COBIT 2019

- Vsebina in slike v tem gradivu so povzete po knjigi COBIT 2019: *Framework Introduction*

1

I. Obvladovanje podjetja in IT [11]

In the light of digital transformation, information and technology (I&T) have become crucial in the support, sustainability and growth of enterprises. Previously, governing boards (boards of directors) and senior management could delegate, ignore or avoid I&T-related decisions. In most sectors and industries, such attitudes are now ill-advised. Stakeholder value creation (i.e., realizing benefits at an optimal resource cost while optimizing risk) is often driven by a high degree of digitization in new business models, efficient processes, successful innovation, etc. Digitized enterprises are increasingly dependent on I&T for survival and growth.

Given the centrality of I&T for enterprise risk management and value generation, a specific focus on enterprise governance of information and technology (EGIT) has arisen over the last three decades. EGIT is an integral part of corporate governance. It is exercised by the board that oversees the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from I&T-enabled business investments (**figure 1.1**).

Figure 1.1—The Context of Enterprise Governance of Information and Technology

Source: De Haes, Steven; W. Van Grembergen; *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*, 2nd ed., Springer International Publishing, Switzerland, 2015, *https://www.springer.com/us/book/9783319145464*

Enterprise governance of information and technology is complex and multifaceted. There is no silver bullet (or ideal way) to design, implement and maintain effective EGIT within an organization. As such, members of the governing boards and senior management typically need to tailor their EGIT measures and implementation to their own specific context and needs. They must also be willing to accept more accountability for I&T and drive a different mindset and culture for delivering value from I&T.

2

Razmejitev med obvladovanjem (*Governance*) in vodenjem (*Management*) [13]

COBIT is a framework for the governance and management of enterprise information and technology,[4] aimed at the whole enterprise. Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limited to the IT department of an organization, but certainly includes it.

The COBIT framework makes a clear distinction between governance and management. These two disciplines encompass different activities, require different organizational structures and serve different purposes.

- **Governance** ensures that:
  - Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives.
  - Direction is set through prioritization and decision making.
  - Performance and compliance are monitored against agreed-on direction and objectives.

In most enterprises, overall governance is the responsibility of the board of directors, under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

- **Management** plans, builds, runs and monitors activities, in alignment with the direction set by the governance body, to achieve the enterprise objectives.

In most enterprises, management is the responsibility of the executive management, under the leadership of the chief executive officer (CEO).

COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure.[5]

COBIT defines the design factors that should be considered by the enterprise to build a best-fit governance system.

COBIT addresses governance issues by grouping relevant governance components into governance and management objectives that can be managed to the required capability levels.

3

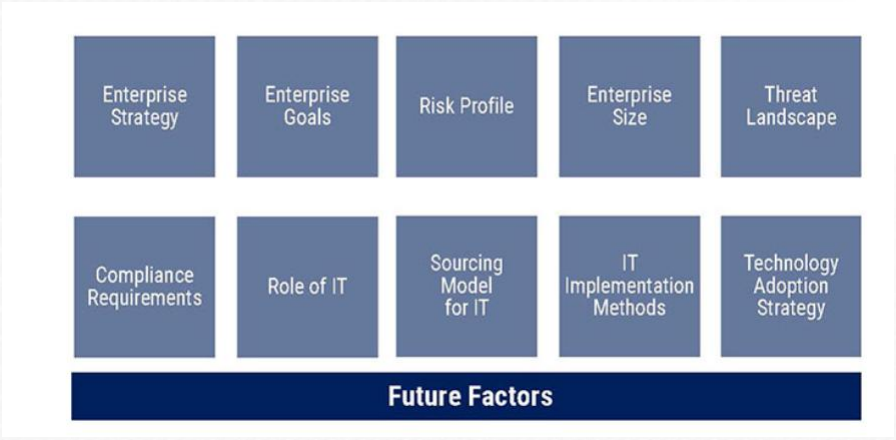
Deležniki obvladovanja [15]

Figure 2.1—COBIT Stakeholders

Stakeholder	Benefit of COBIT
Internal Stakeholders	
Boards	Provides insights on how to get value from the use of I&T and explains relevant board responsibilities
Executive Management	Provides guidance on how to organize and monitor performance of I&T across the enterprise
Business Managers	Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for new strategic opportunities
IT Managers	Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.
Assurance Providers	Helps to manage dependency on external service providers, get assurance over IT, and ensure the existence of an effective and efficient system of internal controls
Risk Management	Helps to ensure the identification and management of all IT-related risk
External Stakeholders	
Regulators	Helps to ensure the enterprise is compliant with applicable rules and regulations and has the right governance system in place to manage and sustain compliance
Business Partners	Helps to ensure that a business partner's operations are secure, reliable and compliant with applicable rules and regulations
IT Vendors	Helps to ensure that an IT vendor's operations are secure, reliable and compliant with applicable rules and regulations

