APO012 process.

In his research, he concluded that by using EA notation is possible to adopt a single unified database that covers both COBIT5 PAM and COBIT5 GEIT rationales and allows the reduction of spent resources for process assessment due to the reduction of duplicate documentation [12]. The knowledge that we were able to extract from Cadete's research is that there is a gap in COBIT5's description of principles and is possible to reduce that gap by mapping COBIT5 to other standards. Although Cadete focused his research on GEIT and Process Assessment Model, the scope of his work did not cover the complete detailing and mapping of COBIT5's work products.

5. Proposal

In this section we will propose a representation for COBIT5's work products for their identification when analysing an organization's information items and processes.

The proposal of this thesis is: Describe in an easy to understand representation the description of COBIT5s work products using definitions from established standards and mappings.

This section corresponds to Design and Development phase of the DSRM methodology.

Observing the level 1 descriptions present on COBIT5's PAM (Process Assessment Model) we can spot several inconsistencies on the description of the work products. Some work products are described with little detail and others are only referenced as part of a process or a document.

The main objective of this proposal is to define in more detail what each work product is and where it is expected to be found on the enterprise's information items. We started by retrieving the information that COBIT5 provides for each work product, including its description and key concepts that are required to be detailed in order to fully understand the work product. Observing the detailed description that COBIT5 provides in its glossary for the outputs, we observed that although not all, most of the descriptions specify that the work product is a part of another concept, leaving to the reader the need for knowledge regarding the work product concepts. This section of the thesis includes the tables present on the Appendix. The tables present on the appendix were removed from this section in order to improve the readability of this document.

5.1. APO04 – Manage Innovation

For the initial proof-of-concept we chose APO04 as is shown in the table below. We recurred to ITIL for additional descriptions that better describe the work product.

Table 1: APO04 Work Product Mapping

Outcome/Work Product	COBIT5 Work Product Description	COBIT5 PAM Description	Detailed Description	References
WP1	Innovation plan	Innovation plan with the summary of approved and evaluated opportunities,	A set of guidelines and metrics to promote and support innovation within the enterprise.	ITIL Service Design[8]

		business benefits and risk articulated		Business Model Canvas [19]
WP2	Recognition and reward programme	Part of the strategic IT plan	A program that allows enterprise personnel to submit and explore innovative ideas that generate value to the business.	
WP3	Innovation opportunities linked to business drivers	Part of an innovation plan for applications and IT infrastructure articulated in a strategic IT plan	The innovation opportunities are classified and grouped to the corresponding business drivers.	ITIL CSI[10]
WP4	Research analyses of innovation possibilities	Found in an innovation planning process and will form part of a strategic IT plan	Evidence that the enterprise has a process to analyse innovation ideas and their feasibility.	
WP5	Evaluations of innovation ideas	Found in an innovation planning process and will form part of a strategic IT plan	Innovative ideas are evaluated and the results of the evaluation are recorded.	
WP6	Proof-of-concept scope and outline business case	Validation of assumptions for a proof of concept and will be part of the business case	A proof-of-concept that supports a innovative idea and subsequent business case scenario to support the proof-of-concept and assess the viability.	ITIL CSI[10] Business Model Canvas[19]

WP7	Test results from proof-of-concept initiatives	Part of a pilot or test found in an evaluation report	Measurable results from the proof-of-concept that allow conclusions to be taken regarding viability of the said initiative. Pilot Initiative: A limited Deployment of an IT Service, a Release or a Process to the Live Environment. A pilot is used to reduce Risk and to gain User feedback and Acceptance.	ITIL CSI[10] ITIL Service Design[8]
WP8	Results and recommendations from proof-of-concept initiatives	Part of a pilot or test found in an evaluation report	List of recommendations extracted from the results of a proof-of-concept initiative.	ITIL CSI
WP9	Analysis of rejected initiatives	Part of a pilot or test found in an evaluation report	Evidence that reject ideas are analysed for useful information regarding the reasons of being rejected and future viability.	
WP10	Assessments of using innovative approaches	Part of an innovation plan	Assessments of business processes that implement innovative ideas that passed the proof-of-	

			concept phase and were approved.	
WP11	Evaluation of innovation benefits	Part of the business case preparation and planning	Evaluation of possible benefits from innovative ideas and their impact on the business.	
WP12	Adjusted innovation plans	Final adjusted innovation plan	Evidence that innovation plans are adjusted and revised regularly and take into consideration new ideas for innovation a proof-of-concept evaluations.	

Although ITIL is able to fully describe some of the work products that are present in the APO process, ITIL shows its limitations when presented with the waterfall structure of COBIT5's enabling processes, therefore we needed to provide our own descriptions for the remaining work products that need to be verified and agreed-on by the experts.

Another way of adding additional knowledge for a specific work product is by providing an example or template to help the practitioner understand what to look for and ask for when performing a capability assessment. As an example, we will used APO01 Work Product 1 – Innovation Plan. The description that COBIT5 provides for this work product is well structured and detailed, however we can improve on the description by providing a template that will serve as a reference. Instead of creating a template for this work product, we concluded that Business Model Canvas matches the description of the work product and is a good example of an innovation plan as we can observe below.

