

AFAI-ISACA · CIGREF · IFACI

IT GOVERNANCE AUDIT GUIDE FOR COMPANIES IN THE DIGITAL ERA

2ND EDITION · 2019 UPDATE

IT GOVERNANCE AUDIT GUIDE FOR COMPANIES IN THE DIGITAL ERA

2019 EDITION

Cigref • Afai-Isaca • Ifaci

STEERING COMMITTEE

Henri d'AGRAIN

Managing Director, Cigref

Pascal ANTONINI

Partner, EY

Chairman of AFAI

Régis DELAYAT

*Previous Advisor to the President for
digital technology, SCOR,*

*Cigref Ex-Vice-Chairman
and AFAI Administrator*

Patrick GEAI

*Previous Transversal IT
Audits Manager, LA POSTE,
AFAI Administrator*

Jean-Louis LEIGNEL

MAGE Conseil

AFAI Administrator

Philippe MOCQUARD

Managing Director, IFACI

Yohann VERMEREN

Partner, KPMG

*Vice-Chairman of IFACI IT
Professional Group*

COORDINATION

Clara MORLIÈRE

Mission Officer, Cigref

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	P. 2
PREFACE	P. 3
IMPACTS OF THE DIGITAL TRANSFORMATION ON COMPANIES AND THEIR IT	P. 5
GUIDE'S UPDATE	P. 8
VECTORS DESCRIPTION	P. 10
BIBLIOGRAPHY	P. 107
GLOSSARY	P. 108
APPENDICES	P. 109

12 VECTORS

FROM STRATEGIC ALIGNMENT TO IMPLEMENTATION
BUSINESS PROJECTS AND COMMUNICATION TO THE ENTIRE COMPANY

1. Strategy

Integrate digital challenges into the company's strategic plan

P. 10

2. Innovation

Spread digital culture and promote innovative technologies

P. 18

3. Risks

Take into account the digital risks (cyber and technological) in the strategic stakes and business processes

P. 26

4. Data

Manage, capitalise and protect company data

P. 36

5. Architecture

Align the IT architecture with strategic stakes

P. 42

6. Project portfolio

Optimise the value of IT and manage its evolutions

P. 50

7. Projects

Control project and solution implementation

P. 58

8. Human resources

Organise and manage talent and skills

P. 68

9. Providers & Suppliers

Steer relationships with providers of digital solutions and services

P. 76

10. Services

Provide digital services that meet client expectations

P. 84

11. Budget & Performance

Steer the IT budget and performance

P. 92

12. Marketing & Communication

Showcase services and communicate on the technological challenges

P. 100

ACKNOWLEDGEMENTS

CONTRIBUTORS · EXPERTS

Gönül BASODA, IT Operations Manager, HARMONIE MUTUELLE
Sylvain BIZOUARD, Internal IT Audit Director, AXA FRANCE
Pierre CALVANESE, Chairman, IGC GROUP
Isabelle CARRE, Internal Audit Director, AIR FRANCE KLM
Frédéric CHARLES, Digital Strategy & Innovation Director, SUEZ ENVIRONNEMENT
Marc DEMERLÉ, Mission Officer, GDPR Corporate IT Referent, ENGIE
Gilles DU CREHU, Risks and Internal Inspections, EDF
Philippe EBERT, Application Technical Architecture Manager, DASSAULT AVIATION
Philippe ELBAZ, Transversal Activities Manager, GROUPEMENT DES MOUSQUETAIRES
Tanguy FOURNIS, CISA, Mission Officer, Internal IT Inspection, SMA Groupe
Sabine GUILLAUME, CIO, METROPOLE EUROPEENNE DE LILLE
Jean-Pascal GUILLEMET, Associate, ERNST & YOUNG
Bruno HEMMATI, Strategic vendor management director, ORANGE
Philippe HERVIAS, Head of IS Audit, SANOFI
David METIVIER, Internal IT Audit and Operations Director, SODEXO
Joel PELCE, Internal IT Risks Audit Inspection Manager, GRDF
Olivier PERNAUDET, Inspector of Armies, MINISTERE DES ARMEES
Marie-Noelle QUIOT, General Inspector of Armies, MINISTERE DES ARMEES
Guy-Pierre RODRIGUEZ, IT Compliance & Performance Manager, GROUPE ADP
Jean-François SZYMCZAK, Senior Manager, KPMG
Olivier SZNITKIES, Head of audit EMEA, LAFARGEHOLCIM
Gilles TROLEZ, Audit and Risk Control Director, CARGLASS
Nicolas VIALLET, SDS/BPERF, MINISTERE DES ARMEES