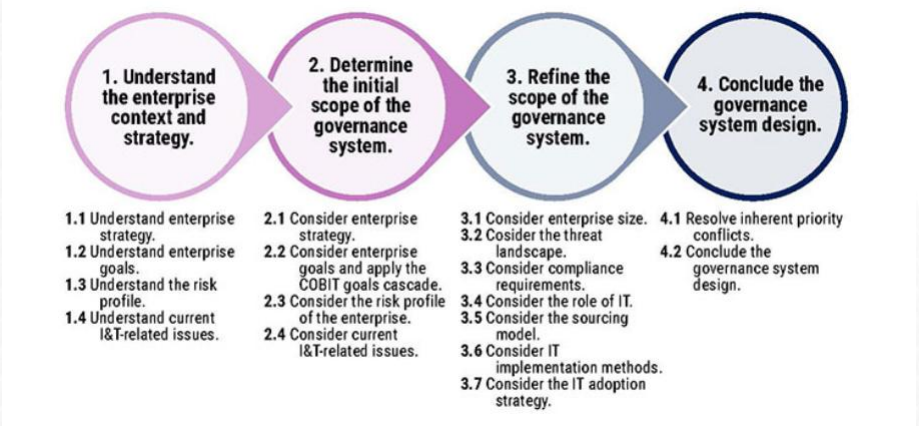
4

Elementi vpliva na sistem obvladovanja



5

Tok načrtovanja sistema obvladovanja



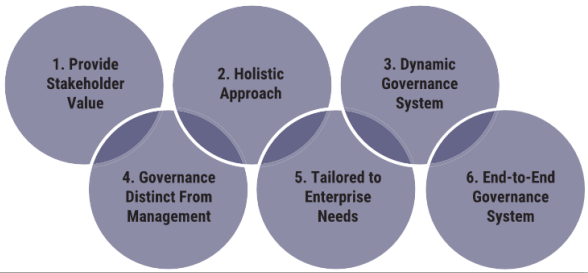
6

6 principov sistema obvladovanja [17]

The six principles for a governance system are (**figure 3.1**):

1. Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.
2. A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.
3. A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.
4. A governance system should clearly distinguish between governance and management activities and structures.
5. A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.
6. A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless where the processing is located in the enterprise.[6]

Figure 3.1—Governance System Principles



7

Domene COBIT 4.1 in domene COBIT 2019

- PO – Plan and Organise
- AI – Acquire and Implement
- DS – Deliver and Support
- ME – Monitor and Evaluate

- EDM – Evaluate, Direct and Monitor
- APO – Align, Plan and Organise
- BAI – Build, Acquire and Implement
- DSS - Deliver, Service and Support
- MEA – Monitor, Evaluate and Assess

8

Opredelitev obvladovanja in vodenja preko ciljev [20, 21]

4.2 Governance and Management Objectives

For information and technology to contribute to enterprise goals, a number of governance and management objectives should be achieved. Basic concepts relating to governance and management objectives are:

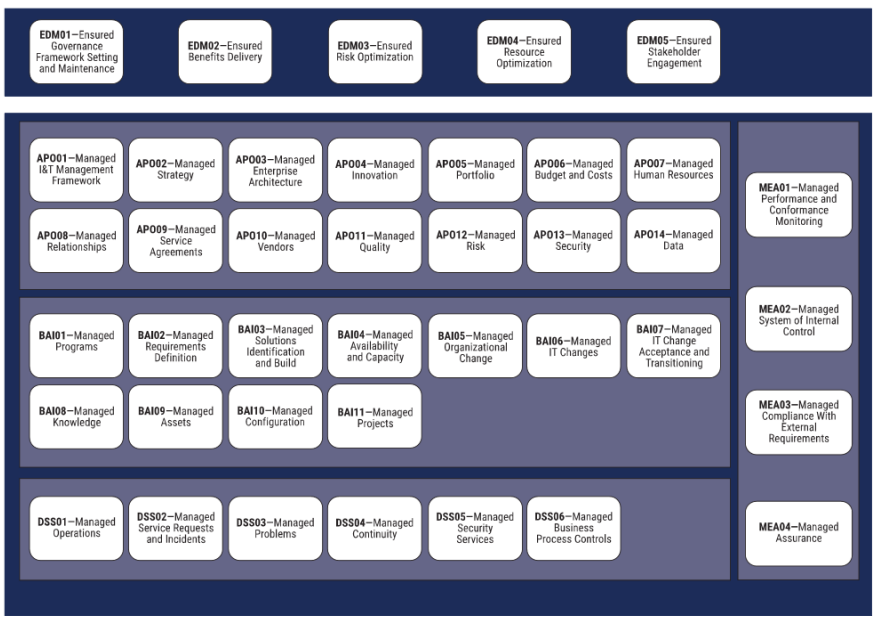
- A governance or management objective **always relates to one process** (with an identical or similar name) and a series of related components of other types to help achieve the objective.
- A governance objective relates to a governance process (depicted in the dark blue background in **figure 4.2**), while a management objective relates to a management process (depicted on the lighter blue background in **figure 4.2**). Boards and executive management are typically accountable for governance processes, while management processes are the domain of senior and middle management.

The governance and management objectives in COBIT are grouped into five domains. The domains have names with verbs that express the key purpose and areas of activity of the objective contained in them:

- Governance objectives are grouped in the **Evaluate, Direct and Monitor** (EDM) domain. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.
- Management objectives are grouped in four domains:
  - **Align, Plan and Organize** (APO) addresses the overall organization, strategy and supporting activities for I&T.
  - **Build, Acquire and Implement** (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.
  - **Deliver, Service and Support** (DSS) addresses the operational delivery and support of I&T services, including security.
  - **Monitor, Evaluate and Assess** (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

9

Figure 4.2—COBIT Core Model



10

10

Komponente sistema obvladovanja [21, 22]

4.3 Components of the Governance System

To satisfy governance and management objectives, each enterprise needs to establish, tailor and sustain a governance system built from a number of components.

