



WHITE PAPER

# **IT VALUE CREATION**

in the (central) government



# Abstract

IT governance in the public sector is critical for ensuring that information technology investments align with governmental objectives, deliver value to citizens, and meet accountability and compliance requirements.

## Problem

Differences between the public and private sector, such as complex interdependencies, process intricacies, and the fact that not all government goals are financial, pose challenges in defining IT value and governing holistic value creation within government. There is strong interest among public-sector IT leaders in establishing clear guidelines for value-driven IT governance.

## Purpose

This white paper focuses on how IT contributes to public value. It aims to clarify the concept of IT value creation in the public sector, present relevant scientific findings on the governance challenges involved, and offer guidelines to address these challenges.

## Advice

The [central] government increasingly relies on IT to create social value, but quantifying this value remains a significant challenge. Unlike the private sector's focus on financial metrics, government IT value assessment is complex and lacks easily quantifiable measures. Case studies and research confirm this difficulty. While frameworks like COBIT (ISACA. (2018). COBIT 2019 Framework – Governance and Management Objectives) offer helpful guidance, adapting them to the unique context of [central] government is crucial for effective value measurement.

## Conclusions

To maximize IT value in central government, adopt a three-pronged approach: (1) conduct thorough benefit, cost, and risk analyses to inform budget allocation; (2) establish clear, measurable outcomes using comprehensive documentation (vision statements, plans, business cases); and (3) foster continuous stakeholder engagement through regular communication and collaborative sessions.

## Limitations

Additional research is needed to refine and expand the current guidelines, making this a high-priority area for future public-sector IT governance efforts.



<b>Introduction.....</b>	<b>4</b>
<b>Problem Statement and Purpose .....</b>	<b>5</b>
<b>Theoretical Background– IT Value in COBIT .....</b>	<b>6</b>
Enterprise Governance of Information and Technology	
IT Value	
Differences between Public and Private Sectors	
Public Sector Challenges	
<b>Research Approach and Result .....</b>	<b>13</b>
Round Table Session – Integrating IT Governance for a Secure Future	
Case – Context and Life Cycles for Value Creation in the Dutch Government	
Case – Good Practices Implementing IT Governance in the Belgian Government	
<b>Discussion and Guidelines .....</b>	<b>24</b>
Guidelines	
Suitability of COBIT and Other Frameworks	
<b>Conclusion .....</b>	<b>29</b>
<b>Acknowledgments .....</b>	<b>30</b>
Research Sponsors	
Development Team	
Expert Reviewers	
<b>References .....</b>	<b>31</b>

# Introduction

As the central government grows increasingly reliant on IT (Osunji, 2021; Rekenkamer, 2025), it becomes critical to maximize its benefits through efficient resource allocation and effective risk management — a process referred to as IT value creation. Therefore IT governance in the public sector is essential. This white paper explores this dynamic and highlights how it can enhance IT governance within central government institutions.

IT governance in the public sector ensures that technology investments align with governmental objectives, deliver value to citizens, and meet accountability and compliance requirements. With regulatory frameworks such as NIS2, GDPR, and broader cybersecurity mandates becoming increasingly critical (EU, 2018; 2025), IT governance provides a structured framework for decision-making, planning, implementation, and oversight. It ensures that IT resources are used effectively, responsibly, and in alignment with public sector priorities.

Research finding indicates that public sector organizations often demonstrate limited understanding of IT governance principles (Al Qassimi, 2015). This underscores the need to strengthen the processes, structures, and relational mechanisms that support accountability and contribute to the effective implementation of IT governance across government initiatives.

Implementing IT governance in central government is inherently complex. This complexity stems from a politically sensitive and highly dynamic environment with significant societal impact (Rusu & Viscusi, 2017, p. 8; Morool, 2014, p. 9; Liu & Ridley, 2005), as well as outdated and

fragmented technological infrastructures (Algemene Rekenkamer, 2007, p. 7; Beijert & Koedijk, 2016; Aussems, 2025). Moreover, governments often undertake large-scale, high-risk IT projects that face a heightened risk of failure (Nawi et al., 2014, p. 69).

Despite these challenges, the societal imperative for governments to extract greater value from IT — in the form of improved public service delivery, operational efficiency, and enhanced stakeholder trust — remains strong. IT value creation is an actively debated topic and is defined in COBIT as achieving a balance between benefits, resources, and risks. However, in public sector settings, this definition is often difficult to interpret and apply, which impedes the widespread adoption of IT value creation as a practical governance tool.

In this white paper, we explore how IT governance can drive value creation in the complex IT landscapes of the Dutch and Belgian governments. The document is structured as follows: Section 2 outlines the problem definition related to IT governance in government. Section 3 provides definitions of IT value and IT governance, along with the key characteristics of the public sector. Section 4 presents practical insights based on a roundtable discussion and two detailed case studies. Section 5 synthesizes theoretical and practical findings into actionable guidelines. Finally, Section 6 offers concluding remarks.

# Problem Statement and Purpose

This white paper explores the concept of IT value within governments and the governance of integrated value creation, taking into account the unique challenges and issues faced by the public sector in contrast to the private sector.

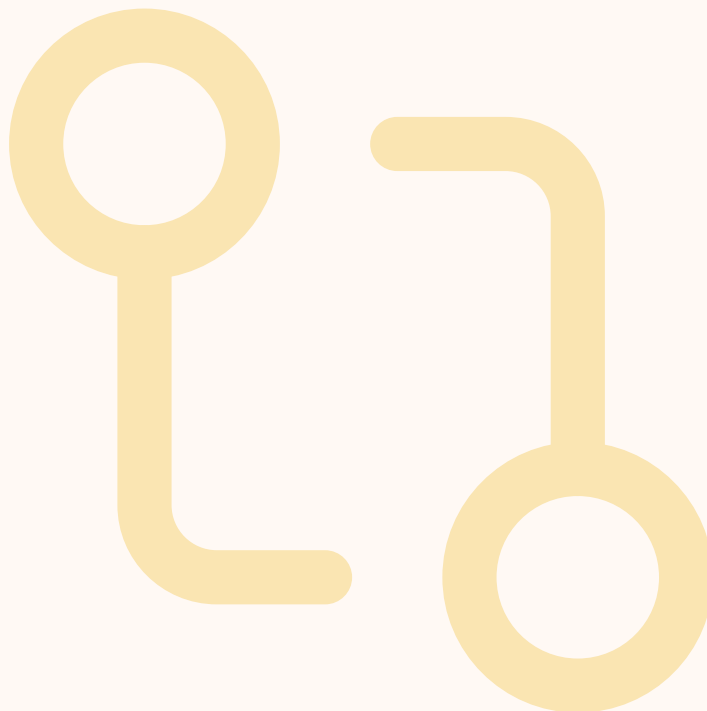
The problem lies in the ambiguity surrounding the definition and governance of IT value creation within government organizations.

While value in the private sector can ultimately be quantified financially, public sector value is multifaceted and often not primarily driven by financial considerations [Dawson et al., 2017, p. 1184].

As defined by Talbot, (2011, p. 30) public value involves meeting self-interest, public or social interest, and procedural interest. Public or social interest can be further understood as focusing on societal benefits and enhancing quality of life. In this context, value creation refers to aligning government actions, resources, and policies with citizens' needs and

expectations, promoting social welfare, and achieving public policy goals, including aspects such as greater efficiency (e.g., lower taxes) and improved accountability.

This white paper addresses the question of how to define IT value in the public sector, and how to enhance the monitoring and control of IT value creation to support effective IT governance. We propose recommendations to address this and discuss how value creation from a COBIT perspective can support compliance with regulatory requirements such as GDPR, NIS2, and other frameworks (EU, 2025 ; EU, 2018).



# Theoretical Background – IT Value in COBIT

Information technology (IT) is essential for both public and private organizations, driving innovation and efficiency. However, the management of IT value varies significantly between sectors, with the public sector focusing on public service outcomes and regulatory compliance, while the private sector emphasizes profit and market competitiveness. This chapter explores IT governance through COBIT, examining enterprise governance, IT value, sector-specific challenges, and the unique difficulties faced by the public sector in aligning IT investments with strategic goals.

## Enterprise Governance of Information and Technology

### 3.1

The COBIT framework makes a clear distinction between governance and management.

Governance encompasses the activities and responsibilities undertaken by the governing body to evaluate stakeholders' needs, conditions, and options to establish balanced and mutually agreed objectives.

It provides direction through prioritization and decision-making while monitoring performance and compliance with the established objectives and directives.

Management plans, builds, operates, and monitors activities to achieve enterprise objectives aligned with the direction set by the governing body.

