Cigref
SUCCEED
WITH DIGITAL

AUDITING DIGITAL GOVERNANCE

Major changes to the Digital Governance Audit Guide

NOVEMBER 2023

Cigref

Auditing digital governance

Major changes to the Digital Governance Audit Guide

November 2023

EDITORIAL

Organisations today are finding that, with the acceleration of technological developments, the *"softwarisation"* of products and production chains, and the digitisation of all organisational processes, the contribution of digital technology to the company's value chain is increasing considerably. For Cigref's member organisations, this phenomenon is characterised by an increase in their dependence on digital technology and a rise in the associated vulnerabilities and risks.

The last three years have seen a wealth of developments, some of which have had a structuring effect on the operational models of digital departments and on the governance of digital technology within companies. The growth, performance and resilience of organisations now depend on digital technologies.

We are seeing the spread of 'agile' approaches, the hybridisation of IT *sourcing* (cloud or in-house), the evolution of *make-or-buy* models, but also the development of new practices such as DevOps and, above all, a change in the roles and missions of digital departments.

It was against this backdrop that Cigref launched an update of the "IT Governance Audit Guide". The result was a working group made up of members with a variety of professional backgrounds, whose task was to reconsider the 12 core vectors of the Audit Guide in the light of developments in the digital function since 2019.

The results of the group's work are therefore presented in this note, which provides a summary of best practices to be shared, and which will offer good material for the next edition of the Guide, on which we will be working with our long-standing partners, ISACA-AFAI and IFACI.

Djilali KIES
CIO at TDF, Working group leader

ACKNOWLEDGEMENTS

Our thanks go to **Djilali KIES, Chief Information Officer** at **TDF**, who steered this work, and to all the people who participated in and contributed to this Cigref working group (in alphabetical order):

Olivier CAIL - MAÏSADOUR

Michel CAPEL - FAYAT

Claudio CIMELLI - MINISTRY

Fabienne CHEVALIER - MINISTRY OF ECOLOGY

Michel DEBLBECQ - ELIS

Erik DU BOISHAMON - MINISTRY OF INTERIOR AFFAIRS

Bruno GIVELET - SYSTÈME U

Gaëlle GOSSE DE GORE - DPD GROUP

Mélanie GRAS - SAVENCIA

Nicolas GRIMAULT - SODEXO

Michel HALABI - AIR FRANCE KLM

Franck HOSTIOU - PIERRE FABRE

Julien JOLIBOIS - MALAKOFF HUMANIS

Bertrand LASQUELLEC - GROUPE AVRIL

Frédéric LEBOEUF - VINCI

Thibaut MITANCHEZ - SFR

Julien MONTAROU - TOTALENERGIES

Guillaume MONTIGNY - BNP PARIBAS

Coralie NICOLLET - MATMUT

Stéphane OLIVE - ACCOR

Michel PEPINO - VIRBAC

Sofiane SAMAH - MSA

Nadia SELLAMI - ACCOR

Vasco ROGEON - SNCF

Nicolas VACHÉ - SYSTÈME U

Our thanks also go to Aliette DIÉVAL, jurist, who contributed to this work during her internship at Cigref. This document was designed and written by Elena SILVERA, Project Manager at Cigref.

TABLE OF CONTENTS

1 INTRODUCTION

Why update the IT Governance Audit Guide?

In 2019, the year of the last version of the *Audit Guide*, the increasing impact of digital technology on the activities of businesses and public authorities was already being noted. Since then, technological developments and transformations have accelerated significantly.

The extension of the missions undertaken by the "Information Systems Departments" is influencing the very terminology used by these entities in certain groups. We now speak of "Digital and Transformation Departments", "Technology and Innovation Departments" or other variations of these names, which clearly reflect the changes that have affected the "IS Department" in recent years. For this reason, we have chosen to call this report *Auditing digital governance* rather than "Auditing IT governance".

The acceleration in the pace of change is naturally leading to an inflation in the expectations expressed by the IT Department's "customers" (in particular the business lines), as well as a change in the IT Department's service offering and operating model. These factors therefore call for an update in the governance of information systems, or, to put it more accurately, "digital governance".