- Components are factors that, individually and collectively, contribute to the good operations of the enterprise's governance system over I&T.
- Components interact with each other, resulting in a holistic governance system for I&T.
- Components can be of different types. The most familiar are processes. However, components of a governance system also include organizational structures; policies and procedures; information items; culture and behavior; skills and competencies; and services, infrastructure and applications (**figure 4.3**).
  - **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs that support achievement of overall IT-related goals.
  - **Organizational structures** are the key decision-making entities in an enterprise.
  - **Principles, policies and frameworks** translate desired behavior into practical guidance for day-to-day management.
  - **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. COBIT focuses on information required for the effective functioning of the governance system of the enterprise.

11

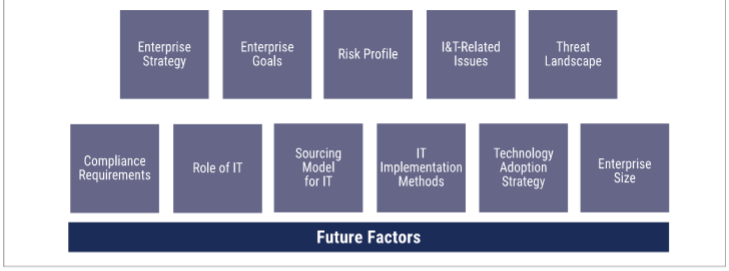
- **Culture, ethics and behavior** of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.
- **People, skills and competencies** are required for good decisions, execution of corrective action and successful completion of all activities.
- **Services, infrastructure and applications** include the infrastructure, technology and applications that provide the enterprise with the governance system for I&T processing.

Figure 4.3—COBIT Components of a Governance System

12

Faktorji vpliva na sistem obvladovanja [23-27]

Figure 4.4—COBIT Design Factors



1. **Enterprise strategy**—Enterprises can have different strategies, which can be expressed as one or more of the archetypes shown in **figure 4.5**. Organizations typically have a primary strategy and, at most, one secondary strategy.

Figure 4.5—Enterprise Strategy Design Factor

Strategy Archetype	Explanation
Growth/Acquisition	The enterprise has a focus on growing (revenues).[10]
Innovation/Differentiation	The enterprise has a focus on offering different and/or innovative products and services to their clients.[11]
Cost Leadership	The enterprise has a focus on short-term cost minimization.[12]
Client Service/Stability	The enterprise has a focus on providing stable and client-oriented service.[13]

13

2. **Enterprise goals** supporting the enterprise strategy—Enterprise strategy is realized by the achievement of (a set of) enterprise goals. These goals are defined in the COBIT framework, structured along the balanced scorecard (BSC) dimensions, and include the elements shown in **figure 4.6.**

Figure 4.6—Enterprise Goals Design Factor

Reference	Balanced Scorecard (BSC) Dimension	Enterprise Goal
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business-service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

14

3. **Risk profile** of the enterprise and current issues in relation to I&T—The risk profile identifies the sort of I&T-related risk to which the enterprise is currently exposed and indicates which areas of risk are exceeding the risk appetite. The risk categories[14] listed in **figure 4.7** merit consideration.

Figure 4.7—Risk Profile Design Factor (IT Risk Categories)

Reference	Risk Category
1	IT investment decision making, portfolio definition and maintenance
2	Program and projects lifecycle management
3	IT cost and oversight
4	IT expertise, skills and behavior
5	Enterprise/IT architecture
6	IT operational infrastructure incidents
7	Unauthorized actions
8	Software adoption/usage problems
9	Hardware incidents
10	Software failures
11	Logical attacks (hacking, malware, etc.)
12	Third party/supplier incidents
13	Noncompliance
14	Geopolitical issues
15	Industrial action
16	Acts of nature
17	Technology-based innovation
18	Environmental

15

4. **I&T-related issues**—A related method for an I&T risk assessment for the enterprise is to consider which I&T-related issues it currently faces, or, in other words, what I&T-related risk has materialized. The most common of such issues[15] include those in **figure 4.8**.

Figure 4.8—I&T-Related Issues Design Factor

Reference	Description
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value
C	Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT-related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
G	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives, or other forms of wasted resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
K	Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT
L	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions
M	Excessively high cost of IT
N	Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems
O	Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages
P	Regular issues with data quality and integration of data across various sources
Q	High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation
R	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department[16]
S	Ignorance of and/or noncompliance with privacy regulations
T	Inability to exploit new technologies or innovate using I&T

16

5. **Threat landscape**—The threat landscape under which the enterprise operates can be classified as shown in **figure 4.9**.

Figure 4.9—Threat Landscape Design Factor

Threat Landscape	Explanation
Normal	The enterprise is operating under what are considered normal threat levels.
High	Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment.

17

6. **Compliance requirements**—The compliance requirements to which the enterprise is subject can be classified according to the categories listed in **figure 4.10**.

Figure 4.10—Compliance Requirements Design Factor

Regulatory Environment	Explanation
Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.
Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements that are common across different industries.
High compliance requirements	The enterprise is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions.