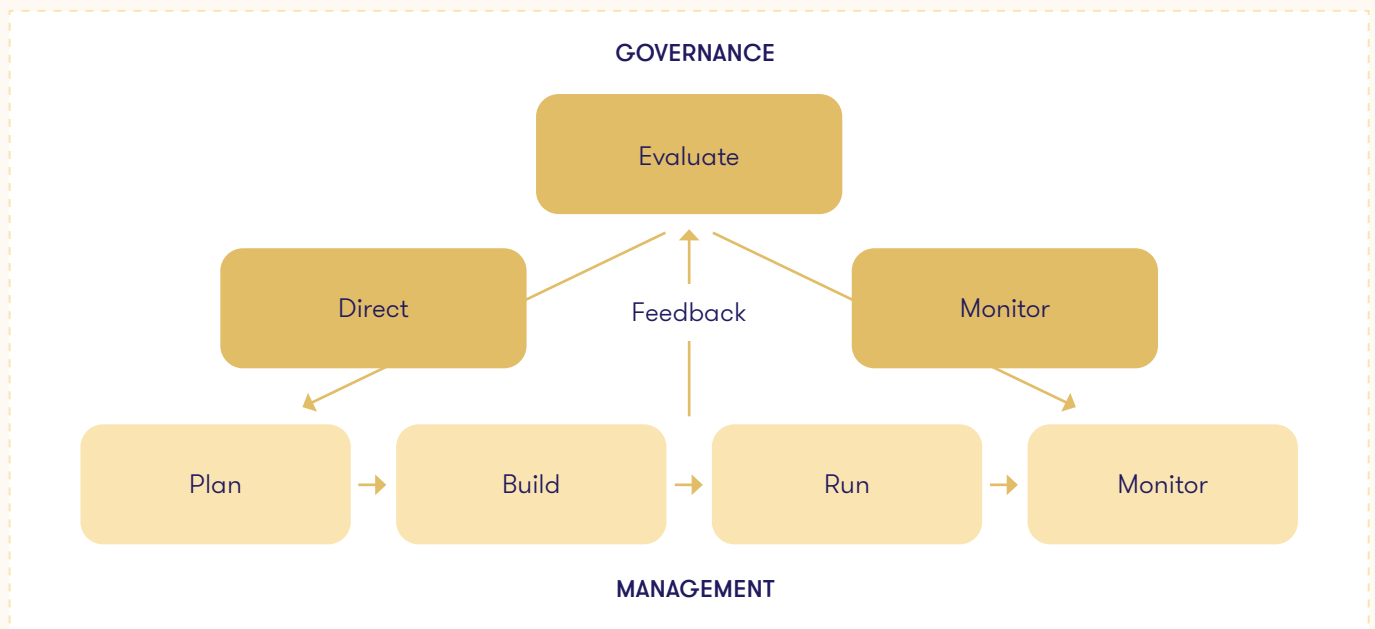


Figure 1: The COBIT distinction between governance and management (ISACA, 2018)

The governance and management objectives for Enterprise Governance of Information and Technology (EGIT) stem from the needs and drivers of stakeholders

as identified in the goal cascade. This goal cascade enables the translation of enterprise objectives into prioritized alignments (ISACA, 2018).

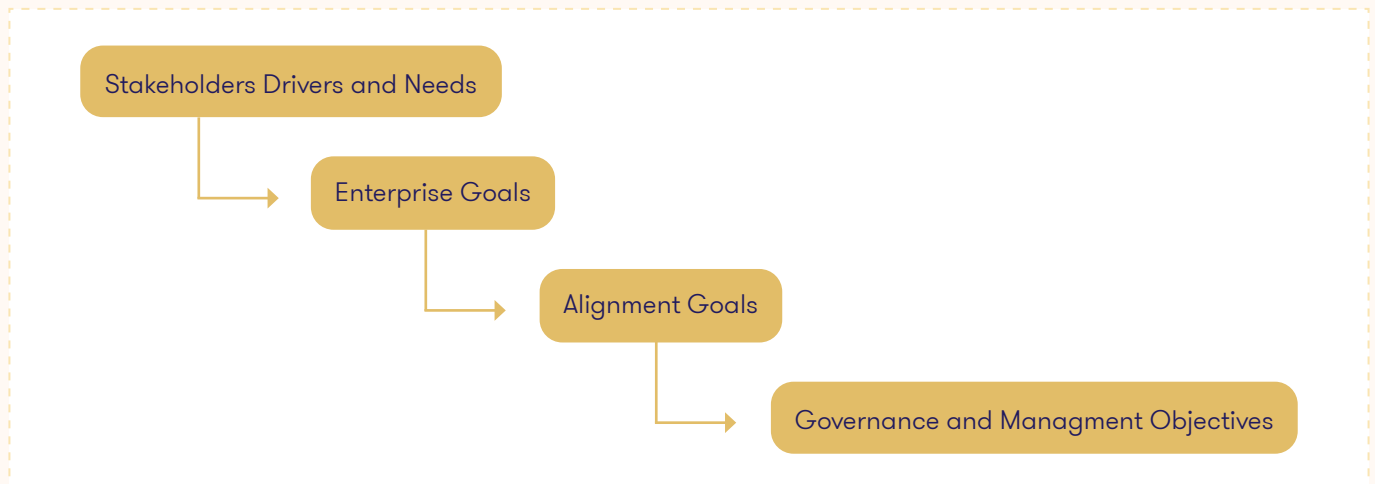


Figure 2: Goal cascade (ISACA, 2018)

## IT Value

## 3.2

COBIT states that every enterprise requires a governance system to meet stakeholder needs and create value through the use of information and technology, known as Enterprise Governance of Information and Technology (EGIT) (ISACA, 2018, p. 11).

Organizations need a practical strategy and governance framework to achieve this value. Effective governance fosters alignment, which drives value creation, as illustrated in the accompanying figure (ISACA, 2018, p. 11).

Value is defined as the equilibrium among benefits, risks, and resources. To create value, it is crucial to achieve an optimal balance between realizing benefits, managing risk levels, and utilizing resources effectively to meet the organization's objectives (ISACA, 2018, pp. 11-12).



Figure 3: From enterprise governance to value creation (ISACA, 2018)

Due to their fundamentally different objectives from those of the private sector, public bodies have unique needs regarding IT governance (Winkler, 2013) particularly in how they define and manage value creation and its components: benefits realization, risk management, and resource optimization.



Figure 4: The optimal balance for value creation (ISACA, 2018)

### Benefits Realization

Benefits realization emphasizes achieving desired business outcomes through IT-enabled investments. Creating public value is inherently more complex than simply maximizing profit. In addition to improving administrative efficiency, larger political and social benefits must be considered. Public IT governance must address a wide range of stakeholders, including political and administrative actors, and strive for alignment to a greater extent than seen in the private sector.

### Risk Optimization

Risk optimization aims to minimize IT-related risks that could hinder enterprise objectives. Public organizations often enforce stricter oversight, impose formal budgetary controls, and exhibit heightened risk awareness. As a result, they tend to adopt a more risk-averse posture, leading to slower innovation and a reputation as late adopters of IT advancements.

### Resource Optimization

Resource optimization ensures that the appropriate capabilities – people, processes, infrastructure, and technology – are available to support strategic goals. Public sector entities often face shortages in IT competencies due to their limited ability to offer competitive compensation to attract qualified professionals.



Differences between  
Public and Private Sectors

3.3

Public sector corporate governance is generally more complex than that of the private sector, which makes IT control more important (Liu & Ridley, 2005). On one hand, this is due to the intricate relationships between those with primary accountability — such as parliament and ministers (Madham, 2014). On the other hand, this complexity stems from differences in environmental factors, interactions between organizations and their environments, and internal structures and processes, all of which make IT governance in the public sector more complex than in the private sector (Liu & Ridley, 2005). Public sector entities are also perceived as having fewer incentives to improve corporate governance and transparency in disclosures (Madham, 2014).

Sethibe, Campbell, and McDonald (2007) provide an overview of the characteristics of nonprofit organizations, including a strong focus on accountability, conservative risk management, substantial investment constraints, strategic objectives, and the influence of political forces. However, regarding value creation, the absence of a profit-driven objective may be the most critical factor. In the private sector, the profit motive provides a clear benchmark for determining value. In contrast, its absence in government creates challenges for implementing transparent value creation processes.

PUBLIC SECTOR	PRIVATE SECTOR
Objectives and Goals	
IT governance aims to ensure transparency, accountability, and the efficient use of public funds. The primary goal is to serve the public interest by delivering services that align with policy objectives and government mandates. Performance is often measured by regulatory compliance, cost-effectiveness, and equitable service access.	The primary objective of IT governance is to support business growth, improve profitability, and gain a competitive edge. Governance is more directly linked to achieving financial goals, enhancing customer experience, and increasing shareholder value.
Regulatory & Compliance Requirements	
High levels of regulatory oversight — driven by legislation, governmental standards, and public scrutiny — govern IT operations. This focus on compliance adds operational complexity and may delay decision-making.	Compliance is often guided by industry-specific regulations (e.g., finance, healthcare) and frameworks such as GDPR for data privacy or NIS for cybersecurity. Processes tend to be more streamlined and adaptive to market needs.
Stakeholder Accountability	
Accountability to the public and elected officials requires greater transparency. IT governance decisions often go through multiple layers of approval and are subject to public scrutiny, involving actors such as politicians, agencies, and citizens.	Accountability is primarily to shareholders, boards, and customers. While transparency remains important, it is internally managed, allowing companies more discretion in communicating governance decisions.

PUBLIC SECTOR	PRIVATE SECTOR
Decision-Making Processes	
Decision-making is typically centralized and hierarchical, influenced by bureaucracy. It is often slower due to the need for legislative approval and multi-stakeholder consultation. IT projects are subject to public tenders with rigid procurement rules that limit agility.	Decision-making tends to be agile and decentralized. Private companies have greater flexibility to pursue IT innovations and partnerships, with streamlined approval processes and the ability to adapt frameworks quickly to meet changing business needs.
Risk Management	
Risk management is cautious. Public agencies prioritize continuity of service, citizen trust, and compliance over innovation. A «caution-first» approach dominates, minimizing reputational and financial risk.	Private companies are often more willing to take calculated risks for competitive advantage. IT governance frameworks are more adaptable to evolving risk profiles and support proactive investment in emerging technologies.
Funding and Resource Allocation	
IT project funding depends on government budgets, which are subject to public spending priorities and require legislative approval. This dependency restricts large-scale innovation and limits responsiveness to technological change.	Funding is driven by ROI expectations. Companies can adjust budgets quickly to seize market opportunities. IT investments are strategically aligned with growth objectives, enabling faster innovation and transformation.
Performance Metrics and Evaluation	
Metrics focus on service delivery efficiency, public value, and regulatory compliance rather than financial return. Success is evaluated through citizen satisfaction, access, responsiveness, and transparency.	Metrics are primarily financial and operational—profitability, efficiency, cost savings, and market performance. Customer satisfaction also plays a role, but the emphasis is on measurable business outcomes.
Innovation & Flexibility	
Innovation tends to be slower due to regulatory constraints, tight budgets, and risk aversion. IT governance emphasizes long-term service continuity, security, and stability over rapid technological advancement.	Private companies are more agile in adopting new technologies, including cloud and agile methodologies. They invest heavily in R&D to maintain a competitive edge and encourage experimentation and iterative development.
Cybersecurity and Privacy	
Public agencies prioritize cybersecurity due to the sensitivity of citizen data and the potential national impact of breaches. Emphasis is placed on compliance and maintaining public trust.	Cybersecurity is also critical, with strategies centered on protecting proprietary and customer data. The approach is often tailored to industry-specific risks and compliance obligations, with a greater focus on competitive resilience.