The 2019 Guide presented the IT Department as an entity with a number of interrelated roles and mandates to ensure *RUN*, *BUILD* and "vision" within the organisation (see diagram below)[1] .

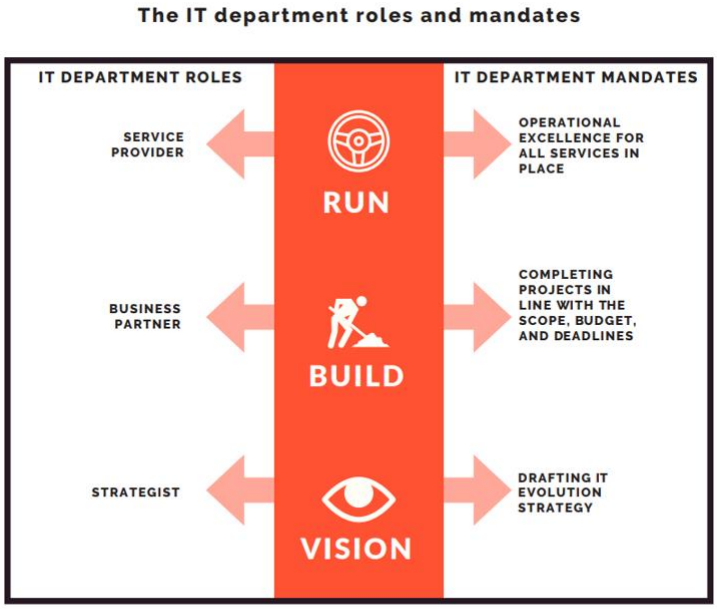

Figure 1. The IT department roles and mandates. Source: IT Governance Audit Guide, 2019

[1] "RUN represents the 'recurring' work that 'enables an IT department to function', often summarised as 'maintenance in operational conditions', or 'everything that does not come under BUILD'. As a reminder, BUILD is made up of projects, improvements and efforts deployed to generate value within the company", Cigref report *Levers for reducing IT Department costs*, June 2023. See also *Economic and Ecological IT Management Model*, 2022 edition.

In this approach, and as far as RUN is concerned, the IT Department's role is that of a service provider for the 'rest' of the company, and as such, its mandate is to ensure the operational excellence of all the services in place.

As far as BUILD is concerned, the IT Department acts as a partner to the business lines, ensuring that projects are carried out within the scope, budgets and deadlines assigned to it.

Finally, 'vision' places the IT Department in the role of strategist. Its remit is to draw up and implement a strategy for the development of the company's information system and digital technology.

Today, these roles and mandates do not seem to have lost any of their relevance, but a number of factors make it necessary to update this description. These “IT fundamentals” are directly affected by a number of recent changes in the business world.

Key developments

The general context contains factors that explain the transformations affecting the IT Department: the spread of teleworking, the “agilisation” of practices as well as the phenomenon of inshoring (or “backshoring”) and the return to the “local”.

Until a few years ago, information systems consisted of a heritage of applications and infrastructures that were not pooled. Then, these models underwent a gradual hybridization movement, which saw the emergence of a coexistence between the old, so-called “legacy IS” and new service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These new service models, linked to the cloud, are contributing to a major upheaval in working practices, delivery models and IT sourcing. If the changes we are seeing today are more than just trends, it is mainly because the cloud has become so widespread that every company or public authority now uses both the cloud and on-premises solutions[2] .

How do you read this report?

This document is an appendix to the *IT Governance Audit Guide*, published in 2019. As such, it provides useful additions to the successful implementation of IT governance in the light of the latest impacting developments in technology and digital innovation. The structure of the document follows that of the Guide: the vectors are presented one by one, following the order of the Guide. However, several vectors have not been studied this year and may be the subject of future work: “Projects”, “HR”, “Project portfolio”, and “Service providers & suppliers”. Note: whereas the Guide presented four dimensions for each vector (stakes for the company, threats, related risks factors and best practices), this document considers only two elements: new threats and new best practices. It should be remembered that vectors are self-supporting: they can be analysed and 'audited' separately. But they can also be considered as a whole for a holistic analysis of digital governance.