7. **Role of IT**—The role of IT for the enterprise can be classified as indicated in **figure 4.11**.

Figure 4.11—Role of IT Design Factor

Role of IT[7]	Explanation
Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.
Factory	When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.
Turnaround	IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency on IT for the current running and continuity of the business processes and services.
Strategic	IT is critical for both running and innovating the organization's business processes and services.

8. **Sourcing model for IT**—The sourcing model the enterprise adopts can be classified as shown in **figure 4.12**.

Figure 4.12—Sourcing Model for IT Design Factor

Sourcing Model	Explanation
Outsourcing	The enterprise calls upon the services of a third party to provide IT services.
Cloud	The enterprise maximizes the use of the cloud for providing IT services to its users.
Insourced	The enterprise provides for its own IT staff and services.
Hybrid	A mixed model is applied, combining the other three models in varying degrees.

18

9. **IT implementation methods**—The methods the enterprise adopts can be classified as noted in **figure 4.13**.

Figure 4.13—IT Implementation Methods Design Factor

IT Implementation Method	Explanation
Agile	The enterprise uses Agile development working methods for its software development.
DevOps	The enterprise uses DevOps working methods for software building, deployment and operations.
Traditional	The enterprise uses a more classic approach to software development (waterfall) and separates software development from operations.
Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as "bimodal IT."

10. **Technology adoption strategy**—The technology adoption strategy can be classified as listed in **figure 4.14**.

Figure 4.14—Technology Adoption Strategy Design Factor

Technology Adoption Strategy	Explanation
First mover	The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage.
Follower	The enterprise typically waits for new technologies to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with adoption of new technologies.

11. **Enterprise size**—Two categories, as shown in **figure 4.15**, are identified for the design of an enterprise's governance system.[18]

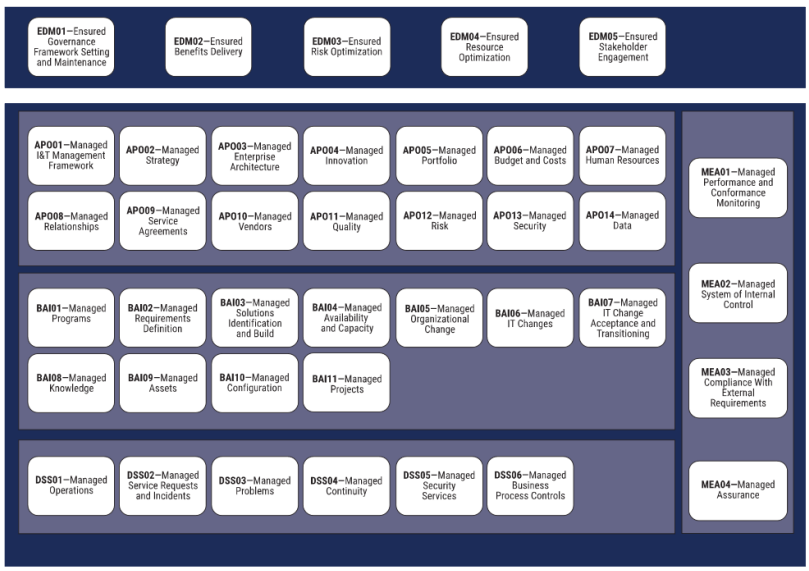
Figure 4.15—Enterprise Size Design Factor

Enterprise Size	Explanation
Large enterprise (Default)	Enterprise with more than 250 full-time employees (FTEs)
Small and medium enterprise	Enterprise with 50 to 250 FTEs

19

Cilji obvladovanja in vodenja [21, 33-35]

Figure 4.2—COBIT Core Model



20

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose

Reference	Name	Purpose
EDM01	Ensured governance framework setting and maintenance	Provide a consistent approach, integrated and aligned with the enterprise governance approach. I&T-related decisions must be made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
EDM02	Ensured benefits delivery	Secure optimal value from I&T-enabled initiatives, services and assets; cost-effective delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03	Ensured risk optimization	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.
EDM04	Ensured resource optimization	Ensure that the resource needs of the enterprise are met in the optimal manner, I&T costs are optimized, and there is an increased likelihood of benefit realization and readiness for future change.
EDM05	Ensured stakeholder engagement	Ensure that stakeholders are supportive of the I&T strategy and road map, communication to stakeholders is effective and timely, and the basis for reporting is established to increase performance. Identify areas for improvement, and confirm that I&T-related objectives and strategies are in line with the enterprise's strategy.
APO01	Managed I&T management framework	Implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes; organizational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behavior; and services, infrastructure and applications.
APO02	Managed strategy	Support the digital transformation strategy of the organization and deliver the desired value through a road map of incremental changes. Use a holistic I&T approach, ensuring that each initiative is clearly connected to an overarching strategy. Enable change in all different aspects of the organization, from channels and processes to data, culture, skills, operating model and incentives.
APO03	Managed enterprise architecture	Represent the different building blocks that make up the enterprise and its interrelationships, as well as the principles guiding their design and evolution over time, to enable a standard, responsive and efficient delivery of operational and strategic objectives.
APO04	Managed innovation	Achieve competitive advantage, business innovation, improved customer experience, and improved operational effectiveness and efficiency by exploiting I&T developments and emerging technologies.