## Public Sector Challenges

The differences between the public and private sectors, of course lead to several specific challenges for the public sector (Campbell, 2010) (Gartner, 2022) (Paranteau J., 2024):

- ^ Budgetary constraints are particularly challenging for public-sector organizations. Limited funding for large-scale IT projects is often tied to political cycles, which can result in delays or restrictions when implementing new technology solutions, ultimately hindering the organization's ability to keep pace with technological advancements.
- ^ The public sector pursues multiple objectives, which are often intangible or conflicting, and its programs involve numerous stakeholders with competing interests. Poor solution design or a lack of stakeholder engagement frequently leads to digital services that fail to meet citizens' needs, resulting in low adoption rates and dissatisfaction with public services.
- ^ The public sector's obligation to achieve societal goals makes it more vulnerable to political fluctuations. Political influence and frequent structural reorganizations can destabilize governance mechanisms. Shifting political priorities may overshadow long-term benefits, creating pressure to deliver short-term outcomes. Departmental agendas can also change significantly with each new administration.
- ^ Resistance to change is common within public sector cultures. Public servants are often risk-averse and see limited value in abandoning long-standing practices they perceive as effective.
- ^ Public sector organizations typically operate with lower market exposure, which limits opportunities to implement explicit incentive mechanisms tied to productivity and effectiveness. In addition, they face more stringent legal and procedural constraints.
- ^ The persistence of organizational silos remains a significant concern, impacting all aspects of digital transformation—from strategy and funding to execution. These silos exist across different levels of government, departments, and functional domains.
- ^ The shortage of digital talent and technical expertise in the public sector significantly limits its capacity to implement and sustain modern information systems.
- ^ Public sector managers face challenges in developing effective incentive mechanisms to boost individual performance. Wage disparities between the public and private sectors often result in high turnover, especially in specialized skill areas.
- ^ Public sector systems are high-value targets for cyberattacks due to the sensitive nature of the data they manage. Such breaches can undermine public trust and lead to severe operational and financial consequences. Ensuring data protection and privacy is a critical priority for public organizations.
- ^ Legacy systems and outdated IT infrastructure limit scalability and interoperability, increase maintenance burdens, and make digital transformation efforts complex, costly, and time-consuming.

The Belgian Court of Audit (Belgian Court of Auditors, 2024) has published a report entitled 'Steering the digital transformation of the justice system by the Federal State', in which it assesses the measures taken to digitally modernize the Belgian justice system.

The main findings show:

- ^ Lack of a coherent strategy clearly defining the objectives and resources required.
- ^ Roles and responsibilities are not clearly defined, resulting in dysfunctional decision-making and implementation of digital projects.
- ^ Over-reliance on consultancy poses risks in terms of budget management, potential conflicts of interest and commercial influence, without sufficient control over these risks.
- ^ The absence of a transversal digitization policy at federal level limits the synergy between the various public services.



Based on the recommendations, the Federal Justice took some actions:

- ^ Integration of internal players into a single team, with a clarification of roles and responsibilities.
- ^ Implementation of a new governance structure.
- ^ Strengthening internal control and decision-making capabilities.
- ^ Improved portfolio and project management.

# Research Approach and Result

To gain insight into the meaning of IT value within governments, the implementation of IT governance, and the achievement of comprehensive value creation, we gathered extensive input from ISACA members and analyzed two specific cases. One case offered contextual background, while the other illustrated best practices. The following section interprets, discusses, and presents guidelines derived from these findings.

## Round Table Session – Integrating IT Governance for a Secure Future

4.1

On October 14, 2024, ISACA hosted a roundtable session in Antwerp titled “Integrating IT Governance for a Secure Future.” More than 100 participants — from the Netherlands and Belgium — shared their insights and perspectives. They represented roles in ICT management, cybersecurity, CIO offices, and IT governance, with some also active in project management, risk management, and auditing.

Steven De Haes opened the session by presenting highlights from the Global Benchmark of Enterprise Governance of IT, conducted in late 2023 and covering responses from 598 participants across 95 countries [De Haes et al., 2024]. He also shared key findings from his research in areas such as Digital Strategy, IT Governance and Management, IT Strategy and Alignment, IT Value and Performance Management, IT Assurance and Audit, and Information Risk and Security.

During the round table session, the following key points were discussed:

- ^ The value of IT was linked to its contributions to political commitments, societal outcomes, efficiency gains through cost reduction, and the enablement of new services and innovations.
- ^ IT value creation was considered essential across core and innovation processes, as well as operational and support functions, and to a lesser extent, advisory, control, oversight, and regulatory functions.
- ^ The implementation and monitoring of IT value creation rely on a variety of frameworks and standards, including ITIL, ISO, NIS2, COBIT, SAFe, and PRINCE2.
- ^ To ensure IT value, organizations: (1) allocate budgets based on benefits, costs, and risks; (2) define measurable outcomes through documents such as vision statements, annual and project plans, and business cases; and (3) facilitate stakeholder engagement through stand-ups, workshops, and PI (Program Increment) events.



Perhaps the most critical point raised during the session was the need for concrete guidelines to make IT value creation actionable and practical within the public sector. This aligns with findings from De Haes et al. (2024), which indicate that the implementation of governance objectives (EDM - Evaluate, Direct, Monitor) (Figure 6) tends to lag behind other management objectives (Figure 5). They “can be more challenging to implement. It often requires long-term planning and buy-in from board and top management, which might explain the slightly lower score” (De Haes et al., 2024).

It is reassuring to note that government organizations perform at an average level in the implementation of governance and management objectives compared to other sectors. As De Haes states, “since the introduction of COBIT 2019, organizations are improving across all dimensions of the framework” (De Haes et al., 2024).

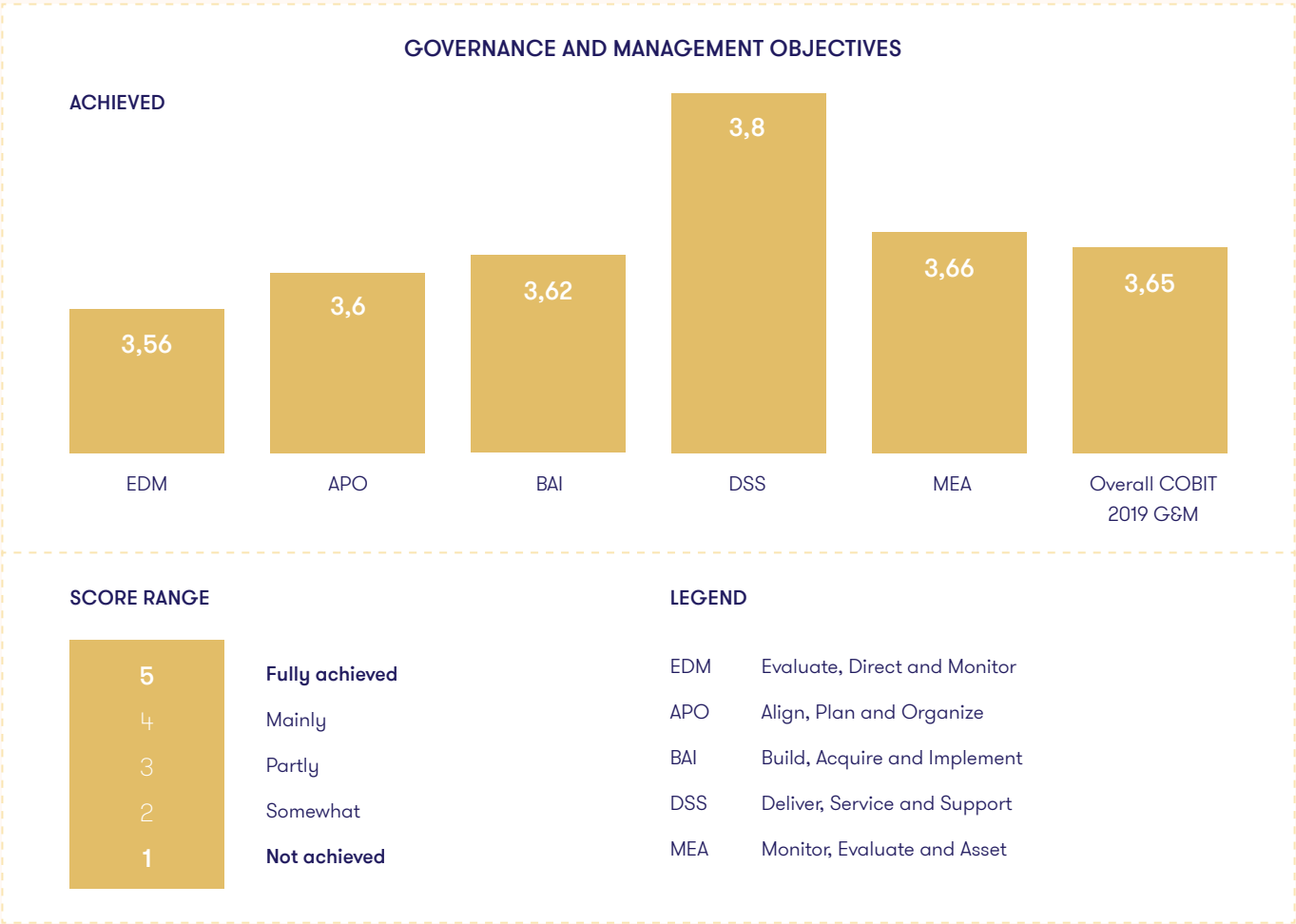


Figure 5: Governance and Management Objectives Achieved [De Haes et al., 2024]