[2] On-premises is defined as the use of a company's own hardware for its own systems and applications, see Cigref report *Cloud Migration Strategies: a structural challenge for companies, 2023 version.*

2 STRATEGY

The Strategy vector was subtitled “Integrating digital issues into the company's strategic plan”. This formulation calls for several comments. First of all, digital is no longer an isolated entity within the company. On the contrary, it is a major challenge for any organisation. Secondly, it follows that the company's strategy must take digital into account. Finally, these developments mean that digital strategy should be seen as a pillar of the company's overall strategy.

The main development is the growing importance of digital in the company's value chains and products. In some companies and business sectors, digital strategy is tending to merge with overall strategy. For all organisations, digital technology is now a key factor in growth, performance and industrial risk. The role of CIOs is evolving towards a regalian role that goes beyond information systems and concerns digital technology in its entirety, covering Information Technology, Operational Technology (IT and OT) and products. Finally, the value of products is assessed in conjunction with their beneficiaries, i.e. the business lines, which implies close collaboration between the CIO and the business lines in support of strategy.

2.1 NEW THREATS

The main threat to the strategy vector is that digital technology is not sufficiently taken into account in the company's strategy, also known as “lack of vision”. Minimising the importance of digital technology, or failing to sufficiently anticipate the risks and opportunities associated with it, would be a major strategic error. The company then runs the risk of disruption or loss of market share. More than ever before, the IT Department needs to provide the company's 'vision' on these issues to enable it to achieve its objectives. This ability to analyse current situations, to look ahead, and to take the right decisions as a result is required not only in the IT Department but also in other parts of the company, from which a number of best practices can be deduced.

2.2 NEW BEST PRACTICES

- ***Digital transformation issues benefit from sponsorship at the highest level of the company.***
  - Digital leaders sit on the organisation's executive bodies.
  - Cross-functional governance (with senior management) and steering bodies monitor the company's digital strategy and translate it into projects.
  - Digital strategy and risk are high on the Board's agenda.

- ***Strategic intelligence is largely carried out within the IT Department and the Business Units.***

The Guide recommended that “the results of monitoring [should] be shared with the managers involved in developing the company's strategy”. This recommendation is still valid, but it should be extended to the whole company.

- ***The strategy is translated and regularly updated into a transformation roadmap and various policies (architectural, cyber, resilience).***
  - This roadmap should demonstrate the company's ability to implement its strategy and integrate new projects as and when required.
  - The digital strategy includes resilience: it is sufficiently flexible to be able to incorporate unforeseen events and react in the event of a crisis of an economic, political, health or cyber nature....

- ***The organisation is starting to think about CSR.***

The company sets up a committee to discuss the measurement of CSR performance. This should enable the company to be prepared in the event of a regulatory or legal obligation to report on the company's CSR performance (as part of the company's extra-financial *reporting*).

3 INNOVATION

At a time when "everything is becoming digital", the desire to "disseminate digital culture and promote innovative technologies"[3] is no longer enough. More and more often, innovation is entrusted to the IT Department, or in any case, it is dealt with jointly, by the same players as technology. The aim of innovation is now to "explore and promote new technologies and digital uses to drive performance and growth". Exploring new technologies and new digital uses are essential to the IT Department's ability to vision and anticipate business developments.

The main developments identified are, first and foremost, work in *labs,* spaces dedicated to qualification, experimentation and exploration (within the IT Department). IT Departments are also encouraging "intrapreneurship"[4] and using Shadow IT as a laboratory for detecting, testing and promoting new uses. The aim is to encourage people to test and explore these technologies. These new methods are driving progress, but they are also giving rise to new threats.

3.1 NEW THREATS

Working in labs is part of an innovation dynamic within the IT Department. However, innovation must not ignore scalability issues, as this would run the risk of confining the IT Department to a playground of exploration that never leads to a product. Value and the ability to industrialise must be taken into account very early on in the exploration process.

In addition, through its labs and monitoring work, the IT Department identifies innovations that can meet business needs. The threat inherent in this abundance of innovation is that of not being able to distinguish between what brings value and what does not. The IT Department, in partnership with the business units, must be able to discriminate between elements that add little value, or are of no interest to the company.