21

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose *(cont.)*

Reference	Name	Purpose
APO05	Managed portfolio	Optimize the performance of the overall portfolio of programs in response to individual program, product and service performance and changing enterprise priorities and demand.
APO06	Managed budget and costs	Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of I&T-related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of I&T solutions and services.
APO07	Managed human resources	Optimize human-resources capabilities to meet enterprise objectives.
APO08	Managed relationships	Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.
APO09	Managed service agreements	Ensure that I&T products, services and service levels meet current and future enterprise needs.
APO10	Managed vendors	Optimize available I&T capabilities to support the I&T strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.
APO11	Managed quality	Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.
APO12	Managed risk	Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.
APO13	Managed security	Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.
APO14	Managed data	Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.
BAI01	Managed programs	Realize desired business value and reduce the risk of unexpected delays, costs and value erosion. To do so, improve communications to and involvement of business and end users, ensure the value and quality of program deliverables and follow-up of projects within the programs, and maximize program contribution to the investment portfolio.
BAI02	Managed requirements definition	Create optimal solutions that meet enterprise needs while minimizing risk.
BAI03	Managed solutions identification and build	Ensure agile and scalable delivery of digital products and services. Establish timely and cost-effective solutions (technology, business processes and workflows) capable of supporting enterprise strategic and operational objectives.
BAI04	Managed availability and capacity	Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.
BAI05	Managed organizational change	Prepare and commit stakeholders for business change and reduce the risk of failure.
BAI06	Managed IT changes	Enable fast and reliable delivery of change to the business. Mitigate the risk of negatively impacting the stability or integrity of the changed environment.
BAI07	Managed IT change acceptance and transitioning	Implement solutions safely and in line with the agreed expectations and outcomes.

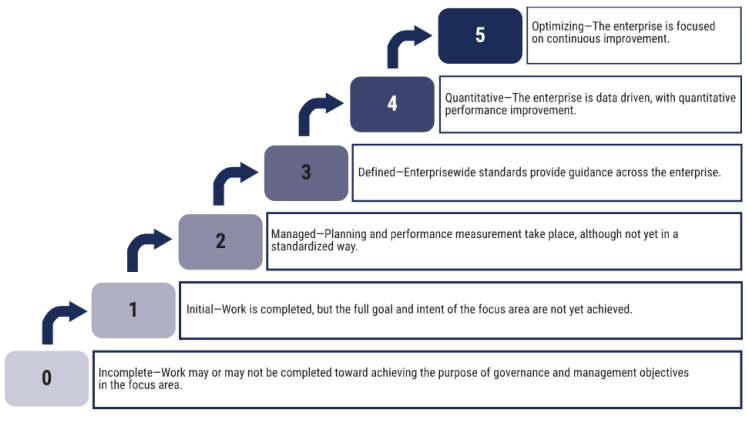
22

Figure 5.1—COBIT Core Model: Governance and Management Objectives and Purpose *(cont.)*

Reference	Name	Purpose
BAI08	Managed knowledge	Provide the knowledge and management information required to support all staff in the governance and management of enterprise I&T and allow for informed decision making.
BAI09	Managed assets	Account for all I&T assets and optimize the value provided by their use.
BAI10	Managed configuration	Provide sufficient information about service assets to enable the service to be effectively managed. Assess the impact of changes and deal with service incidents.
BAI11	Managed projects	Realize defined project outcomes and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users. Ensure the value and quality of project deliverables and maximize their contribution to the defined programs and investment portfolio.
DSS01	Managed operations	Deliver I&T operational product and service outcomes as planned.
DSS02	Managed service requests and incidents	Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Assess the impact of changes and deal with service incidents. Resolve user requests and restore service in response to incidents.
DSS03	Managed problems	Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems, and identify root causes as part of problem resolution.
DSS04	Managed continuity	Adapt rapidly, continue business operations, and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).
DSS05	Managed security services	Minimize the business impact of operational information security vulnerabilities and incidents.
DSS06	Managed business process controls	Maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation.
MEA01	Managed performance and conformance monitoring	Provide transparency of performance and conformance and drive achievement of goals.
MEA02	Managed system of internal control	Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.
MEA03	Managed compliance with external requirements	Ensure that the enterprise is compliant with all applicable external requirements.
MEA04	Managed assurance	Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.

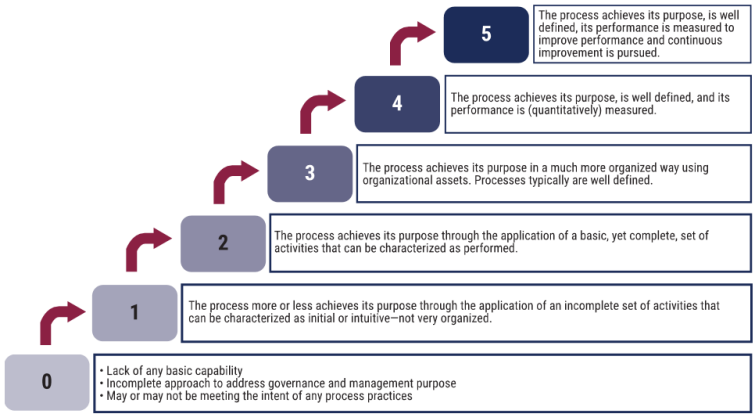
Zrelostni model [40]