## Case – Context and Life Cycles for Value Creation in the Dutch Government

4.2

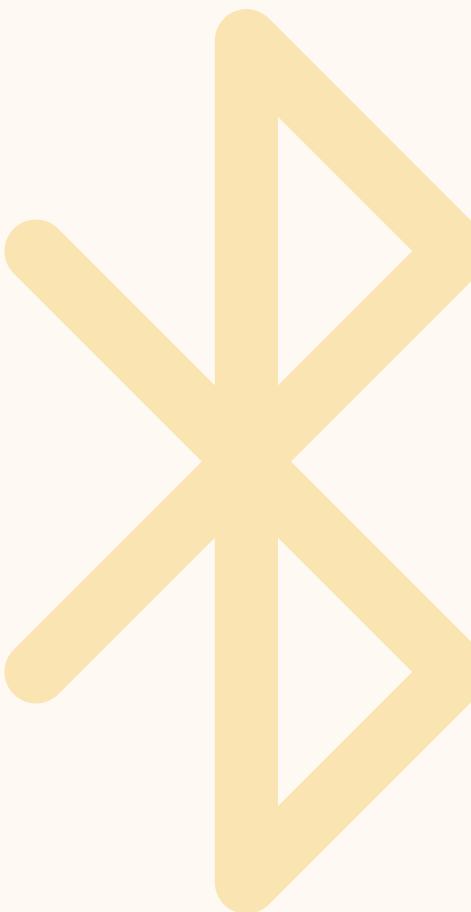
This case presents a perspective on IT value creation within the Dutch central government. It provides contextual input for formulating guidelines.

### Value assessment

Within the Dutch central government, a planning cycle takes place at the beginning of each year in every ministry. During this cycle, directors outline the goals they intend to achieve, identify potential risks, and specify the financial resources required. These plans are submitted to the Directors General (DG) for approval, who then coordinate with the Secretary-General (SG). All financial claims are processed by the financial department, assessed for fiscal feasibility and policy alignment, and then forwarded — with recommendations — to the Board of Directors, composed of the SG and the DGs.

Due to the high failure rate of IT projects, the central government has established several safeguards, including a central advisory committee for IT project assessments and mandatory evaluations within each ministry. Additionally, CFOs in some ministries closely scrutinize IT-related claims, often more than standard financial requests.

In these ministries, IT claims are evaluated according to the full scope of value assessment criteria as defined in the COBIT framework.

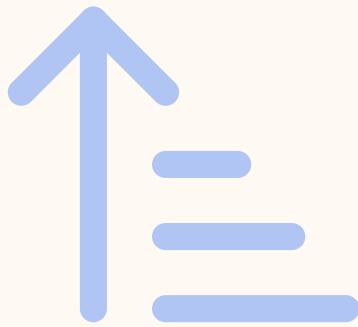


Benefits	Necessity and urgency are assessed similarly to standard claims. However, since many IT requests stem from an accumulation of regulations and frameworks, the political and administrative implications of not implementing a proposal are also taken into account. Benefits may include fulfilling political commitments (e.g., enabling policy implementation through IT), complying with IT governance frameworks, increasing operational efficiency, and mitigating risks related to legacy systems and cybersecurity.
Resources	Costs are assessed not only in terms of feasibility but also in terms of cost-reduction potential, based on differentiating between core needs and optional features. Given the overload of executive services, portfolio management is used to evaluate whether the necessary human resources are available. Special attention is given to the availability of required, often highly specialized, IT expertise.
Risks	In light of the high failure or delay rate of IT projects in both public and private sectors, internal control mechanisms are assessed with increased scrutiny.

After evaluating all these dimensions, the CFO submits their recommendations regarding the IT claims — including proposed adjustments to resources and approach — to the Board of Directors, which ultimately makes the final decision.

However, the CFO exerts significant influence over IT funding decisions, as they are responsible for budget approval and report independently to the Ministry of Finance.

The CIO also has a means of exerting influence by issuing a CIO assessment for a project, which is submitted to the National Audit Committee for ICT. This may lead to an investigation by the committee, which reports directly to the Council of Ministers.



## Value realization

During large-scale projects execution, progress is monitored by multiple governance bodies:

- ^ At the start of a project, the CIO issues a formal assessment. Both the CIO and CFO evaluate the business case, and final approval is granted by the Board of Directors.
- ^ Projects are overseen by a steering committee composed of directors, including representatives from the client's business unit, as well as the CFO and CIO.
- ^ Large-scale projects may be reviewed by the external and independent Advisory Commission for ICT Assessment (AC-ICT), which provides recommendations to the minister regarding the project's initiation and/or continuation. The assessment evaluates whether the project has a clearly defined objective (i.e., a valid business case) and whether there is reasonable confidence that the objective can be achieved efficiently (i.e., a strong chance of success).
- ^ Quality Assurance Boards recommend that the steering committee ensure all critical decisions and associated risks are clearly identified, formally presented, and justified in writing.
- ^ The CIO requires the project manager to submit an annual report detailing progress and compliance with key frameworks, with a particular emphasis on security.

Key challenges arise during this evaluation process:

- 1 Different organizational units are typically responsible for evaluating costs, benefits, and IT risks — namely the CFO, Policy Directors General, and CIO. Although they sit together on the Board of Directors, the CFO and CIO do not hold the same decision-making authority as the Policy Directors.
- 2 In times of budgetary constraints, it becomes difficult to compare the often subjective and politically sensitive value of competing initiatives and to decide which can be responsibly rejected. This evaluation is typically based on identifying which political or administrative commitments can be safely deprioritized, a responsibility that falls to the Policy Director General and the Secretary-General. A comprehensive value assessment is not always performed.
- 3 In the private sector, resources are generally viewed as costs and can be mathematically compared to anticipated benefits, which are often expressed in financial terms. In the public sector, however, benefits are more difficult to quantify and rarely convertible into monetary value. As a result, there is often no clearly defined upper limit for acceptable costs, and required resources are not always considered a constraint.



- ^ The CFO considers risk management essential to realizing value, as it helps prevent cost overruns and ensures that intended benefits are preserved. Effective risk management is treated as a prerequisite for the allocation of financial resources, and the CFO organizes regular risk assessment sessions to safeguard the required quality standards.



One of the key challenges in realizing value is the influence of governmental life cycles, which can disrupt or undermine the process.

- ^ The central government operates under two relatively fixed cycles: the EU policy cycle, which spans approximately seven years, and the cabinet cycle, which typically lasts four years.
- ^ The government also defines the life cycles of IT components, including financial depreciation periods of up to seven years.
- ^ A skilled and experienced executive is critical for value management, encompassing benefit realization, cost control, and risk mitigation. The CFO acknowledges the importance of IT literacy in policy development and therefore initiates training programs and provides ongoing support to ensure compliance with relevant policies.
- ^ The central CIO (CIO-Rijk) is committed to positioning IT at the core of public policy. The department's CIO initiates pilot projects and proofs of concept (PoCs) to foster interest and understanding of IT's potential to create new value.
- ^ In practice, many projects exceed the length of both cabinet and EU policy cycles. According to publicly available data from the Dutch government, major projects have an average duration of 5.2 years (as of January 2025), with 50% lasting more than six years and approximately 25% extending beyond eight years.

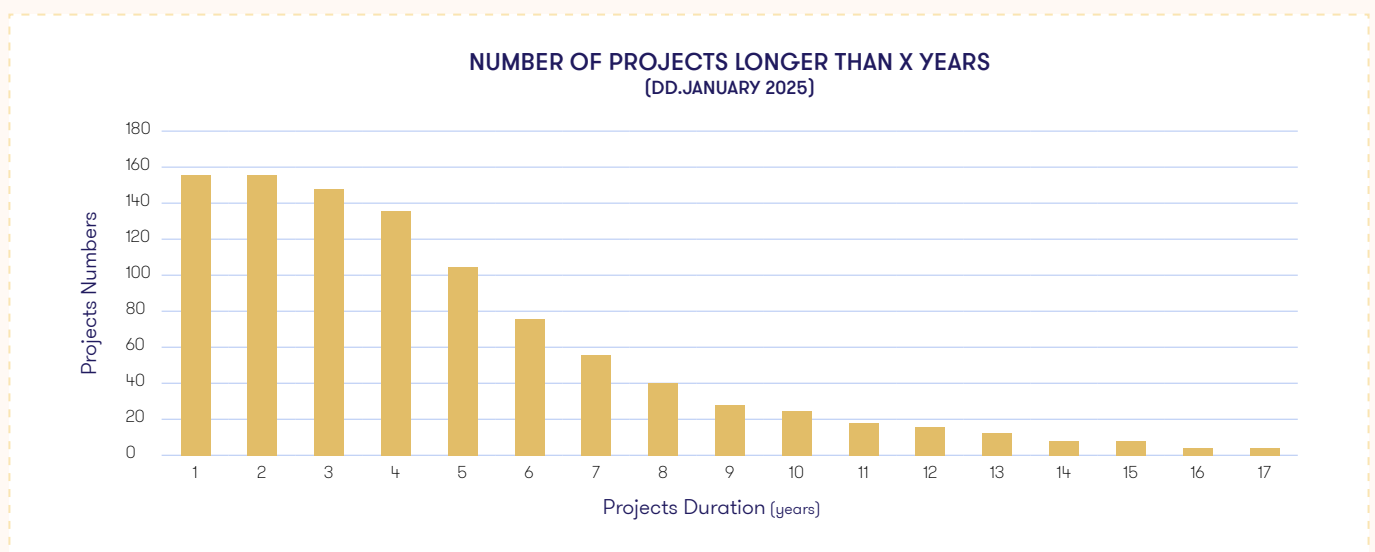


Figure 6: Project duration in Dutch government (Source: [www.rijksictdashboard.nl](http://www.rijksictdashboard.nl))

Political decisions and unexpected elections may lead to IT disinvestment, causing a decline in realized value.