AFAI-ISACA

WWW.AFAI.FR

The Association Française de l'Audit et du conseil Informatiques (AFAI) is the ISACA's French chapter and is the association of reference for IT professionals.



CIGREF

WWW.CIGREF.FR

Cigref is a network of major French companies and public administrations set up in order to develop its members ability to acquire and master digital technology.



IFACI

WWW.IFACI.COM

The Institut Français de l'Audit et du Contrôle Interne (IFACI) brings together 5,500 internal audit and control professionals and, more widely, all the roles that help control risk.

PREFACE

With the integration of digital technologies in companies, organisations evolve and change both in their strategic and operational approaches. IT is at the core of the company's business, and IT develops and accelerates digital technologies within the company. It supports the company's activity; hence its effective functioning is vital.

Faced with the changes to companies brought about by the digital transformation, IT governance is directly impacted and, as a consequence, evolves to adapt to the new operating methods and opportunities that technology provides.

Companies' IT governance is a steering approach whose purpose is to provide an optimum contribution to value creation, align the digital strategy with the company's strategy, optimise the use of resources and control risks according to the stakes.


Our three associations published the Guide d'audit de la gouvernance des SI (*The IT Governance Audit Guide*) in 2011, but wanted to update it given the changes to companies and their IT. A shared study on the impacts of companies' digital transformation has allowed us to update all the "vectors". The recommendations in this guide are strategic and operational.

It is important to specify that, since this guide covers IT governance, it also covers all the company's activities. Indeed, everyone within the company must control their IT in a transversal way to make digital technology a success in the company. The IT department is one of the key players in IT governance, but it is not the only one. Convergence, objectives among all departments and good teamwork are prerequisites to effective and appropriate management.

Given the impacts listed, the steering committee has suggested a new set of twelve vectors. Some vectors in the 2011 edition have been merged and integrated, and two new vectors were added. The two additional topics play vital roles in the transformation: the culture of innovation and company data management. Creating dedicated vectors seemed obvious given their significance.

Once again, this new version of the *IT Governance Audit Guide* seeks to serve as a concrete tool for auditors, inspectors, IT professionals and, more widely, all employees in companies.

Pascal Antonini, Chairman, AFAI-ISACA
Bernard Duverneuil, Chairman, Cigref
Jean-Marie Pivard, Chairman, Ifaci