Figure 6.3—Maturity Levels for Focus Areas



Poleg zrelostnega modela tudi zmožnostni model [39]

Figure 6.2—Capability Levels for Processes



25

6.4.2 Rating Process Activities

A capability level can be achieved to varying degrees, which can be expressed by a set of ratings. The range of available ratings depends on the context in which the performance assessment is made:

- Some formal methods leading to independent certification use a binary pass/fail set of ratings.
- Less formal methods (often used in performance-improvement contexts) work better with a larger range of ratings, such as the following set:
  - *Fully*—The capability level is achieved for more than 85 percent. (This remains a judgment call, but it can be substantiated by the examination or assessment of the components of the enabler, such as process activities, process goals or organizational structure good practices.)
  - *Largely*—The capability level is achieved between 50 percent and 85 percent.
  - *Partially*—The capability level is achieved between 15 percent and 50 percent.
  - *Not*—The capability level is achieved less than 15 percent.

26

Način opisa ciljev (procesov) v COBIT 2019

- Opis po komponentah sistema obvladovanja

Figure 4.3—COBIT Components of a Governance System

Domain: Align, Plan and Organize Management Objective: APO02 — Managed Strategy	Focus Area: COBIT Core Model
Description	
Provide a holistic view of the current business and I&T environment, the future direction, and the initiatives required to migrate to the desired future environment. Ensure that the desired level of digitization is integral to the future direction and the I&T strategy. Assess the organization's current digital maturity and develop a road map to close the gaps. With the business, rethink internal operations as well as customer-facing activities. Ensure focus on the transformation journey across the organization. Leverage enterprise architecture building blocks, governance components and the organization's ecosystem, including externally provided services and related capabilities, to enable reliable but agile and efficient response to strategic objectives.	
Purpose	
Support the digital transformation strategy of the organization and deliver the desired value through a road map of incremental changes. Use a holistic I&T approach, ensuring that each initiative is clearly connected to an overarching strategy. Enable change in all different aspects of the organization, from channels and processes to data, culture, skills, operating model and incentives.	
The management objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG01 Portfolio of competitive products and services • EG05 Customer-oriented service culture • EG08 Optimization of internal business process functionality • EG12 Managed digital transformation programs	AG08 Enabling and supporting business processes by integrating applications and technology
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG01 a. Percent of products and services that meet or exceed targets in revenues and/or market share b. Percent of products and services that meet or exceed customer satisfaction targets c. Percent of products and services that provide competitive advantage d. Time to market for new products and services	AG08 a. Time to execute business services or processes b. Number of I&T-enabled business programs delayed or incurring additional cost due to technology-integration issues c. Number of business process changes that need to be delayed or reworked because of technology-integration issues d. Number of applications or critical infrastructures operating in silos and not integrated
EG05 a. Number of customer service disruptions b. Percent of business stakeholders satisfied that customer service delivery meets agreed levels c. Number of customer complaints d. Trend of customer satisfaction survey results	
EG08 a. Satisfaction levels of board and executive management with business process capabilities b. Satisfaction levels of customers with service delivery capabilities c. Satisfaction levels of suppliers with supply chain capabilities	
EG12 a. Number of programs on time and within budget b. Percent of stakeholders satisfied with program delivery c. Percent of business transformation programs stopped d. Percent of business transformation programs with regular reported status updates	

A. Component: Process	
Management Practice	**Example Metrics**
APO02.01 Understand enterprise context and direction. Understand the enterprise context (industry drivers, relevant regulations, basis for competition), its current way of working and its ambition level in terms of digitization.	a. Level of understanding within I&T management of current enterprise organization and context b. Level of knowledge within I&T management of enterprise goals and direction c. Level of understanding of key stakeholders for I&T and their detailed requirements

Activities	Capability Level
1. Develop and maintain an understanding of the external environment of the enterprise.	2
2. Develop and maintain an understanding of the current way of working, including the operational environment, enterprise architecture (business, information, data, applications and technology domains), enterprise culture and current challenges.	
3. Develop and maintain an understanding of future enterprise direction, including enterprise strategy, goals and objectives. Understand the ambition level of the enterprise in terms of digitization, which may include a range of increasingly aspirational goals, from cutting costs, increasing customer centricity, or getting to market faster by digitizing internal operations, to creating entirely new revenue streams from new business models (e.g., platform business).	
4. Identify key stakeholders and obtain insight on their requirements.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 6

Management Practice	Example Metrics
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise. Assess the performance of current I&T services and develop an understanding of current business and I&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	a. Percent of staff satisfied with current capabilities b. Percent of business owner satisfaction with investment in and utilization of the internal and external asset base to meet critical success factors

29

Activities	Capability Level
1. Develop a baseline of current business and I&T capabilities and services. Include assessment of externally provisioned services, governance of I&T, and enterprisewide I&T-related skills and competencies.	2
2. Assess digital maturity across different dimensions (e.g., ability of leadership to leverage technology, level of accepted technology risk, approach to innovation, culture and knowledge level of users). Assess appetite for change.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 6; 9. Review and Revision—Principle 15