Policy discussions often overlook foundational IT issues. Infrastructure, platform, and contract decisions frequently outlast political cycles — often spanning ten years or more, compared to four years at the national level or seven years at the EU level.

Although these decisions fall under the purview of IT management, they may constrain future political direction and even influence the policy agenda itself.

IT components and platforms are often used for significantly longer periods in the public sector than in the private sector. As a result, the predefined depreciation periods are frequently exceeded.

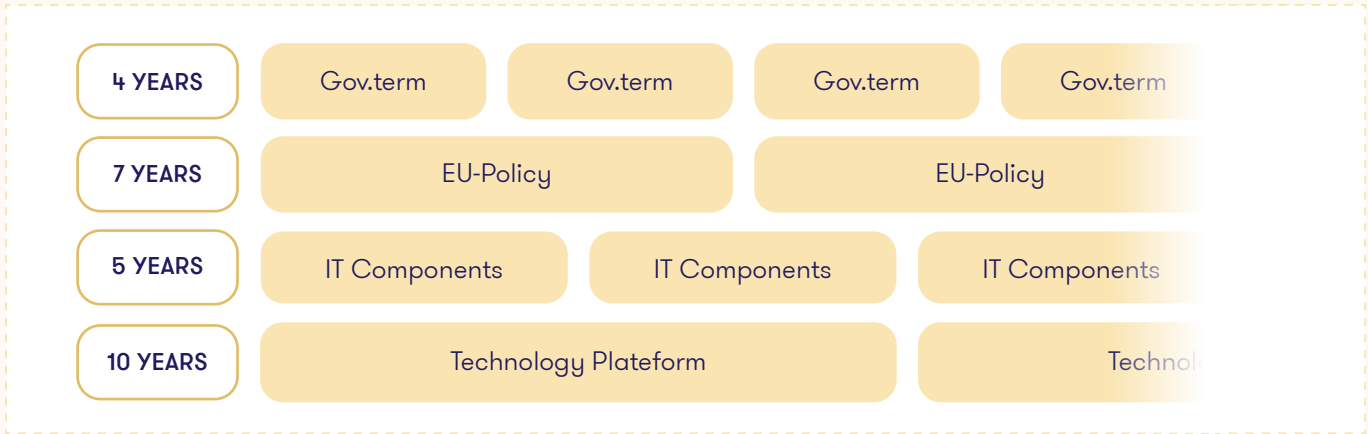


Figure 7: Policy and IT lifecycles within the government

### Case – Good Practices Implementing IT Governance in the Belgian Government

4.3

This case outlines best practices for implementing IT governance and generating value within a Belgian public sector organization.

In COBIT 2019, governance objectives are designed to evaluate, direct, and monitor an organization’s IT resources and capabilities (ISACA, 2018; Terblanche, 2011).

In line with the governance principles outlined in the previous section, relational mechanisms must

be established alongside supporting processes and structures. The objective is to align each governance domain with corresponding management objectives. Five governance clusters — each integrating both governance and management components — were identified through assessments carried out by Belgium’s public internal audit services.

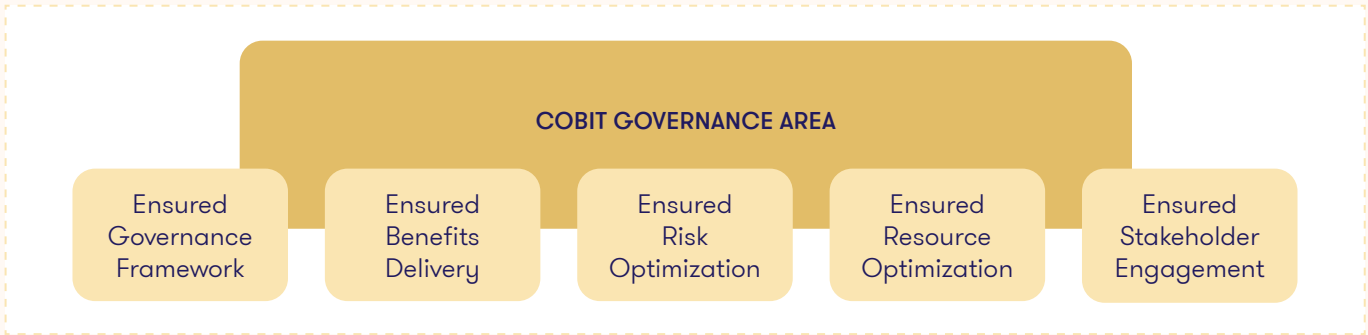


Figure 8: COBIT Governance Area (ISACA, 2018)

## Framework Cluster



Figure 9: Framework cluster (ISACA, 2018)

### PURPOSE

Analyze and clearly articulate corporate IT governance requirements while establishing and maintaining structures, principles, processes, and practices that facilitate effective decision-making. This should ensure transparency of responsibility and authority to achieve the organization's mission and strategic objectives.

### GOOD PRACTICES

- ^ Continuously identify and engage with stakeholders, document their requirements, and assess both the current and future design of the organization's IT governance.
- ^ IT must be represented at the executive management level. The CIO should report to the highest-ranking administrative official to ensure alignment with corporate governance, digital strategies, and public service delivery goals.
- ^ Establish a digital responsibility matrix that clearly defines the roles, responsibilities, and accountabilities related to the strategic alignment and management of digital initiatives, technologies, and data. Additionally, specify the composition and functions of governance bodies and committees, decision-making frameworks, levels of authority, and the information required to support informed decision-making.
- ^ Establish an IT Strategy Committee, with the CIO as a standing member, to assess the current IT strategy and ensure alignment between IT initiatives, the organization's strategic objectives, and its public policy goals.
- ^ Establish a Business Information Manager (BIM) role within each business unit. The BIM will act as a liaison between business functions and the IT department, ensuring that IT strategies and resources are aligned with organizational goals. This role promotes effective decision-making, process optimization, and innovation.

## Benefits Cluster



Figure 10: Benefits cluster (ISACA, 2018)

### PURPOSE

Strengthen the contribution of the IT investment portfolio to the organization's service delivery and asset management strategy, while maintaining acceptable cost levels.

### GOOD PRACTICES

- ▲ Strategic planning: Ensure that public service management contracts are translated into operational plans that encompass both new digital initiatives and routine IT operations. The executive committee should actively participate in the development, prioritization, and validation of IT strategies, ensuring alignment with the organization's overall mission and objectives.
- ▲ Digital portfolio: The strategic alignment process used to build the IT portfolio should be formalized and clearly understood by all stakeholders particularly management, business units, and IT.
- ▲ Projects: Ensure that project selection is based on available resources and that prioritization reflects their expected contribution to benefit realization. Implement a standardized, organization-wide project management methodology that complies with applicable regulatory and compliance requirements. A Project Management Office (PMO) can support the consistent application of this methodology and oversee the reporting of project status across the portfolio.
- ▲ Efficiency control: Regularly assess the performance of portfolio projects to ensure alignment with strategic objectives and to provide management with accurate and consistent reporting on progress and status.
- ▲ Value creation: Ensure a shared understanding of what constitutes value for stakeholders. Focus benefit delivery on outcomes aligned with this value, including cost savings, service efficiency, citizen satisfaction, community well-being, and social equity. Value management practices should enable the optimal realization of IT investments over their full economic life cycle. Establish a benefits realization plan to monitor, manage, and sustain delivery over time.
- ▲ Business case: A structured business case supports value creation by providing a comprehensive analysis of the initiative, proposed solution, costs, benefits, risks, and strategic relevance to the organization. A well-crafted business case is essential to align initiatives with organizational goals, optimize resource allocation, reduce risk exposure, and maximize return on investment. By focusing on benefit realization, the business case helps ensure that IT investments deliver measurable and sustainable outcomes.
- ▲ Enterprise architecture: Establish an architecture board that plays a critical role in aligning the organization's processes, systems, and technology investments with its strategic objectives and operating model.

## Risk Cluster



Figure 11: Risk cluster (ISACA, 2018)

### PURPOSE

Ensure that the organization's risk appetite and tolerance are clearly defined, communicated, and understood, and that IT-related risks are effectively identified, assessed, and managed.

### GOOD PRACTICES

- ^ The impact of risk on both current and future use of IT within the organization should be continuously analyzed and assessed. Levels of risk appetite and tolerance must be clearly established. Risk management practices should ensure that IT-related controls are appropriate, consistent, and effective.
- ^ Defining a digital risk appetite involves determining the level of risk an organization is willing to accept to achieve its strategic objectives in a digital environment. In the public sector, this appetite tends to be conservative, leading to a cautious approach — particularly in areas involving public funding, essential services, and citizen trust. Supervisory governance bodies must ensure that this risk appetite is aligned with societal expectations and the public interest.
- ^ Establishing a formal risk function at the management level is essential for effectively overseeing both organizational and digital risks. As dependence on technology increases, digital risks have become more prominent. Clear risk ownership should be assigned to individuals or teams responsible for mitigating these risks.
- ^ Ensure that each operational department maintains a risk management process to identify, assess, and mitigate digital risks. A centralized risk function should coordinate these efforts and monitor the implementation of mitigation plans. All identified risks should be integrated into the broader Enterprise Risk Management (ERM) framework.
- ^ The organization should maintain a digital risk inventory that includes all relevant risk scenarios. The COBIT for Risk framework (ISACA, 2021) provides a comprehensive taxonomy of risk categories to support this process.
- ^ Organizations should address cybersecurity risks by integrating responsibilities across both management and operational levels. Public sector entities must implement the NIS2 directive to ensure the continuity of essential services during cyberattacks or IT system outages.
- ^ Potential project risks must be proactively managed to minimize adverse impacts and ensure successful delivery.