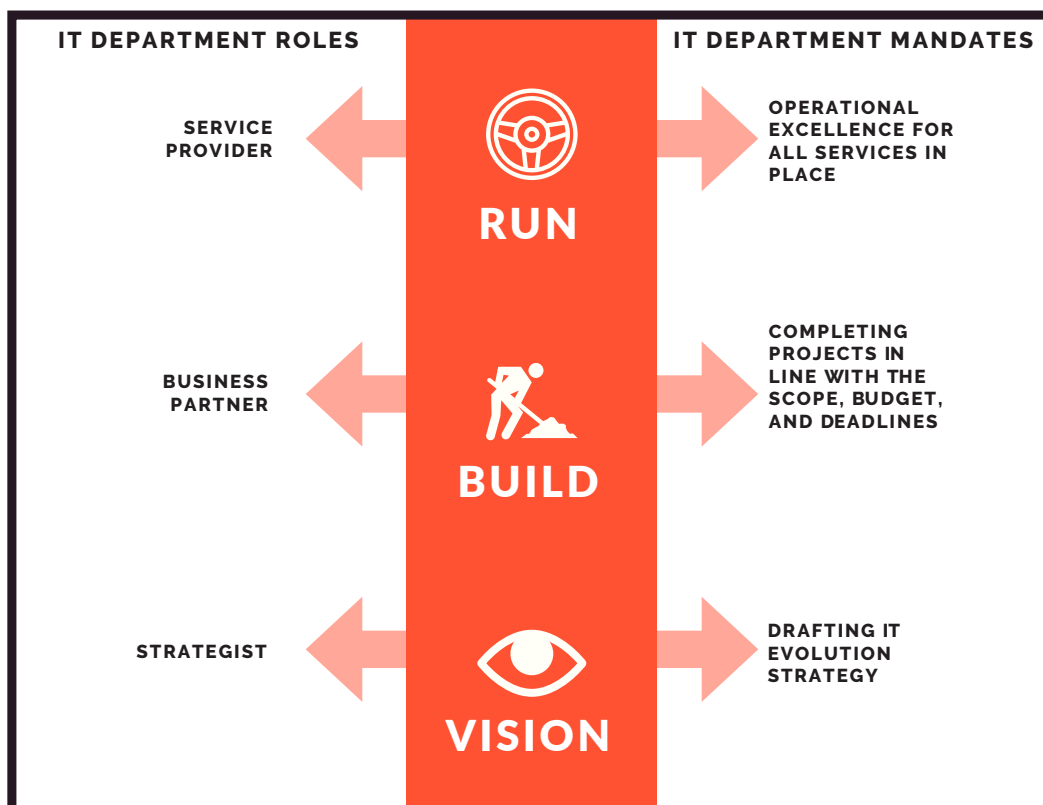
FACED WITH COMPANIES' COMMITMENT TO CHANGE, THE IT DEPARTMENT'S THREE FUNDAMENT ROLES REMAIN THE SAME:

- ▶ **A SERVICE PROVIDER**
Operational excellence for all services in place ('run')
- ▶ **A BUSINESS PARTNER**
Building IT, complete projects within the planned scope, budget and deadlines ('build')
- ▶ **A STRATEGIST**
Drafting IT evolution strategy ('vision')

IMPACTS OF THE DIGITAL TRANSFORMATION ON COMPANIES AND THEIR IT

Faced with companies' commitment to change, the IT department's three fundamental roles remain the same. While these missions are the same, the context, content and resources to perform well and reach these objectives have changed noticeably with companies' digital transformation. The dual revolution of digital technologies and information has had major impacts on companies, their businesses, their employees, its systems and, consequently, on its governance.

The IT department roles and mandates



COMPANIES, BUSINESS UNITS, PROCESSES, EMPLOYEES

MANY TECHNOLOGICAL (ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, INTERNET OF THINGS, ETC.) AND CULTURAL DEVELOPMENTS (USES, AGILITY, BEHAVIOURS) IMPACT COMPANIES' BUSINESS PROCESSES, IN ORDER TO IMPROVE COMPANIES' OPERATIONAL EFFICIENCY AND BUSINESS DEVELOPMENT.

Searching for new business models is imperative and systematic. New organisational models are emerging. Some business units look to outsource their back and middle office processes to focus on their core business using automation and robotic process automation. We are witnessing a total dematerialisation and automation of interactions with the company's ecosystem.

It is essential for companies to strengthen their services to clients to stand out from the global competition. Developing multiple digital services is needed for businesses' competitiveness and characterises the changes to the global economy in France and in the world.

Companies must process the digital transformation's cultural aspect and acclimatise their employees to digital technologies. Many behavioural changes stemming in part from the emergence of digital technology are disrupting business practices, such as the impact of social networks. Companies are rebuilding teams with younger, more digital, more diverse backgrounds.

These profiles can be hard to find and have new expectations in working methods (agility, flexibility, autonomy) which has consequences on their work environment (mobility, desk sharing, remote work) and the alignment of professional and personal tools.

These shifts in business conditions, behaviours and patterns are forcing companies to create a culture of innovation, which is not necessarily natural in companies that are used to allocating expenses/projects based on business cases.

New learning approaches of the Test & Learn type (MVP, PoC, Labs, design thinking, etc.), going from prototypes (Proof of Concept - PoC) to scale project, the introduction of company-wide agility and opening the company to new partners, competitors, start-ups, customers or suppliers, to new community logic, are examples of new practices.