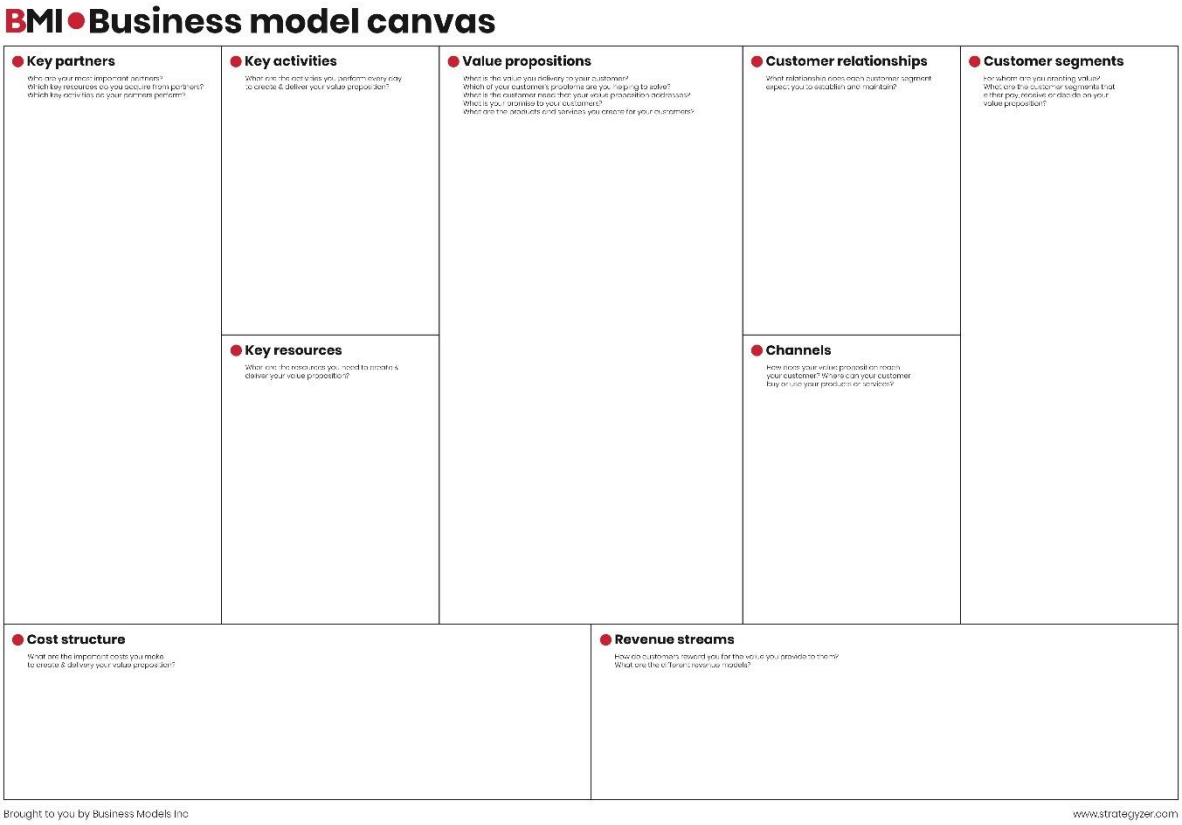

Figure 11: Business Model Canvas [19]

Using this methodology, we expanded the research to the remaining APO processes. Due to the nature of the APO family of processes, their level of granularity varies, with some processes being more low level and related to business operation and management and others more high level, almost reaching the level of the EDM family of processes.

5.2. APO02 – Manage Strategy

After we mapped the APO04 process work products using ITIL, we chose APO02 as the second proof-of-concept. APO02 was chosen due to being heavily related to the ITIL Service Strategy publication and had the potential to be one of the best examples of how the COBIT5 work products can be described in more detail using low level standards and definition. We then proceeded to map APO02's work products in the same fashion as APO04's, and the results can be found on the table below.

Table 2: APO02 Work Product Mapping

Outcome/Work Product	COBIT5 Work Product Description	COBIT5 PAM Description	Detailed Description	References

WP1	Sources and priorities for changes	Part of understanding the enterprise direction and looking at internal and external sources for change. This is part of the strategic planning process.	Changes to the IT should be classified and prioritised and ranked based on the current and future vision of the enterprise.	ITIL Service Strategy[7]
WP2	Baseline of current capabilities	An assessment of current business capabilities as part of the strategic planning process	Data regarding the current enterprise capabilities for future evaluation of changes.	ITIL CSI[10]
WP3	Gaps and risk related to current capabilities	Part of the capability assessment; gaps will be present in either a risk/gap register or remediation log.	List of gaps between current enterprise capabilities and the desired capabilities. Risk associated to those gaps.	ITIL Service Strategy[7]
WP4	Capability SWOT analysis	Part of the assessment of business capability in the strategic planning process	Analysis of the enterprise's strengths and weaknesses using a SWOT matrix.	ITIL Service Strategy[7]
WP5	High-level IT-related goals	Part of the strategic plan road map	List of IT-related goals to be achieved by the enterprise. The high-level goals should describe the vision defined by the enterprise at a High-level.	ITIL Service Strategy[7]

WP6	Required business and IT capabilities	Part of the strategic plan road map	Evaluation of the desired business and IT capabilities. The evaluation should answer the following questions: What do we want? What do we need?	ITIL CSI[10]
WP7	Proposed enterprise architecture changes	Part of both an enterprise architecture plan and the IT strategic plan	List of changes to the enterprise architecture to alight the IT strategy to the enterprise's goals and business needs.	ITIL Service Strategy[7]
WP8	Gaps and changes required to realise target capability	Part of the capability assessment; gaps will be present in either a risk/gap register or remediation log.	Gaps should be identified by performing a capability assessment on IT and business processes. Gaps are defined as unmet criteria when comparing actual performance to expected performance. The changes to achieve the target capability should take into consideration the current capability and the identified gaps.	ITIL CSI[10] ITIL Service Design[8]
WP9	Value benefit statement for target environment	Part of the IT strategic plan and results from the benefits analysis process of the IT Investment portfolio	A statement that succinctly describes the value benefits that are associated to the proposed changes on	ITIL CSI[10]

			the enterprise's strategy.	
WP10	Definition of strategic initiatives	Part of the strategic plan road map	Definition of initiatives that follow the enterprise's vision and strategic plan to generate value.	ITIL Service Strategy[7]
WP11	Risk assessment initiatives	Part of the risk assessment process and will be included in the strategic plan road map	Definition of initiatives to evaluate risk and create a risk management plan.	ITIL CSI[10]
WP12	Strategic road map	A plan that outlines the key steps/phases in getting or achieving a strategic plan	Road map that defines the direction that the enterprise should follow in order to generate value and meet stakeholders needs. Should contain the current state of the enterprise and short-term and long-term objectives to be achieved.	ITIL Service Strategy[7]
WP13	Communication plan	Part of a reporting and monitoring process for strategic planning	A plan that defines the communication flow between the key personnel and the enterprise's departments. Should describe what should be reported, who it should be reported to	ITIL CSI[10]

			and how it should be reported.	
WP14	Communicatio n package	The process outline for all communication dealing with strategic planning, includes the plan, methods and delivery of communication and frequency	The definition of the structure of the packages used on the enterprise's communication plan.	ITIL CSI[10]

Just as expected, the descriptions that are provided by COBIT5 mainly state that the work product is a part of a process or a document, perpetrating the problem of leaving to the practitioner the responsibility of knowing that the work product is and hoping that the enterprise provides enough information on their processes that allows the identification of the work product within the information items. The notable exceptions are WP2 and WP14 where COBIT5 provides a good description of what the work product is and what to look for on the enterprise's internal documentation.

In a similar fashion to APO04, we decided to provide templates as an example of how the work products can usually be found on the enterprises. We decided to provide a template of a communication plan to demonstrate what a usual communication plan would be implemented on an enterprise. In order to keep this section of the thesis within a reasonable size, the communication plan template can be found on the Appendix section.

5.3. Notable Work Product Mapping Examples

Last but not least, to conclude the information that is present on this section of the thesis, we provide on the table below a few notable examples of descriptions from different standards and frameworks that can be applied to the COBIT5's work products.

Table 3: Notable Examples of Work Product Mappings

Outcome / Work Product	**COBIT5 Output/Work Product**	**COBIT5 PAM Description**	**Detailed Description**	**References**
APO01 WP2	Enterprise operational guidelines	Part of the IT-related policies, procedures and practices for the IT management framework	List of guidelines and practices defined by the enterprise for achieving the enterprise's goals.	ITIL Service Operation[9]
APO03 WP10	Implementation phase descriptions	Part of the implementation plan for enterprise architecture	Description of the steps and actions required to achieve the desired architecture.	TOGAF - Phase F: Migration Planning[17]
APO05 WP4	Funding options	Reviewing source of funds statements as they relate to the investment portfolios	The funding sought by the business and IT for services delivered, based on the agreed value of those services. Financial Management calculates and assigns a monetary value to a service or service component so that they may be disseminated across the enterprise once the business customer and IT identify what services are actually desired.	ITIL Service Strategy 5.1 - Financial Management[7]

APO09 WP3	Service catalogues	All IT services and relevant target groups are documented in a catalogue.	A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the ITIL Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.	ITIL Service Design[8]
APO010 WP2	Supplier catalogue	Usually a supplementary system that typically identifies suppliers and associated contracts and categorises them into type, significance and criticality. Supplier and contract evaluation criteria should be established.	A database or structured Document with information about all active and considered suppliers, containing information about the current, previous or proposed contracts.	COBIT5[6]

6. Evaluation

The evaluation of the proposal corresponds to the Evaluation Phase of the Design Science and Research Methodology. In this section we will describe how the different components of our proposal will be evaluated.