## Resource Cluster



Figure 12: Resource cluster [ISACA, 2018]

### PURPOSE

Ensure the availability of adequate IT-related capabilities — including financial resources, human competencies, and infrastructure — to effectively support strategic objectives in a cost-efficient manner throughout the business life cycle.

### GOOD PRACTICES

- ^ Resource management strategies, guiding principles, agreed-upon resource plans, and architectural approaches should be formally established and communicated to optimize both business and IT resources over their full economic life cycle.
- ^ Anticipate budgetary needs for digital services through structured planning, strategic forecasting, and a clear understanding of each project's objectives. Resource allocation should reflect project prioritization. Engage in comprehensive financial planning that spans the entire project lifecycle, including ongoing status monitoring.
- ^ A digital competence matrix should be developed to assess and visualize the digital skills and capabilities of individuals and teams. It allows for mapping current proficiency levels, aligning them with role-specific requirements, and identifying skill gaps for improvement.
- ^ Digital innovation is a key enabler of public sector transformation, driving operational efficiency, improved citizen services, and greater transparency. The deployment of online platforms, mobile apps, artificial intelligence (AI), and smart infrastructure can deliver meaningful and measurable improvements for society.
- ^ Address IT talent shortages and an aging workforce by developing strategies to identify, attract, and retain qualified professionals. Solutions may include proactive talent pipelines, partnerships with academic institutions, and targeted upskilling programs. The use of shared digital services can also help consolidate efforts and resources across multiple public entities.
- ^ Centralize knowledge management by developing integrated repositories that support efficient knowledge sharing, transfer, and long-term retention.
- ^ While many IT services are outsourced due to recruitment challenges, core competencies should remain in-house. These internal resources must be actively managed and supervised to ensure quality and alignment with organizational objectives.
- ^ Streamline IT systems by reducing the number of applications and processes, eliminating redundancies, and retaining only the most essential and value-generating solutions.

## Oversight Cluster



Figure 13: Oversight cluster (ISACA, 2018)

### PURPOSE

Ensure transparency in IT performance and compliance through clearly defined indicators, dashboards, and reporting mechanisms. Obtain stakeholder approval for performance targets, evaluation metrics, and any required corrective measures.

### GOOD PRACTICES

- ^ Quantitatively assess stakeholder engagement mechanisms to ensure accuracy, reliability, effectiveness, and compliance with their reporting and communication requirements.
- ^ Clearly defining roles and responsibilities among IT, business, and management promotes transparency, accountability, and continuous communication.
- ^ Evaluate the effectiveness and performance of corporate IT governance. Confirm whether the governance system and its underlying structures, processes, and relational mechanisms are operating as intended and delivering appropriate IT oversight to support value creation.
- ^ Up-to-date management information supports decision-making by providing key performance indicators and insights into portfolio health.
- ^ Track key objectives and performance indicators to assess whether the organization is realizing the expected value and benefits from IT investments and services. Continuously monitor risk metrics and resource indicators to detect and report deviations or issues and to support timely corrective action.
- ^ Strengthen the Three Lines Model (Institute of Internal Auditors, 2020) by ensuring that second-line functions — such as compliance, risk management, internal control, security, and privacy — are operational and provide adequate support to first-line business units. The third line offers independent assurance, enabling the continuous improvement of business and IT processes. Ensure that all three lines have the necessary IT expertise to carry out their responsibilities effectively.

# Discussion and Guidelines

We have identified the following challenges based on the roundtable discussions and case studies:



1	Decision-making around IT in government is challenging due to complex interdependencies between resources, benefits, risks, administrative environments, distributed responsibilities, and power dynamics.
2	Benefits are diverse and subjective, making them difficult to compare and complicating portfolio decision-making.
3	Translating IT urgency into corporate value remains a significant challenge.
4	Public policy tends to place limited emphasis on foundational IT components such as infrastructure, platforms, and underlying contracts. As a result, IT decisions that influence policy are often not made at the corporate level — or, if they are, are not prioritized, particularly when they concern legacy systems.

These challenges are consistent with the characteristics of the public sector described by Sethibe, Campbell, and McDonald (summarized in Table 1: Private Sector Versus Public Sector) , as well as the challenges outlined in Section 3.5, Public Sector Challenges.

Proposing a specific solution or process for each challenge does not guarantee success. Solutions must be effective within the specific context in which they are applied (Miller, 1986). Additionally, some solutions may emerge from design decisions that appear unrelated to the challenge but are, in fact, emergent properties of the system.

In the case of the Belgian government, however, the previously mentioned challenges do not appear to apply. This may be the result of effective organizational practices; alternatively, the specific context of the organization may not give rise to these challenges. The latter seems less likely, given that this Belgian organization does not differ significantly from its Dutch counterpart. Further research is needed to confirm this.



## Guidelines

IT governance can be implemented in both the public and private sectors through a combination of processes, structures, and relational mechanisms [Campbell, 2010] [De Haes, 2005]. COBIT 2019 remains a relevant and widely used framework; notably, De Haes has been closely involved in its ongoing development and in advancing IT governance practices aligned with COBIT.

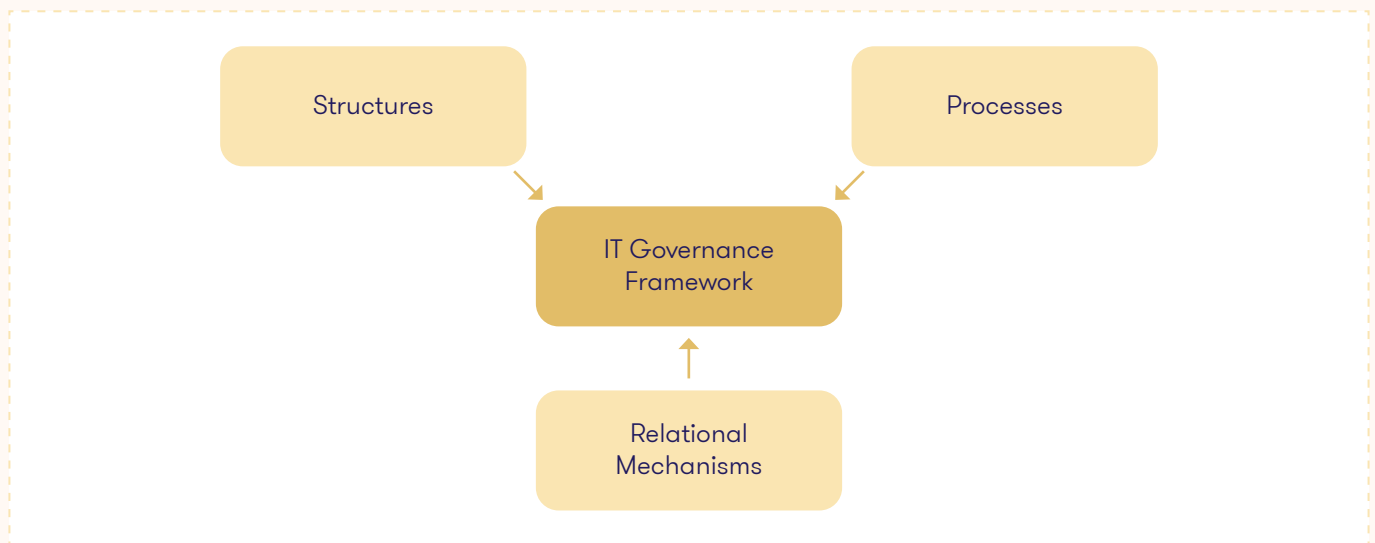


Figure 14: Components of IT governance model [ISACA, 2018]

## Structures

Structures encompass defined roles and responsibilities, the IT organizational setup, the role of the CIO, and governance bodies such as an IT strategy committee or a steering committee. The effectiveness of IT governance is influenced by where decision-making authority resides, and by the presence of a strategic portfolio committee that oversees new investment decisions (based on Campbell, De Haes).

### TAKEAWAYS

- ^ Ensure that the CIO and CFO hold equivalent positions, enabling them to jointly assess the overall value of investments and policy. This likely requires the inclusion of IT at the executive management level. Both the CIO and CFO should report to the highest-ranking administrative official to ensure alignment with public sector governance, digital strategies, and public service objectives.
- ^ Recognize that selecting the most appropriate IT governance model is complex, as it can be difficult to identify all the factors influencing the choice of governance elements. The optimal mix of structures, processes, and relational mechanisms varies significantly from one organization to another (based on Campbell, De Haes).

## Relational Mechanisms

Relational mechanisms refer to the active collaboration between business and IT departments, the exchange of shared knowledge, and the establishment of two-way communication channels

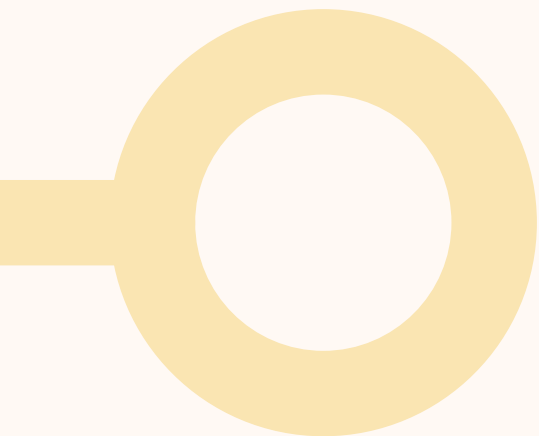
(based on Campbell, De Haes).