The plethora of internal and external structured and unstructured data is both a challenge and an asset for companies. It must be exploited and protected in an optimal manner. Personal data is a major issue for companies' reputations. Its use must be controlled, and the risk of leaks or theft must always be carefully prevented. Cyber and technological risks have become more severe and are now an issue for the Board

of Directors/Executive Committee. Faced with the increased complexity and number of security flaws, cyber attacks and frauds, strong management and greater steering of security are requirements for all businesses.

Regulators' weight is now paramount, and regulations are a heavy and costly constraint for businesses. This constraint impacts all business units, but particularly the IT department.

THE PLETHORA OF INTERNAL AND EXTERNAL STRUCTURED AND UNSTRUCTURED DATA IS BOTH A CHALLENGE AND AN ASSET



INFORMATION TECHNOLOGY AND IT DEPARTMENT

THE INCREASING GLOBALISATION OF CENTRAL SYSTEMS (CORE IT), CHANGES IN RELATIONS WITH SUPPLIERS, AND EMERGENCE OF NEW PLAYERS (START-UPS) AND NEW MODELS (CLOUD COMPUTING) TRANSFORM IT DEPARTEMENT'S ROLES AND MISSIONS.

The IT department now orchestrates multiple solutions and technologies and faces significant challenges in IT integration and architecture. The IT department becomes an integrator of multiple cloud computing systems.

The company must be agile and react quickly to requests and changes. The IT department must reconcile both of these aspects (Core and Fast) of IT development to take advantage of opportunities to innovate and control the risks of 'shadow IT' and 'shadow development'. Shadow IT puts the company in danger in terms of security and compliance, particularly concerning personal data processing.

At the same time, companies are always seeking to optimise IT's operating expenses to have the resources to invest in development. Furthermore, the evolution of suppliers' business models toward cloud computing leads to a transition of investment spending toward operating expenses (CAPEX/OPEX).

For business services, IT expenses are liable to be rebilled on a 'pay-per-use' basis that allows users to control their consumption.

Given the global shortage of digital talent, IT departments need new hires with and sought-after skills and from more diverse backgrounds. Identifying a strategy for sourcing skills and suppliers is imperative.

IT departments' transparency requirements are stronger (dashboards, communication, service management, cybersecurity, etc.), and they must comply with new regulations such as the General Data Protection Regulation (GDPR), Lemaire and Macron laws on digital technology, and the NIS Directive.

Considering these many changes and transformations for companies, it is important to make sure that IT governance their can handle all of these challenges.

1&2 Glossary p. 108

GUIDE'S UPDATE

The audit guide's goal is to obtain a global vision of companies' IT governance in the digital era. This document and the related tool (see the following chapter) are the first steps before a more detailed IT audit that may require a more complete framework (COBIT). It is a tool to assess the level of mastery of best practices in moving toward continuous improvement for both the auditor and the practitioner. The practitioner can use it for a self-assessment. This IT Governance Audit Guide seeks, above all, to be pragmatic. It is the result of work based on the technical know-how and experience of thirty experts (IT departments, auditors, computer scientists and consultants).

OVERVIEW

This guide breaks down the analysis of IT governance into twelve vectors, from the strategic alignment until the completion of business unit projects and communicating to the entire company. The vocabulary is shared bdy all the functions represented within the three cosignatory associations while preserving their specificities.

THE VECTORS' EVOLUTION

A new set of twelve vectors was proposed. Some vectors in the 2011 edition have been merged and integrated, and two new vectors were added. The two additional topics play vital roles in the digital transformation: the culture of innovation and the company data management. Making dedicated vectors for them seemed necessary given the significance of these issues.

See the following page: the evolution of the vectors between the guide's 2011 and 2019 editions.

STRUCTURE

Each vector is introduced by sections that state the 'challenges and threats to businesses' which could result from insufficiently implementing the best practices related to the vector. Each of the best practices identified relies on a certain number of assessment criteria to audit the quality of their implementation. To make this audit easier, 'related risk factors' were identified as being liable to harm the effectiveness of best practices or even prevent them from being properly implemented. While the vectors are related, each is self-contained so as to be audited on its own.