3.2 NEW BEST PRACTICES

- ***Encouraging and supporting digital intrapreneurship***

Shadow IT is no longer seen as a threat in itself. Instead, it is seen as an opportunity for the business, in that it offers users the chance to familiarise themselves with technologies, and potentially make interesting discoveries for the business. Organisations are therefore invited to "organise and manage a space of freedom" with the aim of encouraging digital "intrapreneurship", detecting initiatives that should be generalised (development of processes and tools) and those that should be managed or banned (security or compliance risks).

[3] Innovation vector, *Audit guide*, 2019, p20.

[4] The term "intrapreneurship" is a contraction of "*intra*" and "entrepreneurship". It refers to the possibility offered to employees of an organisation to undertake and innovate within the organisation *itself.*

- The IT Department supports the business units in low-code *to* encourage digital entrepreneurship.

➢ ***Events are organised to promote new digital technologies.***

These events promote a culture of innovation within the company. For example, hackathons.

➢ ***The IT Department works with the business units to organise processes for ideating and exploring new digital uses.***

The role of the IT Department is to control the technology and ensure its reliability, operability and maintenance. The end use of the technology is on the business side. More than ever, the IT Department needs to equip itself with the means to qualify new technologies and anticipate changes. Together with the business, it defines the new uses to be explored. These uses concern the disruption of processes[5] or new product concepts, to support growth. New skills in leading innovation with business units and external partners are now part of the IT Department's remit.

➢ ***The company is setting up a digital factory.***

The IT Department's organisation is moving into "product mode", via the widespread adoption of an "agile" culture[6] . This accelerates transformation as a function of value increments. Ultimately, this approach makes it possible to deal with uncertainty.

[5] Process disruption is the result of a two-stage questioning process: 1: "what if we did things differently?", for example, the organisation chooses to use AI to plan maintenance; and 2: "what if we did something else?", for example, using digital technology to launch a new product.

[6] Agility is defined in the Cigref report *Agile at scale* as a means of "adapt[ing] more quickly to market needs, to identify new reserves of performance, to deliver more value more quickly to their customers as well as attract and retain talent. This agile transformation is scaling up to smooth out the delivery of value from end-to-end, from strategy to execution". According to the same report, organisations are moving "from project mode to product mode to deliver a turnkey product and continuously improve the value it delivers".

4 RISKS

The aim of the Risk vector was to "take into account digital risks in the strategic stakes and business processes". These digital risks covered two areas: technological risks and cyber risks.

In terms of technological risks, the main concern is that of dependencies and "lock-in" (supplier or technological). In terms of cybersecurity, we note that this has become increasingly important, not because attackers have changed their *modus operandi*, but because of the industrialisation of cybercrime and the increase in the volume of attacks.

4.1 NEW THREATS

There are three types of new threat: regulatory, cyber and cloud-related.

The Guide proposed the following best practice: "IS risks should take account of regulatory, legal, contractual and social constraints".[7] In recent years, the **legislative and regulatory landscape** in France, and even more so in Europe, has undergone a number of changes. The impact on the digital sector is significant. In addition to the text of the law, it is the deadlines set for compliance that often put organisations in difficulty. The risk of non-compliance is compounded by a financial risk, as companies incur economic penalties and/or seek expert advice to help them understand the scope of the provisions in question, and the actions they need to take to comply.

Secondly, the main development in cyber risk, already identified in the Guide, is the increase in the volume of attacks. This means that we need to rethink the way we deal with cyber security within the organisation, bearing in mind that protection and response systems evolve more slowly than the threat itself.

Finally, the cloud, and SaaS in particular, entails an increased risk of dependence on software publishers. This is an issue of sovereignty and a new risk of lock-in that needs to be taken into consideration[8] .

These three main threats present companies with a variety of challenges, but they also share a common challenge: the threat of not being able to activate its response mechanisms quickly. It must therefore equip itself with the necessary resources to react in the event of a crisis (cyber, geopolitical, etc.).

[7] Criterion no. 7, Good practice no. 3, Risk vector, *Audit guide...* mentioned above, p31.

[8] On this point, see the "*11 Fair Principles*", drawn up by Cigref with its European partner associations Beltug, CIO Platform Netherland and VOICE.