The evaluation of our proposal will be performed using the following steps:

1. **Expert Review:** Present the design artifact to experts in the field of research, which consists in Enterprise Governance of IT, COBIT5 and ISO/IEC standards.
2. **Pries-Heje et al. framework:** Formal scientific evaluation using a framework made for Design Science Research.

Pries-Heje defines three research questions that need to be answered before applying its framework for Design Science Research Evaluation[13]:

- **What is actually evaluated:** The artifact is the center of the evaluation and therefore must be clearly defined. The artifact can be regarded as a design or a process.
- **How is it evaluated:** The chosen evaluation method. It can be naturalistic or artificial.
- **When was it evaluated:** The researcher must decide if the evaluation is performed *ex ante* (before the design of the artifact) or *ex post* (after the design of the artifact).

The design artefact of our proposed solution that will be evaluated will be the following: The mapping of COBIT5 Outputs using other standards and ArchiMate models.

Given the nature of our problem and its underlying proposed solution, implementing and evaluating its impact in an enterprise is not feasible within the timeframe that this research is bound to follow. In terms of risk, implementing an experimental framework for internal control can pose a severe risk for any enterprise. Therefore, the chosen evaluation method will be artificial evaluation. The evaluation will be performed by Expert Review, where several auditors with experience in COBIT5 and ISO standards will provide feedback on the proposal and its feasibility.

The evaluation is *ex post* since given the nature of the research problem, the evaluation will be performed after the design of the artefact.

6.1. First Iteration

After we finished mapping the APO work products using descriptions from other standards and relevant knowledge, we presented the artefacts to experts on COBIT5 for their evaluation and if they agreed with the descriptions and the mapping.

One of the experts agreed with the mapping and the descriptions for the work products. The expert also suggested the use of SFIA standard to reference when mapping human resource related work products. The expert also suggested that we provided a few concrete examples for work products as a proof of concept and to add value and credibility to the mapping. The expert also suggested that we highlighted work products whose description is ambiguous and / or are duplicated. Lastly, the expert pointe out that we were overly relying on the ITIL standard, namely ITIL Continual Service Improvement, to achieve the mapping of the outputs. The expert suggested the use of additional references to ISO 27001 for Information Security and ISO 9001 for Risk.

Due to time constraints, we were not able to fully present our results and were only able to present part of the APO family of processes. The second expert also agreed with the descriptions of the work products and with the initial mapping. As an improvement suggestion, the expert suggested exploring work product characteristics other than their description, namely its location on the information items or processes. The expert also pointed out the nature of COBIT5 and why some of the work products may appear duplicated on the same process or even ambiguous to being a result of the waterfall nature of COBIT5's processes.

We then concluded that we needed to provide more examples of templates for work products to increase the value of our research.

6.2. Second Iteration

After we presented the results to the first two experts, we added additional information to our mappings and gathered templates for Innovation Plan, Communication Plan and Service Level Agreement. We also revised our descriptions of the outputs, revising the work products that we previously considered ambiguous. We then presented the updated proposal to the last expert.

The last expert also agreed with the problem definition and the descriptions of the work products and also recognized the usefulness of providing additional knowledge to the definitions of COBIT5. However, the expert also noted that providing templates is only useful for a limited number of work products that are information items. Other work products, namely processes, states or enterprise architectures, cannot be exemplified with a template and therefore require other methods in order to be exemplified. The expert suggested using ontologies or enterprise architecture models to model key concepts of COBIT5 and its work products and use the models to compare to the models from the descriptions provided by the other standards.

After we presented the results to the expert, we concluded that our research has limitations in what type of work products it can provide examples for and how we can extend the research using other representations that can cover every type of process output present in COBIT5.

7. Conclusion

In this thesis, we researched the viability of improving the documentation of COBIT5. Fully understanding a best-practices standard such as COBIT5 is not possible and despite the efforts of ISACA to revise and improve their documentation, there are still a lot of concepts that are ambiguous, and their meaning is based on the interpretation of the practitioner performing the assessment.

COBIT5's process outputs and their PAM counterparts, the level 1 work products, are a prime example of limitations of COBIT5's design.

7.1. Lessons Learned

COBIT5 provides descriptions of the process outputs that for a practitioner that has enough knowledge of IT Governance and Management technical terms and in most cases this description is enough information when performing a process capability assessment. Due to its nature, COBIT5 references and borrows a lot of information from established standards related to IT and the authors made the decision to keep the description of technical terms simple and instead reference other standards that can help an practitioner to better understand COBIT5.

Using other standards and frameworks such as ITIL or ISO standards, it is possible to achieve a more complete description of the work products and what ISACA and the COBIT5 authors defined as process outputs and work products.

Mapping COBIT5's work products using related standards allows the practitioner to better understand what concepts and information items relate to the process work products and the use of templated as an example further illustrates the work product.

7.2. Main Limitations

One of the main limitations of the description of the work products using only definitions and example templates is that it only mitigates the problem. Work products that correspond to an information item can be exemplified by providing a template to the former. However, the implementation and structure of the information item varies from enterprise to enterprise and therefore the usefulness of the template is limited.

Other limitation of our research is that certain work products have a structure that cannot be represented using a template or a generic example. These work products usually are enterprise processes, parts of other work products or even states of information items and require other methods of representation to extend their description.

One possible solution to this problem is the suggestion made by Paulo Faroleiro, the expert that evaluated our proposal. His suggestion was to model the COBIT5 process outputs using an ontological approach to avoid the problems of misinterpretations of the descriptions while providing enough flexibility that allows every output to be modelled, independently of the latter being an information item, state of an information item, process or activity. Using a formal Enterprise Architecture notation like ArchiMate would be the preferred method for this approach.

7.3. Future Work

Although we only modeled a small group of work products, the work found in this thesis can be expanded by modelling all of the remaining COBIT5's work products, further expanding the knowledge of COBIT5 and providing useful information for knowing what to ask and look for when performing a Process Capability Assessment on an enterprise's processes. Our proposal results proved that it is possible to extend the definitions of COBIT5's process outputs using relevant / related standards and frameworks.

Other option for further work is to follow the suggestion of the experts and model the COBIT5's outputs using Enterprise Architecture notation, such as ArchiMate. This second option not only extends our research, but also extends the research present on Cadete's [12] and Lourinho's [11] master thesis.