GOVERNANCE

This guide's update is based on the same methodology and organisation as that used for the 2011 edition which led to its success. Each vector was reviewed by experts from the three associations to take into account the different points of view. We want to thank the three leaders of these working groups: Patrick Geai, Jean-Louis Leignel and Yohann Vermeren as well as all the contributors who were involved in updating this guide.

ASSESSMENT METHODS

Once the vector(s) are chosen and according to the goals and scope of the audit the company wishes to undertake, then the auditor/assessor needs to review all of the best practices that belong to each vector and assess the level of mastery of each of the criteria concerned.

Sometimes, a best practice's criteria give a progression of its mastery level. However, there is no weighting to be applied, and each criterion can be evaluated independently of the others. To evaluate a practice, all of the criteria for the best practice concerned should be examined. It is possible for a criterion to be 'not applicable' to an organisation's environment.

It is up to the auditor/assessor to weight the various best practices and vectors according to the context of their assignment in the audited company. Then, they can judge the overall level of mastery for each best practice and give their assessment for the entire vector. Of course, we recommend gathering proof (documents, dashboards, indicators, emails, etc.) to support the level of mastery identified.

In their final evaluation, the guide user should take care to identify key points of attention and offer a deeper audit if necessary.

Evolution of vectors between the 2011 and 2019 editions of the guide

	2011	2019
Vector 1	IT planning and integration into the company's strategic plan	STRATEGY : Integrate digital challenges into the company's strategic plan
Vector 2	Systems and corporate architecture in service of strategic stakes	INNOVATION : Spread digital culture and promote innovative technologies NEW
Vector 3	Project portfolio management centred on value creation for business units	RISKS : Take into account the digital risks (cyber and technological) in the strategic stakes and business processes
Vector 4	Management of IT risks according to their impacts on business units	DATA : Manage, capitalise and protect company data NEW
Vector 5	Alignment of the IT function with business unit processes	ARCHITECTURE : Align the IT architecture with strategic stakes
Vector 6	Mastery of project completion according to business stakes	PROJECT PORTFOLIO : Optimise the value of IT and manage its evolutions
Vector 7	Provide IT services that meet client expectations	PROJECTS : Control project and solution implementation
Vector 8	Steer outsourced services	HUMAN RESOURCES : Organise and manage talent and skills
Vector 9	IT management control that fosters transparency	PROVIDERS/SUPPLIERS : Steer relationships with providers of digital solutions and services
Vector 10	Prospective management of IT skills	SERVICES : Provide digital services that meet client expectations
Vector 11	Manage and measure IT performance	BUDGET & PERFORMANCE : Steer the IT budget and performance
Vector 12	Manage communication	MARKETING & COMMUNICATION : Showcase services and communicate on the technological challenges

STRATEGY

INTEGRATE DIGITAL
CHALLENGES INTO THE
COMPANY'S STRATEGIC PLAN

STAKES FOR THE COMPANY

1

Enrich the company's strategy with a business-line view of its digital transformation and its future IT.

2

Optimise the IT contribution to the company's strategy by identifying digital and organisational initiatives to undertake in the upcoming years.

3

Integrate technology opportunities, which are increasingly important for business processes, into the company's strategy.

4

Align IT's evolution with the company's strategic stakes by involving General Management and business units.

5

Be ready for the digital transformation that is impacting all companies.

THREATS TO THE COMPANY

1

Lose competitiveness by missing technology opportunities.

2

Lose competitiveness through difficulties in integrating digital transformation projects.

3

Not fully benefiting from digital investments given the company's strategic objectives by not sufficiently anticipating appropriate action plans.

RELATED RISK FACTORS

- 1 A lack of knowledge of the company's strategy.
- 2 A lack of IT adaptation and efficiency.
- 3 A lack of knowledge of the impact of new technologies on the business model.
- 4 A lack of dialogue between the IT function and General Management.

BEST PRACTICES

- 1 Organisation, the planning and transformation process. ✓
- 2 Strategic content, the inclusion of business and technological targets. ✓
- 3 Communication so business units can understand and approve. ✓
- 4 Measure through financial and non-financial indicators. ✓
- 5 Steering the implementation of the IT strategy. ✓

Best practice 1: ORGANISATION.

The IT department is involved in the company's planning and transformation process (strategy, medium-term plan and budget).