4.2 NEW BEST PRACTICES

- ***The company implements continuous awareness-raising and the involvement of all players in risk prevention.***

The business units, like the IT Department, are trained to prevent risks, to anticipate them and to react to them when they arise. Cybersecurity and compliance are two significant examples: it's worth remembering that people are the main vector of risk. We can therefore improve risk management by raising the awareness of all those involved in the organisation.

- ***Cyber security is seen as a strategic or industrial risk for an organisation.***

Managing cyber risk is a resilience issue for businesses. The aim is not just to prevent the risk from occurring or to reduce its impact, but *to ensure that the organisation can continue to operate in the event of* a crisis.

5 DATA

For the Data vector, the Guide highlighted an initial good practice, "Data Repository", under which "the company must identify data and manage it as a major corporate asset". This good practice is now an obvious prerequisite for all organisations, which need to go further in their data management. A new formulation is therefore proposed: "The organisation must implement its own data governance, and manage it as one of its major assets".

5.1 NEW THREATS

The Guide recommended that, depending on the issues at stake, "a risk map […] based on the data's criticality (confidentiality, integrity, availability, traceability)" should be put in place as part of the protection of the company's data. This mapping must be updated on a very regular basis, given the rapid evolution of risks.

5.2 NEW BEST PRACTICES

- ***The company has a data strategy.***

This strategy takes into account new technological possibilities as well as technical, legal and regulatory constraints. It begins at the product design stage, and includes consideration of the purpose of the data: will it remain in-house? will it be shared? From the design stage onwards, we need to systematically address access conditions and confidentiality issues, and ensure that applicable regulatory obligations are taken into account.

- ***The company is setting up a "Data factory" type entity.***

This unit is responsible for implementing and managing the data catalogue, standardising data exchanges and managing inter-application flows. It also works on *analytics* requirements.

- ***The business units receive support in managing data and the associated risks.***

The IT Department or the Chief Data Officer may be responsible for increasing the skills of the business units in data management.

- ***The company is implementing a policy based on artificial intelligence.***
  - Use cases for artificial intelligence are currently being identified or have already been identified by the company.
  - A legal and technological watch dedicated to artificial intelligence is carried out.

6 ARCHITECTURE

The Architecture vector is undergoing a number of changes: architecture is becoming more strategic, and is harmonising and evolving with the widespread adoption of the cloud.

The sub-title of the vector, “Aligning IS architecture with strategic challenges”, already suggested a link between architecture and strategy. This link has been confirmed over time: as a service provider, the IT Department ensures the operational excellence of all the services in place. In addition, the Guide recommended that an “organisation [...] be put in place to ensure the application of the reference framework and to manage its development in order to meet project requirements and take account of technological developments”. There has been a change on this point: this organisation takes the form of an overall authority that defines and updates an architectural and technological policy designed to anticipate business developments. This authority updates the company's architectural policy to make it a factor of acceleration and resilience.

The work carried out by Cigref on cloud migration revealed that the massive adoption of the cloud has a particular impact on the Architecture vector:

> **IS architecture in the age of the Cloud**
>
> The provision of tailored cloud services makes it easier for the user to understand, use and upgrade infrastructure and software and take up standard solutions through SaaS mode. The IT architecture becomes more flexible and resilient and can offer “agile” services (“Business as a Service”), leading to innovation and a greater openness to the user ecosystem.
>
> **Extract from the report *Cloud Migration Strategies*, 2023**

The simplification made possible by the cloud is matched by the need to build a resilient architecture. The aim is for this architecture to be solid enough to provide a framework for usage, but flexible enough to adapt to the cloud.

6.1 NEW THREATS

- ***Loss of control, degradation of scalability and performance***

This threat is not new, but the democratisation of access to digital technology and the proliferation of citizen developers are increasing the threat, while at the same time bringing innovation. The main challenge is to make the architecture more systemic and encourage global thinking among the company's players. However, citizen developers create applications without sufficient IT knowledge, which poses problems of data management and script development, and includes a risk of non-

portability during migrations. Their initiatives can open up frontiers that are difficult to control, increasing the risk of data leakage and the challenges associated with Shadow IT.

Generally speaking, poor control of the architecture leads to poor scalability of the IT department, and therefore of the business, and creates security risks.

However, it is impossible to prohibit these initiatives, especially as they have very positive aspects on a number of levels: innovation, corporate culture, business line involvement and improved ideation processes. A number of best practices are therefore needed in this rapidly expanding field.