Bibliography

[1] W. Grembergen and S. Haes, *Enterprise Governance of Information Technology*. 2009.

[2] S. de Haes and W. van Grembergen, “An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment,” *Inf. Syst. Manag.*, vol. 26, no. 2, pp. 123–137, 2009.

[3] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.

[4] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” vol. 24, no. 3, pp. 45–77, 2007.

[5] Isaca, *A Business Framework for the Governance and Management of Enterprise IT*. 2013.

[6] ISACA, *COBIT ® Process Assessment Model (PAM): Using COBIT ® 5*. 2013.

[7] S. Operation, “ITIL Version 3 Service Strategy,” *Serv. Manag.*, vol. 34, no. 19, pp. 1–396, 2011.

[8] L. Hunnebeck and A. T. Orr, “ITIL Version 3 Service Design,” *Service Design*. p. 456, 2011.

[9] S. Operation, “ITIL Version 3 Service Operation,” *Serv. Manag.*, vol. 34, no. 19, pp. 1–396, 2011.

[10] S. Operation, “ITIL Version 3 Service Management,” *Serv. Manag.*, vol. 34, no. 19, pp. 1–396, 2011.

[11] R. F. J. E. Lourinho, “Mapping and Integration of Enterprise Governance of IT Practices,” 2017.

[12] G. Cadete, “Using Enterprise Architecture for COBIT 5 Process Assessment and Process Improvement,” 2015.

[13] J. Pries-Heje, R. Baskerville, and J. R. Venable, “Strategies for Design Science Research Evaluation,” *Eur. Conf. Inf. Syst.*, no. 2004, p. 87, 2008.

[14] I. S. 9001:2008, “INTERNATIONAL STANDARD ISO / IEC / IEEE Quality management systems— Requirements,” vol. 2008, 2008.

[15] ISO, “ISO 31000:2009 Risk management -- Principles and guidelines,” *Iso 310002009(E)*, vol. 2000, p. 34, 2009.

[16] International Standards Organisation (ISO), “ISO/IEC 27001:2005-10 : Information technology - Security techniques - Information security management systems - Requirements,” vol. 2005, 2005.

[17] The Open Group, “ArchiMate 3.0.1”,
Available: http://pubs.opengroup.org/architecture/archimate3-doc/

[18] The Open Group, “The TOGAF Standard”,
Available: http://www.opengroup.org/subjectareas/enterprise/togaf

[19] Strategyzer, “Business Model Canvas”, Available:
https://strategyzer.com/canvas/business- model-canvas

[20] SFIA, “Skills Framework for the Information Age”,
Available: https://www.sfia-online.org/en

Appendixes

Appendix A – APO01 Work Product Mapping

Table 4: APO01 Work Product Mapping

Outcome/Work Product	**COBIT5 Work Product Description**	**COBIT5 PAM Description**	**Detailed Description**	**References**
WP1	Definition of organisational structure and functions	Part of the IT management framework related to IT organisation	The organizational structure is defined according to the business and stakeholder's needs. Core functions within the enterprise structure are defined and described.	ITIL Service Design[8]
WP2	Enterprise operational guidelines	Part of the IT-related policies, procedures and practices for the IT management framework	List of guidelines and practices defined by the enterprise for achieving the enterprise's goals.	ITIL Service Design[8]
WP3	Communication ground rules	Part of a monitoring and reporting process in the IT management framework	Set of rules that define the flow of communication within the enterprise. These rules should describe what should be reported, how it should be reported and to who should be reported.	ITIL Service Operation[9]

WP4	Definition of IT-related roles and responsibilities	A RACI chart will outline these roles and responsibilities.	Definition of key IT-related roles within the enterprise. Each definition should include the role description, its responsibilities, main activities and accountability. RACI charts should be defined to better describe each role and associated activities.	ITIL Service Design[8] ITIL Service Operation[9]
WP5	Definition of supervisory practices	Part of the IT-related policies, procedures and practices for the IT management framework	Set of practices for the supervisory of the IT and its personnel. Usually associated to the role of the Process Owner.	ITIL Service Design[8]
WP6	IT-related policies	Policies and/or operating practices/ standards that reflect IT operations and accountabilities	Set of policies defined by the enterprise for IT management and operation.	
WP7	Communication on IT objectives	Part of a monitoring and reporting process for defining an IT framework	IT objectives are communicated to the key personnel within the enterprise, either in the form of frequent meetings or access to a document containing the defined objectives.	ITIL Service Operation[9]

WP8	Evaluation of options for IT organisation	Part of the IT management framework related to IT organisation	A set of options for the organization of IT is defined as part of process design or continual improvement. The evaluation of the former should produce a report that contains the benefits and costs associated with each option.	ITIL Service Design[8]
WP9	Defined operational placement of IT function	Part of the IT management framework related to IT organisation	The IT function should be traceable and its placement within the enterprise should be defined and described.	ITIL Service Operation[9]
WP10	Data classification guidelines	Part of an enterprise architecture plus data retention and risk management policy	Guidelines for data classification and storage. The guidelines should cover the several types of data collected by the enterprise and should provide complete descriptions for its classification and storage method.	
WP11	Data security and control guidelines	Part of the IT-related policies, procedures and	Guidelines define by the enterprise for data storage and security.	ITIL Service Operation[9]

		guidelines, but specific to data security		
WP12	Data integrity procedures	Part of the IT-related policies, procedures and guidelines, but specific to data security; these are the more detailed procedures.	Part of Database Management. List of procedures and practices for maintaining data integrity and readability.	ITIL Service Operation[9]
WP13	Process capability assessments	Part of a monitoring and reporting process for defining an IT framework such as COBIT PAM	Frequent assessments and evaluation of capability of the enterprise's business processes.	ITIL CSI[10]
WP14	Process improvement opportunities	Opportunities to improve arising from the use of a monitoring and reporting process for defining an IT framework	List of possible improvements to a business process within the enterprise as part of a Continual Service Improvement evaluation. Usually part of a business case for process improvement.	ITIL CSI[10]
WP15	Performance goals and metrics for process improvement tracking	Part of a monitoring and reporting process for defining an IT framework	Performance goals defined by the enterprise for each business process. Each goal should provide a metric for performance measurement during	ITIL CSI[10]

			process assessments.	
WP16	Non-compliance remedial actions	Part of the IT-related policies, procedures and practices for the IT management framework	List of actions to achieve process compliance to the expected performance after a process assessment concluded that a business process is not performing according to the standards defined by the enterprise.	ITIL CSI[10]