Criterion 1

The IT department participates in the development of the company's strategic plan and budget.

- ▶ The IT department ensures that business units consider opportunities provided by new technologies as well as existing IT constraints.
- ▶ The IT department takes full part in drafting the company's strategic plan (the IT department is involved in decisions-making regarding the company's strategic programs in terms of technical feasibility, giving estimates of lead times and costs).

Criterion 2

The results of the company's technology watch (see VECTOR 2 · INNOVATION) are shared with managers involved in developing the company's strategy.

- ▶ For example, these results can be reports to company executives of findings and observations made in technology events for business unit use.
- ▶ Ideas for innovation include new uses, business models, services, processes, etc. in addition to innovation in products and tools.
- ▶ Certain decisions concerning strategic programmes are driven by technological breakthroughs (ex: Internet of Things, blockchain, etc.).
- ▶ The IT department is a driving force in the company planning process by suggesting technological innovations from which the company could benefit.
- ▶ Recommendations made by the IT department relative to innovations are included in the company's strategic plan.

Criterion 3

The IT department has worked with business units to draft the digital section of the company's strategic plan.

- ▶ This digital section is drafted in partnership with business units as part of the company's medium-term planning process.
- ▶ The IT department details the major technical stages (major evolution thresholds) that are prerequisites to the various objectives in the company's strategic plan.
- ▶ The company's particular characteristics (new ranges of services, new markets, internal or external growth, international, acquisitions or refocusing, etc.) are integrated to define the digital strategy's major orientations.
- ▶ All units (service and/or geographic lines) fully involve IT managers (central or local) in their strategy development process.

Criterion 4

The digital section is coherent and included in the company's strategic plan on the same level as other company functions.

- ▶ Since the purpose of the strategic plan is to coordinate the plans of the various functions and allocate the necessary resources to them, the digital section is necessarily a part of it.
- ▶ Budget allocations are consistent with the expected contribution of IT to the company's strategic plan.

Best practice 2: STRATEGIC CONTENT.

The digital section of the company's strategic plan includes the technological and business targets and the planning of resources needed to achieve them.

Criterion 1

The strategic plan's digital section details the covered business targets (processing, functional map) and the main impacts (organisation, skills, technologies).

Criterion 2

The digital section includes evolution thresholds given the business stakes and budgetary constraints (implementation calendar and stages).

- ▶ The thresholds reflect "stable stages" or major milestones in the transformation on which the company can capitalise (implementation of new services, etc.).
- ▶ These thresholds do not prevent the fast changes and speedy development related to digital technologies, for instance.

Criterion 3

The digital section specifies the resources (IT department and business units, internal and external, financial, skills and technologies, etc.) needed to achieve the target.

- ▶ Action plans derived from the digital section that specify the implementation of resources (on the IT department and business unit sides) must be included and approved in the company's strategic plan.

Criterion 4

The digital section identifies the sourcing strategy in order to reach the objectives of the company's strategic plan (human, financial, security, the scope of activity, etc.).

- ▶ It is necessary to specify whether the required resources previously defined in criteria 3 (see above) need to come from internal sourcing (skills development) or if they must be acquired externally (purchasing, partnerships, hiring, etc.).

Criterion 5

The investments resulting from the strategic plan's digital section are in line with the business-expected benefits.

- ▶ The goal here is not to draft a business case but to specify the purpose and business value of the requested investments so that an allocation can be registered in the strategic plan. Investments should then be approved on a case-by-case basis as part of projects.

Criterion 6

The digital section takes into account ethical stakes and corporate social and environmental responsibility issues identified in the company's strategy.

- ▶ Ethics by design, ethics of use and societal ethics.
- ▶ See the framework document from Cigref and Syntec Numérique '[Digital ethics](#)'

Best practice 3: COMMUNICATION.

The digital section is communicated, as part of the company's strategic plan, to raise business units' awareness and improve their understanding.

Criterion 1

The IT department specifies the objective expected of communicating the strategic plan's digital section (sharing, take-up, mobilisation, transparency).

- ▶ A communication plan for the digital section must be drafted as a complement to the communication plan for the company's strategic plan.