## Processes

Processes aim to align business and IT by supporting decision-making and performance monitoring through tools such as the IT Balanced Scorecard. In the public sector, these processes are shaped by societal obligations and expectations, and are subject to periodic yet significant structural changes driven by political cycles (based on Campbell, De Haes).

The government's annual budgeting, control, and accountability cycle functions as a value management process. This process — together with the CFO's existing mandate — can be leveraged to evaluate the value of IT investments. Interim reporting and accountability checkpoints should be used to monitor value realization throughout the year.



### TAKEAWAYS

- ^ Avoid fragmenting responsibility for value components — such as benefits, resources, and risks — across multiple organizational layers. In particular, foster IT affinity and awareness among policy directors to support integrated decision-making.

### TAKEAWAYS

- ^ Establish a strategic alignment process to define the IT portfolio, ideally integrated into the budgeting cycle. Project prioritization should be based on the availability of resources.
- ^ Mitigate risks that may compromise value realization — whether in terms of benefits or resources. Develop a digital risk inventory that includes all relevant risk scenarios. The COBIT for Risk framework (ISACA, 2021) offers a comprehensive overview of risk categories to support this process.
- ^ Implement a benefit realization plan to monitor, manage, and sustain the delivery of expected benefits.
- ^ It is essential to implement the Three Lines of Defense Model (Institute of Internal Auditors, 2020). The model supports organizations in structuring processes that enable goal achievement while ensuring sound governance and risk management. In the first line, operational staff directly own and manage risks. The second line sets policies, defines risk tolerances, monitors compliance, and supports the first line. The third line, represented by internal audit, provides independent assurance of the overall effectiveness of both the first and second lines.

## What is Value in the Government?

It is essential to develop a clear understanding of what constitutes value for stakeholders. Current research has not yet clearly defined how value is determined in the public sector.

It is understood that public sector value does not result from a mathematical formula producing net returns, as is typically the case in the private sector.

Governments are accountable to both political leadership and society for achieving established goals and meeting expectations. Public sector management tends to be more risk-averse than

its private sector counterparts (Sethibe, Campbell, & McDonald, 2007), often prioritizing the prevention of accountability-related risks.

This raises the question of whether accountability risk mitigation could serve as a viable starting point for assessing value in the public sector. Just as the private sector ultimately expresses its overall value through net returns, this perspective may provide a foundation for articulating public sector value in relation to accountability obligations. This proposition could serve as a basis for future research.

## Public Sector IT Scoreboard

Public sector funding originates primarily from the taxpayers it serves. Success is not measured by shareholder value or profit, but by how effectively the agency fulfills the mission assigned to it by political authorities (Išoraitė, 2008). Accordingly, the four dimensions of the Balanced Scorecard can be reinterpreted as follows:

### TAKEAWAYS

- ^ Public contribution (replacing the financial perspective): mission effectiveness entails accountability for the responsible use of public funds in line with budgetary targets. As a result, program performance, resource efficiency, and proactive risk management are essential concerns.
- ^ User orientation: this dimension focuses on service quality, continuity, and the organization's capacity to respond to emerging citizen needs.
- ^ Internal processes: organizational strength depends on robust infrastructure and the adoption of innovative solutions to improve operational efficiency.
- ^ Learning and growth: human capital is strengthened through relevant competencies, continuous development, and the engagement of motivated teams.

## Suitability of COBIT and Other Frameworks

During the roundtable session, it was noted that various frameworks are used — often in combination — to manage IT-driven value creation. The principal methodologies referenced include ITIL, ISO, NIS2, COBIT, SAFe, and PRINCE2.

### COBIT

COBIT 2019 was developed as an umbrella framework that “aligns with other relevant standards, frameworks, and/or regulations” (Information Systems Audit and Control Association, 2018).

The Belgian public sector demonstrates that COBIT can be successfully applied to support IT value creation in government contexts.

### Risk Management and NIS2’s Cybersecurity Management

The cybersecurity requirements introduced under the NIS2 directive (EU, 2025) can be effectively aligned with COBIT’s governance and management practices. Within the regulatory framework aimed at strengthening cybersecurity resilience in critical sectors, several key alignment areas can be identified.

By aligning COBIT practices with NIS2 regulatory requirements, organizations can establish a robust governance framework that not only ensures compliance but also reinforces overall cybersecurity resilience.

### TAKEAWAYS

- ^ Governance accountability: COBIT ensures effective and transparent oversight of cybersecurity processes, verifies regulatory compliance, and satisfies governance requirements for board members (cf. EDM01 – Ensured Governance Framework).
- ^ Risk approach: Addressed through COBIT’s risk governance (cf. EDM03 – Ensured Risk Optimization) and risk management (cf. APO12 – Managed Risk).
- ^ Cybersecurity measures: Implemented via COBIT’s security services (cf. DSS05 – Managed Security Services).
- ^ Supply chain security: Covered through third-party relationship management (cf. APO10 – Managed Vendors) and appropriate security control implementation (cf. DSS06 – Managed Business Process Controls).
- ^ Awareness and training: Provided through human resources governance (cf. APO7 – Manage Human Resources).
- ^ Incident management: COBIT ensures prompt incident handling and reporting (cf. DSS02 – Managed Service Incidents).
- ^ Monitoring and improvement: Achieved through COBIT’s Monitor, Evaluate, and Assess domain (MEA), which supports continuous audits and assessments aligned with NIS2 compliance.



# Conclusion

Information Technology (IT) has become a vital enabler of the central government's efforts to generate social value. However, translating this potential into tangible societal outcomes remains a significant challenge. In contrast to the private sector — where IT value is typically expressed in financial terms — public sector IT value involves elements such as resources, benefits, and risks that are inherently more complex and not easily monetized. Findings from the roundtable session, together with case studies from Belgium and the Netherlands, highlight a growing recognition of this complexity and an increased awareness of the challenges involved.

The COBIT framework offers valuable guidance for making IT value creation both measurable and auditable. However, aligning IT value with the specific needs of the (central) government requires a tailored definition and assessment methodology. To support the successful creation of IT value in the central government, the following steps are essential:

**1**

Allocate budgets based on a thorough assessment of benefits, costs, and risks.

**2**

Define clear, measurable outcomes through strategic documentation, including vision statements, annual plans, project plans, and business cases.

**3**

Foster continuous stakeholder engagement through structured interactions, such as stand-ups, workshops, and Program Increment (PI) events.

# Acknowledgments

We would like to thank all members of the working group who contributed to the survey, the roundtable discussion and workshop sessions, and the drafting of this white paper. We are also grateful to the participants from both the public and private sectors in Belgium and the Netherlands for their valuable input. A special acknowledgement goes to **Prof. Steven de Haes** for his excellent contribution to the roundtable session, which greatly enriched the discussions and outcomes.

## Research Sponsors

Belgian Cyber Security Coalition

ISACA Belgium

ISACA Netherlands

## Development Team

### **Maria Haasnoot**

Strategic Business I-Controller, and advisor  
Dutch Central Government

### **Nard Janssens**

Strategic Business I-Controller and advisor  
Dutch Central Government

### **Patrick Soenen**

IT Governance trainer  
ISACA Belgium

## Expert Reviewers

### **Pascal Champagne**

Business Development Manager  
Belgian Cyber Security Coalition

### **Prof. Dr. Barry Derksen**

Board member  
ISACA Netherlands

### **Egide Nzabonimana**

President  
ISACA Belgium





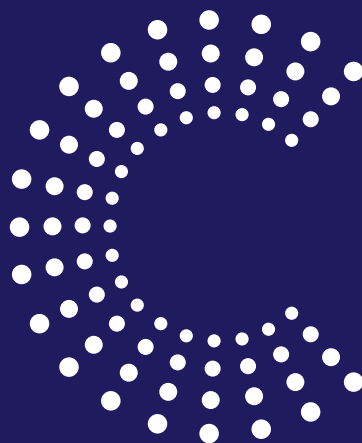
# References

- Al Qassimi, N. &. (2015). IT Governance in a Public Organization in a Developing Country: A Case Study of a Governmental Organization. *Procedia Computer Science*, E-ISSN 1877-0509, Vol. 64, , p. 450-456. Retrieved from <https://www.sciencedirect.com/science/article/pii/S1877050915026769>
- Algemene Rekenkamer. (2007). Lessen uit ICT-projecten bij de overheid - deel A. Vergaderjaar 2007-2008, Kst 26643, nr 100. Algemene Rekenkamer.
- Aussems, M. (2025, 10 1). Digitaliseringsdebaacle bij Justitie: geen strategie, amper competenties, ongekende legacy en slechte samenwerking. Retrieved from ITdaily: <https://itdaily.be/blogs/business/justitie-digitalisering-rekenhof/>
- Beijert, L., & Koedijk, J. (2016, 2). Het is vijf voor twaalf: pak legacy ICT aan! Retrieved from Compact «powered by KPMG Netherlands»: <https://www.compact.nl/articles/het-is-vijf-voor-twaalf-pak-legacy-ict-aan-2/>
- Belgian Court of Auditors. (2024). Pilotage de la transformation numérique de la justice par l'état fédéral / Aansturing van de digitale transformatie van Justitie door de federale overheid. Belgian Court of Auditors.
- Campbell, J. M. (2010). Public and private sector IT governance, identifying contextual differences. *Australasian Journal of Information Systems*. doi:<https://doi.org/10.3127/ajis.v16i2.538>
- Dawson, G. S., Denford, J. S., Williams, C. K., Preston, D., & Desouza, K. C. (2017). An Examination of Effective IT Governance in the Public Sector Using the Legal View of Agency Theory. *Journal of Management Information Systems*, pp. 1180-1208.
- De Haes, S. &. (2005). IT Governance Structures, Processes and Relational Mechanisms. *Proceedings of the 38th Hawaii International Conference on System Sciences*. doi:10.1109/HICSS.2005.362
- De Haes, S., Joshi, A., Huygh, T., & Van Giel, Z. (2024). Global Benchmark of Enterprise Governance of IT (Through the lens of COBIT). Antwerp Management School.
- EU. (2018). The EU Cybersecurity Act. Retrieved from European Union: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- EU. (2025, 3 3). Data protection under GDPR. Retrieved from Your Europe: [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\\_en.htm](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm)
- EU. (2025, 1 25). NIS2-richtlijn. Retrieved from Europese Commissie: <https://digital-strategy.ec.europa.eu/nl/policies/nis2-directive>
- Gartner. (2022). 5 Key Digital Transformation Challenges Government CIOs Must Tackle. doi:<https://doi.org/10.1016/j.procs.2023.10.175>
- The Institute of Internal Auditors (2020, 7 21). Three Lines Model Updated Retrieved from: <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf>
- ISACA. (2018). COBIT 2019 Framework – Governance and Management Objectives.
- ISACA. (2018). COBIT® 2019 Framework: Introduction and Methodology. ISACA.
- ISACA. (2021). COBIT Focus Area – Information & Technology Risk Using COBIT 2019.