Appendix B – APO03 Work Product Mapping

Table 5: APO03 Work Product Mapping

Outcome/Work Product	**COBIT5 Work Product Description**	**COBIT5 PAM Description**	**Detailed Description**	**References**
WP1	Defined scope of architecture	Part of the definition of a reference enterprise architecture model	The extent of information regarding the architecture adopted by the enterprise.	
WP2	Architecture principles	Part of the definition of a reference enterprise architecture model	List of principles that define the adopted enterprise architecture model.	
WP3	Architecture concept business case and value proposition	Business case proposal for an architecture concept	A business case that applies an enterprise architecture model	TOGAF Phase A: Architecture Vision[18]

			to the enterprise and studies the potential value on adopting said model and required changes to the enterprise for its adoption.	
WP4	Baseline domain descriptions and architecture definition	Part of an enterprise architecture model	A baseline description is a description of the enterprise and its current architecture. Domain descriptions should provide a partial overview of how the enterprise is structured and defined according to the current business drivers and stakeholder's needs.	TOGAF Phase B: Business Architecture[18]
WP5	Process architecture model	A typical process architecture model organises the logic for business process and IT infrastructure, which reflects the integration and standardisation requirements of the enterprise operating model.	A model that formally describes the enterprise's processes and supply chains and how they are structured.	
WP6	Information architecture model	Part of an enterprise architecture model, but will specifically relate to how	A model that describes the enterprise's key concepts and how it	

		information is organised	operates the business.	
WP7	High-level implementation and migration strategy	Implementation and migration strategy for architecture	The last stage of implementing an enterprise architecture. Migration strategy is defined as a set of actions required for the implementation of the architectures. The strategy should contain detailed information regarding time, cost and success factors. Should answer the question - "How we plan to get there".	
WP8	Transition architectures	Part of the implementation and migration strategy for architecture	Architectures that replace existing architecture in order to achieve the planned enterprise architecture roadmap.	TOGAF - Transition Architectures[18]
WP9	Resource requirements	Part of the implementation plan for enterprise architecture	Resource requirements required to achieve the architecture roadmap.	
WP10	Implementation phase descriptions	Part of the implementation plan for enterprise architecture	Description of the steps and actions required to achieve	TOGAF - Phase F: Migration Planning[18]

			the desired architecture.	
WP11	Architecture governance requirements	Part of the enterprise architecture model or framework governance requirements	Requirements to achieve the target architecture through the implementation of projects.	TOGAF: Phase G: Implementation Governance[18]
WP12	Solution development guidance	Part of the implementation plan for enterprise architecture	Guidance to ensure that solutions achieve conformance with the target architecture. Scope and priorities should be well defined as well as resources and skills.	TOGAF: Phase G: Implementation Governance[18]

Appendix C – APO05 Work Product Mapping

Table 6: APO05 Work Product Mapping

Outcome/Work Product	**COBIT5 Work Product Description**	**COBIT5 PAM Description**	**Detailed Description**	**References**
WP1	Defined investment mix	Part of the investment portfolio	The overall mix or combination of the various investments, usually contained in a portfolio. The mix should align with the enterprise's vision and strategy.	

WP2	Identified resources and capabilities required to support strategy	Reviewing the strategy to identify the enterprise capabilities in support of the strategy	A list or description of resources that support the enterprise's goal and strategy. The list should contain information regarding WHEN and WHERE said resources support the current and future business opportunities.	
WP3	Feedback on strategy and goals	Part of a monitoring and communications plan to report on portfolio management	Tangible evidence that strategic plans and goals are approved by the board.	
WP4	Funding options	Reviewing source of funds statements as they relate to the investment portfolios	The funding sought by the business and IT for services delivered, based on the agreed value of those services. FM calculates and assigns a monetary value to a service or service component so that they may be disseminated across the enterprise once the business customer and IT identify what services are actually desired.	ITIL Service Strategy[7]

WP5	Investment return expectations	Part of the management of benefits of the portfolios	Investment Expectations based of two premises: 1- The investment cost; 2- The return gain. The expectations should be clearly identifiable on an investment portfolio.	ITIL CSI[10]
WP6	Programme business case	Part of the business case process. There may be several programme business cases, depending on the number and types of portfolios.	The Business Case should articulate the reason for undertaking a service or process improvement initiative. As far as possible, data and evidence should be provided relating to the costs and expected benefits of undertaking process improvement.	ITIL CSI[10]
WP7	Business case assessments	For both project and programmes	Measure the benefits actually achieved. These measurements attest to whether the improvement activity achieved the intended outcomes and should consider: • Whether the envisaged improvements were realized • Whether the	ITIL CSI[10]

			benefits arising from the improvements were achieved • Whether the target ROI was achieved • Whether the intended value-added was actually achieved (VOI) • Whether the outcomes of the preceding points lead to further process improvement actions being re-evaluated • Whether enough time has passed before measuring the benefits. Some benefits will not be immediately apparent; and it is likely that benefits will continue to change over time, as both ongoing costs and ongoing benefits continue to move.	
WP8	Selected programmes with return on investment (ROI) milestones	Part of the programme business case	Investment programmes present of the portfolio should contain defined ROI milestones.	
WP9	Investment portfolio performance reports	Part of a monitoring and communications plan to report on portfolio management	Evidence of evaluation of investment portfolio and previous	

			programmes contained within it.	
WP10	Updated portfolios of programmes, services and assets	Part of the portfolio maintenance process. Assessors should verify that such a process exists and provides sufficient audit reporting to verify that portfolios are effectively maintained.	Evidence that portfolios are up to date and properly documented in order to comply with the enterprise's requirements.	
WP11	Benefit results and related communications	Part of a monitoring and communications plan to report on portfolio management. These will be articulated as part of programme business cases.	Evidence of communication of results and related information throughout the enterprise as established on the communication plan.	
WP12	Corrective actions to improve benefit realisation	Part of a benefits realisation plan	Investment portfolios and programmes should contain a list of corrective actions for benefit realisation based of the performance reports.	

Appendix D – APO06 Work Product Mapping

Table 7: APO06 Work Product Mapping

Outcome/Work Product	COBIT5 Work Product Description	COBIT5 PAM Description	Detailed Description	References

WP1	Accounting processes	For managing IT-related expenditures. Most IT departments will have their own system for managing costs and budgets and business allocations or be part of or integrated into the main enterprise accounting systems.	The process of recording monetary information from the IT.	
WP2	IT costs classification scheme	Part of the IT accounting system	How IT cost are classified within the enterprise. IT costs can be classified as business expenses (IT as a service) or as components of a larger product.	
WP3	Financial planning practices	Part of the enterprise financial planning system integrated into the IT cost and budget systems. Look for the enterprise policy and procedures.	List of practices defined by the enterprise for financial planning of IT	

WP4	Prioritisation and ranking of IT initiatives	Part of the IT budgetary control system, which will be part of the accounting process	Set of guidelines defined by the enterprise for IT initiative prioritization. Current IT initiatives should contain evidence of prioritization and should have a priority ranking	
WP5	Budget allocations	Part of the IT accounting system and agreed on with the business	The percentage of the total IT budget that is allocated to a specific service or investment.	
WP6	IT budget and plan	Also will report outputs from the IT accounting system or process	Definition of a budget to be allocated to the IT based on existing services and infrastructure.	
WP7	Budget communications	Part of the IT financial reporting process. Budgets, plans and variance analysis will be reported as part of this process.	Evidence of communication of budgets and related information throughout the enterprise as established on the communication plan.	