6.2 NEW BEST PRACTICES

One of the solutions to the risk of losing control of the IS is to ensure the solidity of the foundations and architectural standards. This will enable processes to evolve and new technologies and innovative initiatives to be accommodated. A clear, known policy will also provide a framework for initiatives such as *citizen developers*. In order to establish solid architectural foundations and standards, the IT Department and the business departments need to work together, particularly with a view to proposing an appropriate range of services. On the one hand, this must take account of business *inputs*; on the other, it must integrate cyber risk into all layers of the IS and guarantee the interoperability of components.

- ***A global architectural policy has been put in place and is regularly updated in line with the organisation's strategy.***

It must be validated by the Board, shared and applied to all projects.

- ***One entity is responsible for architectural governance.***

Setting up a “Design authority” or “Architectural authority”.

- ***The architectural policy is flexible and resilient.***

These characteristics of flexibility and resilience are essential in a context of “cloudification” (see *IS architecture in the age of the cloud*).

- ***Uses are managed in such a way as to allow innovation and creativity while preserving the company's security.***

- A charter of good practice is signed by every member of staff to avoid any drifting away from low-code or shadow IT.

7 SERVICES

Several factors are driving the IT Department to review the form and content of its services and service catalogue. Economic constraints are one of them, although they are not new in themselves. On the other hand, the democratisation of access to digital technology, the acceleration of change, and energy, regulatory and geopolitical issues all represent new threats to the services offered by the IT Department, and therefore to the organisation as a whole.

7.1 NEW THREATS

Firstly, the democratisation of digital access and the wealth of external offerings mean that the IT Department has to rethink its catalogue of services and update it very frequently. The cloud amplifies this phenomenon by increasing the availability of external products. This means having to qualify technologies, think about how to make them available, their use and usage rights, their business model and how they are billed to internal customers.

Then, the drive towards digital responsibility is forcing the IT Department to rethink certain aspects of its activities: optimising datacentres, re-evaluating requirements, increasing the lifespan of products and preventing service degradation.

On the regulatory and geopolitical front, companies operating internationally have been made aware of the legal and tax risks incurred in the event of a geopolitical crisis (e.g., international sanctions adopted by the European Union against Russia, disruption of strategic supplies, etc.), which again has an impact on the services offered by the IT Department. One of the questions in this respect is whether it is still appropriate to offer a single catalogue of services, or whether it is preferable to adapt the catalogue according to the subsidiary and its geographical location (and therefore to adapt it to the legal and regulatory constraints of the country concerned).

7.2 NEW BEST PRACTICES

- ***Anticipating changes in offerings. The IT Department steps up its monitoring and qualifies new services/offers.***

The IT Department is setting aside resources to qualify new offerings, particularly SaaS. This means being able to proactively monitor the new offerings available, anticipating the demands expressed by the business. Qualification, which is carried out with the *labs in the* majority of cases, is a decisive stage in assessing the relevance of an offering and, where appropriate, adding it to the catalogue of services.

- ***The IT Department is increasing the frequency with which it adds to its catalogue of services.***

This new best practice should make it possible to avoid direct sourcing by the business lines.

8 BUDGET & PERFORMANCE

The Budget and Performance vector is marked by the accelerating adoption of new technologies. In particular, the development of the cloud is changing the way companies manage their budgets and assess performance. A project to migrate to the cloud is costly and requires a change of model from CAPEX to OPEX. This change affects the very way in which the IT Department presents its budgets and defends them before the company's decision-making bodies. What's more, the cloud is leading to an increase in RUN costs. However, the IT Department cannot put a strain on its BUILD to cope with this increase in RUN, at the risk of damaging its ability to innovate. The search for balance must therefore guide the IT Department in its budgetary management. What's more, the cloud and innovation in general are measured against traditional performance criteria, but sometimes also against new criteria that the IT Department needs to establish.

When the IT Department provides IS services in cloud mode (or more precisely in hybrid mode), it often integrates SaaS services with internally-operated assets. As a result, the IT Department is obliged to rethink the performance and SLAs agreed with internal customers (*i.e.,* the business lines).