Management Practice	Example Metrics
APO02.03 Define target digital capabilities. Based on the understanding of enterprise context and direction, define the target I&T products and services and required capabilities. Consider reference standards, best practices and validated emerging technologies.	a. Percent of enterprise objectives addressed by the I&T goals/objectives b. Percent of I&T objectives that support the enterprise strategy

Activities	Capability Level
1. Summarize enterprise context and direction and identify specific I&T aspects of enterprise strategy (e.g., digitizing processes, implementing new technology, supporting legacy architecture, applying new digital business models, developing digital product portfolio, etc.).	2
2. Define high-level I&T objectives and goals and specify their contribution to enterprise objectives.	
3. Detail required I&T services and products to realize enterprise objectives. Consider validated emerging technology or innovation ideas, reference standards, competitor business and I&T capabilities, comparative benchmarks of good practice, and emerging I&T service provision.	3
4. Determine I&T capabilities, methodologies and organizational approaches required to realize the defined I&T product and service portfolio. Consider different development methodologies (Agile, scrum, waterfall, bimodal IT), depending on business requirements. Consider how each could help realize I&T objectives.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

30

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO02.04 Conduct a gap analysis. Identify gaps between current and target environments and describe the high-level changes in the enterprise architecture.	a. Number of high-impact changes required in the different enterprise architecture domains b. Number of significant gaps between current environment and good practices

Activities	Capability Level
1. Identify all gaps and changes required to realize the target environment.	3
2. Describe high-level changes in enterprise architecture (business, information, data, applications and technology domains).	
3. Consider the high-level implications of all gaps. Assess the impact of potential changes on business and I&T operating models, I&T research and development capabilities, and I&T investment programs.	
4. Consider the value of potential changes to business and IT capabilities, I&T services and enterprise architecture, and the implications if no changes are realized.	4
5. Refine the target environment definition and prepare a value statement outlining benefits of the target environment.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Metrics
APO02.05 Define the strategic plan and road map. Develop a holistic digital strategy, in cooperation with relevant stakeholders, and detail a road map that defines the incremental steps required to achieve the goals and objectives. Ensure focus on the transformation journey through the appointment of a person who helps spearhead the digital transformation and drives alignment between business and I&T.	a. Level of stakeholder support for the digital transformation plan b. Percent of initiatives in the I&T strategy that are self-funding (with financial benefits exceeding costs) c. Degree of correspondence between enterprise strategy and I&T strategy and objectives

Activities	Capability Level
1. Define initiatives required to close gaps between current and target environments. Integrate initiatives into a coherent I&T strategy that aligns I&T with all aspects of the business.	3
2. Detail a road map that defines the incremental steps required to achieve the goals and objectives of the I&T strategy. Ensure actions are included to train people with new skills, support adoption of new technology, sustain change throughout the organization, etc.	
3. Consider the external ecosystem (enterprise partners, suppliers, start-ups, etc.) to help support execution of the road map.	
4. Group actions into programs and/or projects with a clear goal or deliverable. For each project, identify high-level resource requirements, schedule, investment/operational budget, risk, change impact, etc.	
5. Determine dependencies, overlaps, synergies and impacts among projects, and prioritize.	
6. Finalize road map, indicating relative scheduling and interdependencies of projects.	
7. Ensure focus on the transformation journey. Appoint a champion of digital transformation and alignment between business and I&T (chief digital officer [CDO] or other traditional C-suite role).	
8. Obtain support and formal approval of plan from stakeholders.	
9. Translate objectives into measurable outcomes represented by metrics (what) and targets (how much). Ensure that outcomes and measures correlate to enterprise benefits.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SG2.1 Information Security Strategy
ITIL V3, 2011	Service Strategy, 4.1 Strategy management for IT services

31

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
APO02.06 Communicate the I&T strategy and direction. Create awareness and understanding of the business and I&T objectives and direction, as captured in the I&T strategy, through communication to appropriate stakeholders and users throughout the enterprise.	a. Frequency of updates to the I&T strategy communication plan b. Percent of stakeholders aware of I&T strategy and direction

Activities	Capability Level
1. Develop a communication plan covering the required messages, target audiences, communication mechanisms/channels and schedules.	3
2. Prepare a communication package that delivers the plan effectively, using available media and technologies.	
3. Develop and maintain a network for endorsing, supporting and driving the I&T strategy.	
4. Obtain feedback and update the communication plan and delivery as required.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

32

B. Component: Organizational Structures

Key Management Practice	Chief Executive Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	I&T Governance Board	Business Process Owners	Project Management Office	Data Management Function	Relationship Manager	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO02.01 Understand enterprise context and direction.		A	R	R				R	R	R	R	R	R	R	R	R	R
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise.		A	R	R				R		R	R	R	R	R	R	R	R
APO02.03 Define target digital capabilities.		R	R	A		R		R	R	R	R	R	R	R	R	R	R
APO02.04 Conduct a gap analysis.		R	R	R	A	R		R		R	R	R	R	R	R	R	R
APO02.05 Define the strategic plan and road map.		R	R	R	A	R	R	R		R	R	R	R	R	R	R	R
APO02.06 Communicate the I&T strategy and direction.	R	R	R	R	A												

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 38502:2017(E)	5.4 Responsibilities of managers