WP8	Categorised IT costs	Part of the IT accounting system and agreed on with the business	Quantification, in financial terms, of the value of IT Services, the cost of the assets underlying the provisioning of those services, and the qualification of operational forecasting.	ITIL Service Strategy[7]
WP9	Cost allocation model	Part of the IT accounting system and agreed on with the business	Internal model for allocating costs associated to IT to the departments that benefit from the IT services	
WP10	Cost allocation communications	Part of the IT financial reporting process. Budgets, plans and variance analysis will be reported as part of this process.	Evidence of communication of cost allocation and related information throughout the enterprise as established on the communication plan.	
WP11	Operational procedures	Based on the regular review performed, revise existing procedures, or create new ones,	List of procedures at operational level to ensure that costs are	

		to meet new or changed requirements	aligned with the budget estimates.	
WP12	Cost data collection method	Part of the IT financial reporting process. Budgets, plans and variance analysis will be reported as part of this process.	Evidence of data collection activities on the cost management process.	
WP13	Cost consolidation method	Part of the IT financial reporting process. Budgets, plans and variance analysis will be reported as part of this process.	Evidence of cost consolidation on the cost management process.	
WP14	Cost optimisation opportunities	Part of the IT financial reporting process. Budgets, plans and variance analysis will be reported as part of this process.	Opportunities for reducing operational costs on the enterprise's processes. Obtained from a cost analysis of each business process.	

Appendix E – APO07 Work Product Mapping

Table 8: APO07 Work Product Mapping

Outcome/Work Product	COBIT5 Work Product Description	COBIT5 PAM Description	Detailed Description	References / Observations
WP1	Staffing requirement evaluations	Part of business and IT planning cycles, usually annually, and forms part of the operating plans and budgets. HR departments will contain planning reports that are input into the main plans.	Evidence of evaluation of IT and enterprise requirements that take into account human resources needed to fulfil said requirements.	Description provided by COBIT5 is already self-explanatory
WP2	Competency and career development plans	Forms part of the business and IT operating plans and be part of the HR systems	List of expected competencies defined by the enterprise to ensure the human resources support enterprise's goals and objectives.	SFIA - IT Management [20]
WP3	Personnel sourcing plans	An evaluation of internal and external sources, depending on the competencies required for both IT and business	List of requirements and actions defined by the enterprise for sourcing personnel.	Description provided by COBIT5 is already self-explanatory

WP4	List of key personnel	Listing of personnel whose job roles are considered critical to the success of the enterprise	List of personnel required for the smooth operation of the enterprise's processes that perform critical functions within the enterprise.	Description provided by COBIT5 is already self-explanatory
WP5	Skills and competencies matrix	A matrix that maps skills and competencies to the specific job or role	A matrix that represents each individual role's skill and competencies similar to a RACI chart.	Description provided by COBIT5 is already self-explanatory
WP6	Skills development plans	A skills plan that identifies competency gaps and plans for development		Description provided by COBIT5 is already self-explanatory
WP7	Review reports	Part of the HR reporting system. Assessors should confirm with management what reports exist.	Evidence that reports on personnel are reviewed and updated regularly.	
WP8	Personnel goals	Forms part of a staff annual appraisal or performance evaluation process	Evidence that the enterprise sets goals for its personnel so they maintain the required performance.	

WP9	Performance evaluations	Usually annually and part of the appraisal process	Evaluation of personnel to ensure that they are performing their activities as expected and have the competencies to fulfil their roles on the enterprise.	
WP10	Improvement plans	Part of the performance evaluation specific to the person being evaluated	List of objectives and actions for personnel improvement, defined by the enterprise. The improvement plans can include qualification and certification programmes.	
WP11	Inventory of business and IT human resources	Part of the HR reporting system. Assessors should confirm with management what reports exist.	Evidence of Human Resources inventory. A complete list of personnel on the enterprise and a file for each individual.	
WP12	Resourcing shortfall analyses	Part of the skills development plans	Evidence of analysis / simulation of a human resources	

			shortfall and associated conclusions/ corrective or pre-emptive actions.	
WP13	Resource utilisation records	Part of the HR system	Stored information regarding human resource utilization on the enterprise.	
WP14	Contract staff policies	Some HR systems contain separate processes and master files for all contracts.	Set of policies for staff contracts set by the enterprise according to the enterprise's vision and goals	
WP15	Contract agreements	Some HR systems contain separate processes and master files for all contracts.	Documents containing contract agreements of each staff/personnel on the enterprise.	
WP16	Contract agreement reviews	Should be done with HR and IT and the business	Evidence that contract agreements are up to date and regularly reviewed.	

Appendix F – APO08 Work Product Mapping

Table 9: APO08 Work Product Mapping

Outcome/Work Product	COBIT5 Work Product Description	COBIT5 PAM Description	Detailed Description	References / Observations
WP1	Clarified and agreed-on business expectations	Forms part of the business and IT operating plans. Sometimes these are reflected in specific SLAs or OLAs		Description provided by COBIT5 is already self-explanatory
WP2	Agreed-on next steps and action plans	Forms part of the business and IT operating plans and/or business and IT service delivery plans	The action plan derived of CSI (continual service improvement) of the IT is understood and agreed by the senior board and stakeholders.	ITIL CSI[10]
WP3	Agreed-on key decisions	Forms part of the business and IT operating plans and/or business and IT service delivery plans	Evidence that every stakeholder understands and agrees on key decisions for CSI (continual service improvement) of IT.	ITIL CSI[10]

WP4	Complaint and escalation status	Forms part of the contract process	A complaint escalation process is defined and in use by the enterprise. Escalation status should be easily known upon request.	
WP5	Communication plan	Part of a reporting and monitoring process for strategic planning	A plan to establish communication and reporting rules within the enterprise. Key activities for the communications plan include: • Identifying stakeholders and target audiences • Developing communications strategies and tactics • Identifying communication methods and techniques • Developing the communications plan (a matrix of who, what, why, when where and how) • Identifying the project	ITIL CSI[10]

			milestones and related communications requirements.	
WP6	Communication packages	The process outline for all communication dealing with relationship planning. It will include the plan, methods and delivery of communication, and frequency.	The message that is communicated through the communication plan. For every reporting activity within the communication plan the purpose and objective of the message must be clearly defined.	ITIL CSI[10]
WP7	Customer responses	Part of the communication package especially for periodic customer (internal and external) surveys and assessments	Customer data and responses in the form of satisfaction surveys are stored and easily accessible for CSI.	ITIL Service Operation[9]

WP8	Satisfaction analyses	Part of the communication package especially for periodic customer (internal and external) surveys and assessments	Customer satisfaction surveys are analysed, and the overall satisfaction level of the customer base is known to the appropriate members of the enterprise.	ITIL Service Operation[9]
WP9	Definition of potential improvement projects	Identify potential opportunities for IT to be an enabler of enhanced enterprise performance as part of the communication package and strategic IT plan.	Use the knowledge gained from a CSI (Continual Service Improvement) to optimize, improve and correct services and processes. Managers need to identify issues and present solutions. Explain how the corrective actions to be taken will improve the service.	ITIL CSI[10]