Another notable change is brought about by agility and agility at scale, which are reshaping the economic management of IT (see IT Department cost management model).

8.1 NEW THREATS

The first two threats identified in the Guide for the "Budget and performance" vector remain the same: "making poor decisions due to a lack of control over all cost elements" and "not controlling the factors that cause projects to get out of hand". As for the third threat, which has become more acute in recent years, "lack of understanding between different departments within the company", the Cigref report *Levers for reducing IT Department costs* now proposes a number of tools for dealing with it. Here again, the difficulty lies in the speed with which threats arise today: IT Departments therefore need to be highly responsive.

8.2 NEW BEST PRACTICES

- ***Projects are managed on the basis of costs, deadlines, functionality and value.***

The notion of *value* is added to the pre-existing criteria. Agility leads the company to review the frequency of performance appraisals, to take account of value increments. Performance assessment becomes "agile".

- ***Adapting capacity planning to hybrid sourcing.***

This best practice relates in particular to controlling and anticipating changes in TCO. Changes in the cost of services purchased from suppliers do not allow for long-term forecasts.

- ***The sourcing strategy is adapted to changing HR needs.***

The skills required in the IT Department and the scarcity of talent are changing the company's HR priorities. This is not just a human resources issue, since projects - and therefore the company's performance - are affected if a project is not carried out due to a lack of available resources.

These best practices are complemented by recommendations made in several recent Cigref reports[9]*.*

[9] Particularly in terms of agility, digital responsibility and IT cost reduction, see Resources.

9 MARKETING AND COMMUNICATIONS

The Marketing and Communication vector aims to “showcase services and communicate on the technological challenges”.

This part of the IT Department's activity is increasingly focused on trust. Businesses, IT Departments and users are increasingly looking for meaning in the services offered to them and in their own activities. This global trend can be seen on a daily basis in the life of the company, both in terms of attracting new talent and offering the guarantees demanded by its ecosystem.

What's more, marketing and communication must help to 'reassure' the users and customers of the IT Department and the company, not only by committing to compliance with regulations (e.g., GDPR) but also by taking initiatives.

9.1 NEW THREATS

If communication is not sufficiently understood, the threat is the loss of confidence of users and customers of the IS (“internal customers”) and customers of the company (“external customers”) induced by the evolution of cyber risks and by the evolution of practices. Certain new methods, such as agility at scale, may give rise to apprehension. On the other hand, the V-cycle may have seemed more reassuring because it was based on precise specifications. These new methods require a major educational effort: they need to be fully understood if confidence is to be won and retained.

Poor communication also increases the strain on human resources and the difficulty of retaining talent because of the “loss of meaning” associated with their activities.

9.2 NEW BEST PRACTICES

- ***The IT Department is flexible and adaptable in its communications.***

Communication needs to be flexible/adaptable, in other words, it needs to evolve and be rethought as we go along, depending on the company's challenges and the current context.

- ***The contribution of an action or project to the organisation's strategy is highlighted as often as possible.***

Through its missions, the IT Department contributes directly to the organisation's overall objectives. Remembering this is essential if you are to avoid becoming a 'black box' or an 'ivory tower' for end users, two pitfalls that were already mentioned in the 2019 Guide as threats (Threat No. 2).

- Encourage collaboration between the marketing manager and the communications manager.

- ***The IT Department pays particular attention to internal and external attractiveness.***

The quest for meaning mentioned above must be taken into account both in the company's external events and in its internal communications.

- This effort involves the development of support tools: for future employees and partners (external attractiveness), and for employees to retain talent (internal attractiveness).

- ***The IT Department offers to run a community within the company.***

This recommendation complements and goes beyond those proposed by the Guide in good practice no. 3: “Communication within the ISD is organised and regular”.

- Creation of guilds or communities to unite teams around common projects and enable the spread of best practice.

- ***The organisation ensures that all those involved in digital projects are on board.***

This good practice ensures that the business lines are not left behind in the company's digital transformation.

- Internal feedback: the IT Department produces a communication plan and presents it to the business units, which are then responsible for relaying it.
- Creation of the role of Business Relationship Manager (BRM) or Digital Business Transformation Manager.