C. Component: Information Flows and Items (see also Section 3.6)

Management Practice	Inputs		Outputs	
APO02.01 Understand enterprise context and direction.	**From**	**Description**	**Description**	**To**
	APO04.02	Innovation opportunities linked to business drivers	Sources and priorities for change	Internal
	EDM04.01	Guiding principles for allocating resources and capabilities		
	Outside COBIT	Enterprise strategy and strengths, weaknesses, opportunities, threats (SWOT) analysis		

▪ 33

33

C. Component: Information Flows and Items (see also Section 3.6) (cont.)

Management Practice	Inputs		Outputs	
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise.	**From**	**Description**	**Description**	**To**
	APO06.05	Cost optimization opportunities	Gaps and risk related to current capabilities	APO12.01
	APO08.05	Definition of potential improvement projects	Capability SWOT analysis	Internal
	APO09.01	Identified gaps in IT services to the business	Baseline of current capabilities	Internal
	APO09.04	Improvement action plans and remediations		
	APO12.01	Emerging risk issues and factors		
	APO12.02	Risk analysis results		
	APO12.03	Aggregated risk profile, including status of risk management actions		
	APO12.05	Project proposals for reducing risk		
	BAI04.03	• Prioritized improvements • Performance and capacity plans		
	BAI04.05	Corrective actions		
	BAI09.01	Results of fit-for-purpose reviews		
	BAI09.04	• Results of cost optimization reviews • Opportunities to reduce asset costs or increase value		
	EDM04.03	Feedback on allocation and effectiveness of resources and capabilities		
APO02.03 Define target digital capabilities.	APO04.05	• Results and recommendations from proof-of-concept initiatives • Analysis of rejected initiatives	Proposed enterprise architecture changes	APO03.03
			Required business and IT capabilities	Internal
			High-level I&T-related goals	Internal
APO02.04 Conduct a gap analysis.	APO04.06	Assessments of using innovative approaches	Gaps and changes required to realize target capability	APO01.03; APO13.02; BAI03.11; EDM04.01
	APO05.01	Investment return expectations	Value benefit statement for target environment	BAI03.11
	BAI01.05	Results of program goal achievement monitoring		
	BAI01.06	Stage-gate review results		
	BAI11.09	Post-implementation review results		
	EDM02.02	Evaluation of strategic alignment		

Stran ▪ 34

34

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*

Management Practice	Inputs		Outputs	
	From	Description	Description	To
APO02.05 Define the strategic plan and road map.	APO03.01	• Defined scope of architecture • Architecture concept business case and value proposition	I&T strategy and objectives	All APO; All BAI; All DSS; All MEA
	APO03.02	Information architecture model	Strategic road map	APO01.01; APO03.01; APO08.01; EDM02.01; EDM02.02
	APO03.03	Transition architectures	Definition of strategic initiatives	EDM02.01
	APO05.01	Funding options	Risk assessment initiatives	EDM02.01, APO12.01
	APO06.02	Budget allocations		
	APO06.03	I&T budget		
	BAI09.05	Action plan to adjust license numbers and allocations		
	DSS04.02	Approved strategic options		
	EDM02.01	Feedback on strategy and goals		
	EDM04.01	Approved resources plan		
	EDM04.03	Remedial actions to address resource management deviations		
APO02.06 Communicate the I&T strategy and direction.	EDM04.02	Communication of resourcing strategies	Communication package	All APO; All BAI; All DSS; All MEA
			Communication plan	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Service strategy, 3.9 Service strategy inputs and outputs

D. Component: People, Skills and Competencies

Skill	Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
Business plan development	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Business Plan Development
Emerging technology monitoring	Skills Framework for the Information Age V6, 2015	EMRG
I&T strategy and planning	Skills Framework for the Information Age V6, 2015	ITSP
Strategy alignment	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.1. IS and Business Strategy Alignment

35

E. Component: Policies and Procedures

Relevant Policy	Policy Description	Related Guidance	Detailed Reference
I&T service strategy principles	For details, refer to related guidance.	ITIL V3, 2011	Service Strategy, 3. Service strategy principles
I&T strategy policy and principles	Provides holistic view of current business and I&T environment, strategic direction and initiatives required to transition to the desired future environment. Ensures that business and I&T strategy reflect target level of digitization.		

F. Component: Culture, Ethics and Behavior

Key Culture Elements	Related Guidance	Detailed Reference
Establish a culture and underlying values that fit the overall business strategy (i.e., customer oriented, innovation driven, product based). Find ways to inject speed into processes and introduce the supporting culture and behavior that allow moving at a faster pace. This could start with changing basic habits such as having more frequent strategy leadership meetings or automating certain activities. In the current context of digital business models, ecosystems and disruption, it is vital for many organizations to prioritize digital transformation in their strategy. Build a culture that challenges the status quo and explores new ways of working (e.g., invest in automation to respond rapidly to customers, develop sophisticated reporting and analytics to interpret customer needs, build innovative interfaces to gather customer data, create mechanisms to deliver content and offers across all relevant channels).	The Scaled Agile Framework for Lean Enterprises	Configurable framework that helps organizations deliver new products and solutions in the shortest sustainable lead time (all chapters)

G. Component: Services, Infrastructure and Applications

- Customer analytics
- Industry benchmarks
- Performance measurement system (e.g., balanced scorecard, skills management tools)
- Technology watch services and tools

36