Appendix G – APO09 Work Product Mapping

Table 10: APO09 Work Product Mapping

Outcome/Work Product	COBIT5 Work Product Description	COBIT5 PAM Description	Detailed Description	References / Observations
WP1	Identified gaps in IT services to the business	Part of a service catalogue process, which contains SLAs and OLAs to allow effective monitoring and reporting of gaps	Evidence that an evaluation process is performed on the IT services. Gaps in IT services can be defined by evaluating how the services are performing and comparing the data to the expected performance.	ITIL CSI[10]
WP2	Definitions of standard services	Usually found in a service catalogue	All Live IT Services, including those available for Deployment.	ITIL Service Design[8]
WP3	Service catalogues	All IT services and relevant target groups are documented in a catalogue.	A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the	ITIL Service Design[8]

			only part of the ITIL Service Portfolio published to Customers and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes.	
WP4	SLAs - Service Level Agreements	SLAs are defined in the service catalogue. An SLA is a part of a service contract where the level of service is formally defined.	An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple customers. A	ITIL Service Design[8]

			good SLA should contain the following concepts: Type of service to be provided; The service's desired performance level; Monitoring process and service level reporting; The steps for reporting issues with the service; Response and issue resolution time-frame; Repercussions for service provider not meeting its commitment.	
WP5	OLAs - Operational Level Agreements	OLAs are defined in the service catalogue. An OLA defines the interdependent relationships amongst the internal support groups of an organisation working to support a SLA.	Agreement between an IT Service Provider and another part of the same Organization. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or	ITIL Service Design[8]

			Services to be provided and the responsibilities of both parties	
WP6	Service level performance reports	Forms part of the monitoring and reporting process and is periodic, usually monthly and/or quarterly	Performance reports that evaluate and compare expected service performance to actual service performance. Similar to process performance reports.	ITIL Service Operation[9]
WP7	Improvement action plans and remediations	Comes out of the monitoring and reporting process and will usually be found in an issues log	List of corrective actions required for the service to meet the target performance. Corrective action is the result of the CSI improvement process evaluation.	ITIL CSI[10]
WP8	SLA revisions	Based on improvement action plans, assessor should verify if and when SLAs are updated.		Description provided by COBIT5 is already self-explanatory

Appendix H – APO010 Work Product Mapping

Table 11: APO010 Work Product Mapping

Outcome/Work Product	COBIT5 Work Product Description	COBIT5 PAM Description	Detailed Description	References / Observations
WP1	Supplier significance and evaluation criteria	Forms part of a procurement system, which will have reports analysing the supplier or vendor master file	A document containing the criteria for evaluating a deciding on suppliers as defined by the enterprise goals and needs. The criteria should respond to que following questions: What is the supplier's role on the enterprise's business strategy; How the supplier is evaluated.	
WP2	Supplier catalogue	Usually a supplementary system that typically identifies suppliers and associated contracts and categorises them into type, significance and criticality. Supplier and contract evaluation	A database or structured Document with information about all active and considered suppliers, containing information about the current,	

		criteria should be established.	previous our proposed contracts.	
WP3	Potential revisions to supplier contracts	New or changed contracts should conform to enterprise standards and legal and regulatory requirements. Any contractual disputes are dealt with and contract revisions made.	Evidence that the enterprise has an active process for evaluating supplier contracts and evidence that supplier contracts are up-to-date.	
WP4	Supplier requests for information (RFIs) and requests for proposals (RFPs)	RFIs and RFPs are part of a formal supplier selection process.	A Request for Information (RFI) is a business process used by customers to collect written information regarding the capabilities of various suppliers. A request for Proposals is a process similar to the RFI but aimed at selecting suppliers for a	

			specified service or asset.	
WP5	RFI and RFP evaluations	Part of the supplier selection process	Evidence that the enterprise regularly reviews RFIs and RFPs. There is an internal process for RFI and RFP evaluation and supplier catalogue is up-to-date	
WP6	Decision results of supplier evaluations	Part of the supplier selection process		
WP7	Supplier roles and responsibilities	Outlined is a supplier catalogue	A document or database containing information regarding the enterprise's suppliers with information regarding their current and previous roles and responsibilities.	
WP8	Communication and review process	Part of a supplier monitoring and reporting process.	Evidence that the enterprise has an	

		Assessors should check for periodic reviews of supplier performance.	internal process for supplier management that is responsible for the communication with the suppliers.	
WP9	Results and suggested improvements	Part of a supplier monitoring and reporting process. Assessors should check for periodic reviews of supplier performance.	List of obtained results corrective actions to be taken in order for supplier management to meet the business requirements.	
WP10	Identified supplier delivery risk	Part of a supplier risk assessment and should be present in the contract process	Risk is defined as the chance of exposure to the adverse consequences of future events. Supplier delivery is the risk associated to the ability of the suppliers to deliver the agreed service or product. This risk can be identified and found on the risk assessment document, work	

			product of the risk management process.	
WP11	Identified contract requirements to minimise risk	Part of a supplier risk assessment and should be present in the contract process	Contract requirements present on the supplier's contract agreement that align and minimise the associated risk found on the risk assessment for the specified service or product provided by the supplier.	
WP12	Supplier compliance monitoring criteria	Part of a supplier monitoring and reporting process. Assessors should check for periodic reviews of supplier performance.	List of requirements and actions specified by the enterprise for supplier compliance. Contained in the document with the remaining criteria for supplier management.	

WP13	Supplier compliance monitoring review results	Part of a supplier monitoring and reporting process. Assessors should check for periodic reviews of supplier performance and compliance, especially with legal and statutory requirements.		Description provided by COBIT5 is already self-explanatory

Appendix I – APO011 Work Product Mapping

Table 12: APO011 Work Product Mapping

Outcome/Work Product	**COBIT5 Work Product Description**	**COBIT5 PAM Description**	**Detailed Description**	**References / Observations**
WP1	Quality management system (QMS) roles, responsibilities and decision rights	A QMS is established to outline clear roles, responsibilities and decision rights (who is accountable and authorised to make the decision).		Description provided by COBIT5 is already self-explanatory
WP2	Quality management plans	An overall quality plan should be maintained that promotes continuous improvement. This should include the need for, and benefits of, continuous improvement. Assessors should		Description provided by COBIT5 is already self-explanatory

		collect and analyse data about the QMS, and check for the effectiveness of the QMS.		
WP3	Results of QMS effectiveness reviews	Part of a continuous monitoring and reporting process	Assessment of actual QMS performance. Acquired data should be compared to the expected performance.	ISO 9001[14]
WP4	Quality management standards	Part of the QMS and should be in line with the IT control framework requirements	Quality standards for a certain product or service adopted by the enterprise for quality assurance.	ISO 9001[14]
WP5	Customer requirements for quality management	Customer requirements should be aligned in the QMS.	List of expected quality criteria and requirements defined by the customer for a specific product or service.	
WP6	Acceptance criteria	Part of the QMS and should be in line with the IT control	Criteria to measure a service or a product in order	

		framework requirements	to determine if it meets the expected quality standards.	
WP7	Review results of quality of service, including customer feedback	Part of a continuous monitoring and reporting process	Evidence that quality control is performed regularly, and customer feedback is performed and taken into consideration.	
WP8	Results of quality reviews and audits	Part of a continuous monitoring and reporting process	Quality reviews and audits present their results in a structured manner that is easy to read and extract relevant information.	
WP9	Process quality of service goals and metrics	Part of the QMS and should be in line with the IT control framework requirements	A set of quality related goals and metrics for the enterprise's processes that reflect the quality plan and standards.	
WP10	Results of solution and service delivery quality monitoring	Part of a continuous monitoring and reporting process and will typically be a periodic report	Service delivery and quality monitoring should produce results that are measurable and quantifiable.	