- ***Digital hygiene practices (cybersecurity) are being promoted.***

Communication is far from being the only solution to cyber risks, but it is one of the tools that can be used to limit the threat. For example, recommend that users change their passwords regularly. (see RISKS)

- ***The company promotes digital responsibility.***

As it will involve many changes to practices within organisations, digital responsibility must be backed up by a major communications effort to raise awareness, build understanding and encourage the adoption of the new practices it will entail.

- Organisation of awareness-raising workshops, such as the “Digital Fresco”, to raise employees' awareness of environmental issues.

CONCLUSION

As a result of the work carried out by the ISD Organisational Modelling working group, it appears that the Audit Guide will need to be updated more extensively in the coming years, drawing on Cigref's other activities. However, we felt that the changes detected merited further investigation before such an update.

For example, the work currently underway on the development of Ops functions will provide food for thought on the governance of digital technology. Similarly, the CSR and HR activities currently underway will provide valuable and necessary input for updating the Guide.

In addition, it will be necessary to continue the analysis of the vectors that were not studied this year, namely the “Projects”, “HR”, “Project portfolio” and “Service providers & suppliers” vectors.

Towards new audit vectors?

The work carried out suggests that new audit vectors should be considered, which could be incorporated into the Guide in its next version.

Firstly, a “corporate social responsibility” vector could appear. The notable change is that the CSR dimension is no longer just one risk among many. At this stage, it already features in a number of good practices. In the future, we will have to address the difficulty of reconciling the company's ambitions in terms of performance and working methods (teleworking) with its objectives of reducing its environmental and energy footprint. CSR is therefore tending to assert itself as an independent entity that can be audited in isolation.

Secondly, the inflation of European and French standards is increasing the compliance requirements that the IT Department has to deal with. Although it is often presented as one of the facets of the Risk vector, it would seem more appropriate to consider it as a “Compliance vector”, which implies a comprehensive approach ranging from anticipation to taking account of changes in standards and their practical application.

Thirdly, we note that a number of factors, such as the growing cyber threat, or the pandemic and the disruption it has caused in working practices, have led to new good practices aimed at being 'prepared' for a crisis of any kind. These elements can be distilled into each of the existing vectors, but they could also be brought together in a Resilience vector.

The fourth and final point relates to the expansion of artificial intelligence, which is currently integrated into the Data vector, but which could eventually justify the addition of a vector in its own right.

Compliance, CSR, Resilience and AI are all areas that need to be explored, not just with a view to updating the Guide, but above all to ensure that organisations are fully involved in their digital transformation.

RESOURCES

Cigref reports on related subjects

Agile at scale: Sustaining and managing the agile transformation to agile at scale, 2023

IT Department cost reduction levers, 2023

Economic and ecological IT management model, 4th edition, updated 2022

New Low Code / No Code development practices: Unlocking value by controlling risk, 2022

CSR policy in IT: Positive contributions made by the IT Department to the company's CSR policy, 2023

Reacting to a massive cyberattack: Managing the consequences of a cyber-crisis, 2023

Cloud migration strategies. A structuring challenge for the enterprise, updated 2023

ABOUT CIGREF

Serving the economic growth and competitiveness of our members, large French companies and public administrations, users of digital solutions and services, through digital success.
Cigref is a network of major French companies and public administrations whose mission is to develop its members' capacity to integrate and master digital technologies. Through the quality of its thinking and the representativeness of its members, it is a unifying force in the digital society. Cigref was founded in 1970 as a not-for-profit association under the law of 1901.

To achieve its mission, Cigref relies on three areas of expertise that make it unique.

Membership
Cigref embodies the collective voice of France's major companies and public authorities on digital issues. Its members share their experiences of using technologies within working groups to bring out the best practices.

Intelligence
Cigref participates in collective discussions on the economic and societal challenges of information technologies. Founded nearly 50 years ago, Cigref is one of the oldest digital associations in France, and draws its legitimacy from both its history and its mastery of technical issues, the foundation of skills and know-how that underpin digital technology.

Influence
Cigref promotes and respects the legitimate interests of its member companies. As an independent forum for exchange and production between practitioners and stakeholders, it is a benchmark recognised by its entire ecosystem.

CONTACT US

www.Cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
Cigref@Cigref.fr


Cigref
SUCCEED
WITH DIGITAL