- Išoraitė, M. (2008). The Balanced Scorecard Method: from Theory to Practice. Intellectual Economics.
- Liu, Q., & Ridley, G. (2005). IT Control in the Australian public sector: an international comparison. Retrieved from [https://figshare.utas.edu.au/articles/conference\\_contribution/IT\\_Control\\_in\\_the\\_Australian\\_public\\_sector\\_an\\_internatio](https://figshare.utas.edu.au/articles/conference_contribution/IT_Control_in_the_Australian_public_sector_an_internatio)
- Madham, P. M. (2014). Corporate Governance and Disclosure Public Sector vs Private Sector. SCMS Journal of Indian Management, pp. 5-20.
- Miller, D. (1986). Configurations of strategy and structure: A synthesis. Strategic Management Journal, 7, pp. 233-249.
- Morcol, G. (2014). Complex Governance Networks: An Assessment of the Advances and Prospects. Complexity Governance & Networks, pp. 5-16.
- Nawi, H. S., Rhamn, A. A., & Ibrahim, O. (2014). Government ICT Project Failure Factors: Project Stakeholders' Views. Journal of Research and Information Systems, 2, pp. 69-77.
- Osunji, O. (2021). Know your suppliers: A review of ICT supply chain risk management efforts by the US government and its agencies. Cyber Security: A Peer-Reviewed Journal 4(3), pp. 232-242.
- Paranteau J. (2024). Public Sector IT Transformation: Challenges and Solutions", OnPoint, 2024. Retrieved from OnPoint: <https://www.c-onpoint.com/public-sector-it-transformation-challenges-and-solutions/>
- Rekenkamer, A. (2025). Het Rijk in de cloud - Donkere wolken pakken samen. Rijksoverheid Nederland.
- Rusu, L., & Viscusi, G. (2017). Information Technology Governance in Public Organizations - vol 38 - Chapter 1. Springer.
- Sethibe, T., Campbell, J., & McDonald, C. (2007). IT Governance in Public and Private Sector Organisations: Examining the Differences and Defining Future Research Directions. Association for Information Systems Proceedings, pp. 833-843.
- Talbot, C. (2011). Paradoxes and prospects of 'public value'. Public Money & Management, pp. 27-34.
- Terblanche, J. (2011). An information technology governance framework. University of Stellenbosch, South Africa. Retrieved from <https://scholar.sun.ac.za/server/api/core/bitstreams/bdb30ac0-fec5-4bc1-8352-d40879a281bb/content>
- Winkler, T. J. (2013). IT Governance Mechanisms and Administration/IT Alignment in the Public Sector: A Conceptual Model and Case Validation. Wirtschaftsinformatik Proceedings 2013, (p. 53). Retrieved from <https://aisel.aisnet.org/wi2013/53>





# CYBER SECURITY **COALITION**

The mission of the Cyber Security Coalition is to bolster Belgium's cyber security resilience by building a strong cyber security ecosystem. We do so by bringing together the skills and expertise of the academic world, the private sector and public authorities on a trust-based platform aimed at fostering information exchange, operational peer-to-peer collaboration, making recommendations for more effective policies and guidelines, and finally carrying out joint awareness-raising campaigns aimed at citizens and organisations. More than 1,400 representatives of our 200+ member organizations participate in our activities and as such contribute to our mission.

[cybersecuritycoalition.be](https://cybersecuritycoalition.be)



ISACA is a global professional association and learning organization with 185,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. With a presence in 188 countries and with 225 chapters worldwide, ISACA is recognized around the world for its guidance, credentials, education, training and community. To serve its professional community across the globe, ISACA has established three offices based in North America, Europe and China.

[isaca.org](https://isaca.org)



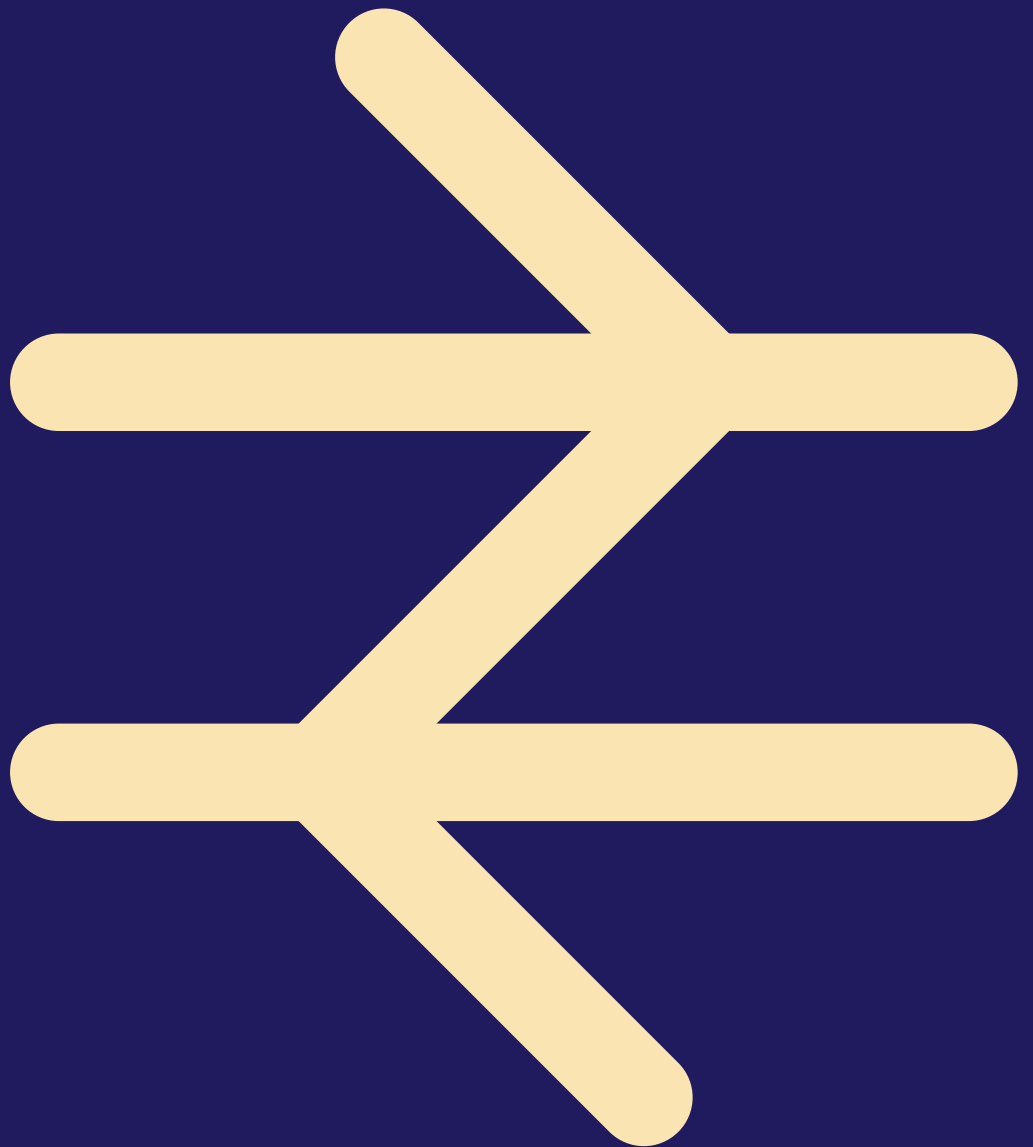
ISACA Belgium is a chapter of ISACA. Our mission is to bring together digital trust professionals for networking, knowledge sharing and personal development. We have been doing so for already more than 39 years. Presently, we represent more than 850 members from 450 different organizations. As such, we are the largest Belgian organization supporting a broad range of Governance, Risk and Compliance topics aiming at increasing trust in digitalization.

[isaca.be](https://isaca.be)



ISACA Netherlands Chapter is the Dutch branch of ISACA, a global professional association dedicated to helping IT professionals and organizations worldwide harness the potential of technology. The chapter supports professionals through knowledge sharing, training, certifications, and networking activities. ISACA Netherlands is committed to strengthening digital trust and fostering professional leadership within the Dutch IT and audit community.

[isaca.nl](https://isaca.nl)



## CONTACT

Egide Nzabonimana  
0032 (0)479 61 64 43  
[egide.nzabonimana@isaca.be](mailto:egide.nzabonimana@isaca.be)

## VERSION

Version:	1.0
Date:	September 2025
Status:	Final Version