			Quality assessment should be able to measure those results.	
WP11	Root causes of quality delivery failures	Part of a continuous monitoring and reporting process and can be found in a root cause log or register	Quality delivery failures should be well documented and accessible, and the root cause of the former should be easily identifiable.	
WP12	Communications on continual improvement and best practices	Part of a continuous monitoring and reporting process and can be found in periodic reporting to management	Quality standards and continual improvement is communicated to the respective entities within the enterprise. Key personnel should be aware of the changes required for continual improvement and best practices.	ITIL CSI[10]
WP13	Examples of good practice to be shared	Part of a continuous monitoring and reporting process and can be found from analysis of review meetings and	A list of good practices and examples for quality assurance should exist and be formatted to	

		management reporting	the target personnel within the enterprise.	
WP14	Quality review benchmark results	Part of a continuous monitoring and reporting process and can be found from a process capability or maturity modelling assessment	Quality reviews and benchmarks present their results in a structured manner that is easy to read and extract relevant information.	ISO 9001[14]

Appendix J – APO012 Work Product Mapping

Table 13: APO012 Work Product Mapping

Outcome/Work Product	**COBIT5 Work Product Description**	**COBIT5 PAM Description**	**Detailed Description**	**References / Observations**
WP1	Data on the operating environment relating to risk	An assessor would review the enterprise risk assessment process that contains a risk profile, scenarios, events, a risk register and reporting tools. The risk profile will show all relevant data on the operating environment.		Description provided by COBIT5 is already self-explanatory
WP2	Data on risk events and contributing factors	Part of the enterprise risk profile	Relevant information regarding	ISO 31000[15]

			events and other factors that may lead to risk and are required for a risk assessment to be performed.	
WP3	Emerging risk issues and factors	Part of the enterprise risk profile	Risk factors that are not present on the enterprise's current risk treatment process and should be taken into consideration for improving risk treatment.	ISO 31000[15]
WP4	Scope of risk analysis efforts	Part of the enterprise risk profile	The definition of the extent to which the enterprise requires the risk analysis to be performed.	ISO 31000[15]
WP5	IT risk scenarios	Part of the enterprise risk profile. Scenario analysis is a process of analysing possible future events by considering alternative possible outcomes and or events, e.g., loss of data due to disaster.	Documented scenarios that demonstrate how a certain risk can occur, the factors that allow the risk to occur and the risk mitigation processes that the enterprise possesses to	

			address the risk after it occurs.	
WP6	Risk analysis results	Outcomes of a risk assessment show impacts, probabilities and how they are managed.		Description provided by COBIT5 is already self-explanatory
WP7	Documented risk scenarios by line of business and function	See risk profile and IT risk scenarios. This is part of the enterprise risk management plan.	Risk scenarios are separated and categorised by their nature and the line of business on which they are based.	ISO 31000[15]
WP8	Aggregated risk profile, including status of risk management actions	The IT risk register contains this information.	A profile for each risk that was identified by a risk analysis. The profile should contain information regarding the risk, the factors that can cause the risk, impact of the risk on the business and remedial actions for mitigating said risk. The risk remedial actions should contain enough information of	

			their status to assess whether they are deployed or proposed.	
WP9	Risk analysis and risk profile reports for stakeholders	Part of the risk assessment process and ongoing monitoring and reporting, usually quarterly for ongoing and at project or programme start-up and also for new IT application and software developments		Description provided by COBIT5 is already self-explanatory
WP10	Results of third-party risk assessments	Part of third-party and contract reviews	Complete risk analysis and results but performed by a third party. The structure of the risk assessment should be similar to the description of the internal risk analysis.	ISO 31000[15]
WP11	Opportunities for acceptance of greater risk	Depends on the organisation's risk appetite, which should be defined in the risk profile	Description of possible scenarios where there is a risk that is above the risk threshold defined by the	ISO 31000[15]

			enterprise. These opportunities should describe the associated factors and benefits for accepting the increased risk.	
WP12	Project proposals for reducing risk	Part of the risk management process, it usually is based on an analysis of the risk register and periodic reporting process	List of proposed changes to either the business model or the enterprise's processes aimed at minimising or mitigating a known and well documented risk.	ISO 31000[15]
WP13	Risk-related incident response plans	Linked to the IT and information security incidence response and reporting process	Defined plan of action and associated procedures to be executed in the event that a certain risk occurs. The plans should align with the associated risk profile.	ISO 31000[15]

WP14	Risk impact communication	Part of the risk assessment and risk reporting process	Risk details and impact are communicated to the respective entities within the enterprise. Key personnel should be aware of the risk and have access to the according risk information.	
WP15	Risk-related root causes	Part of the risk assessment and risk reporting process	Root causes for a specific risk are identified and properly documented.	

Appendix K – APO013 Work Product Mapping

Table 14: APO013 Work Product Mapping

Outcome/Work Product	**COBIT5 Work Product Description**	**COBIT5 PAM Description**	**Detailed Description**	**References / Observations**
WP1	ISMS policy	There will be either a policy, standard or operating practice that will be part of the ISMS.	Policy that applies to part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and	ISO 27001[16]

			improve information security.	
WP2	ISMS scope statement	Part of the ISMS strategy and planning documentation or the ISMS programme outline	Statement that succinctly explains the direction taken by the enterprise for information security.	ISO 27001[16]
WP3	Information security risk treatment plan	Part of the ISMS risk assessment process based on the risk profile	Risk treatment assessment and processes dedicated to information security related risks.	
WP4	Information security business cases	Only if required for an information security project or programme	Real or simulated business cases that demonstrate the need for an ISMS and the procedures defined on the ISMS policy. Part of the "Communicating the vision" concept.	ISO 27001[16]

WP5	ISMS audit reports	Part of internal audit reporting or monthly information security reporting, which will also be integrated into a security incident response and reporting system	Audit reports that assess and measure the performance of the ISMS and its processes. Can be performed by an internal or external audit team.	ISO 27001[16]
WP6	Recommendations for improving the ISMS	Part of normal ISMS monitoring and reporting. Assessors should look for or ask for this.	List of recommended actions for improving the IS processes based on the ISMS performance assessment.	ISO 27001[16]

Appendix L – Typical Communication Plan Template

The typical Communication Plan should contain:

Communication Plan: Project / Process Title

Summary: A brief description of the project or business process.

Goals: A description of the goals that are expected to be achieved with the communication plan

Person	**Business Role**	**Frequency of communication**	**Format / Channel of communication**	**Additional information**

…	…	…	…	…

Communication Types: Detail the communication events present on the plan. The plan should contain information of where the communication event occurs, how often it occurs, who is involved and what deliverables must be presented at the time of the event.