Criterion 2

The IT department has identified the targets for this communication (General Management, business unit directors, IT managers, main actors involved in IT, company employees, external stakeholders).

- ▶ The IT department understands the various departments' expectations for IT and digital technologies and shows how its strategy contributes to them.
- ▶ The IT department communicates with business units concerning the areas where it expects close collaboration to successfully complete its plan (i.e. data migration/retrieval, change management, transition management, etc.).
- ▶ For each of these targets, it has identified communication objectives and means to measure their success.

Criterion 3

The IT department has identified the communication resources (content, form, medium, etc.) to reach the identified targets.

- ▶ The content is appropriate for the sought objectives and for each target identified.
- ▶ Methods (frequency, medium, body, audience, discussion communities, indicators, etc.) are specified.

Criterion 4

The IT department implements and leads this communication that was developed in accordance with the most appropriate methods.

Criterion 5

The IT department measures the effectiveness of this communication (indicators, surveys, feedback, polls, etc.) given the initial objective.

Best practice 4: MEASURE.

Financial and non-financial indicators enable the IT department to report on the execution of the strategic plan's digital section to General Management and business unit departments.

Criterion 1

The IT department has identified and approved the various types of indicators so as to cover all of the stakes of the strategic plan's digital section (see VECTOR 11 · BUDGET & PERFORMANCE).

- ▶ For example: investment ('CAPEX') and operating ('OPEX') budgets, human resources planning, major milestones, sourcing, team diversity, IT carbon accounting, etc.
- ▶ See AFAI-ISACA's 'IT Scorecard' report.

Criterion 2

The IT department measures each of these indicators in accordance with a formal operating method (objective, source, frequency, calculation, etc.).

Criterion 3

The IT department analyses the indicators results and their difference from the objectives to implement preventive or corrective actions in a continuous improvement approach.

Criterion 4

The IT department provides General Management with a dashboard that summarised the results of these indicators and the corrective actions implemented.

- ▶ General Management tracks these indicators on a regular basis, as those of other functions (Finance, HR, etc.).

Best practice 5: STEERING.

An IT strategic steering committee is set up at the General Management level to approve the strategic plan's digital section, arbitrate as required and ensure their implementation.

Criterion 1

The company's Executive Committee manages the digital strategy.

- ▶ The Executive Committee decides on the type of organisation for steering its digital strategy and implements required body.
- ▶ The Chief Information Officer should participate in this steering committee.

Criterion 2

This committee's role (approving the digital section, taking decisions, tracking their implementation) is defined and communicated.

- ▶ The committee must be chaired by General Management.

Criterion 3

This committee includes business unit directors, the Chief Information Officer and a representative from General Management.

- ▶ The representative from General Management is the Chairperson or their delegate.

Criterion 4

This committee meets regularly, communicates their decisions and tracks their execution.

Criterion 5

This committee works with operational steering committees organised with business units.

NOTES...

INNOVATION

SPREAD DIGITAL CULTURE AND
PROMOTE INNOVATIVE
TECHNOLOGIES

STAKES FOR THE COMPANY

1

Ensure that the company has the capacity for digital innovation to support its development and competitiveness.

2

Be able to identify and adapt technology opportunities within the company.

3

Communicate on innovation within the company and to decision-making committees.

4

Create the most favourable conditions for developing concrete innovations: technology monitoring, benchmarks, labs, open innovation, start-ups ecosystem.

THREATS TO THE COMPANY

1

Obsolete products or services compared to the competition: loss of market share, reduced ability to raise prices and finance R&D.

2

Harm to company's competitive advantage and image.

3

Lack of HR attractiveness (hiring, departures, turnover, etc.) and of the required skills to confront technological changes.

RELATED RISK FACTORS

1

A lack of organisation adapted to innovation, and of the appropriate skills.

2

A lack of understanding of the company's operations and strategy.

3

A lack of skills in communication and a lack of a body able to evaluate proposed opportunities.

BEST PRACTICES

1

An established global vision shared throughout the organisation.



2

Organisation with a body in charge of the innovation effort.



3

Technology watch that enlightens innovation efforts and strategy.



4

Organisation's speed in analysing innovation initiatives.



5

Communication and performance, evaluating its effectiveness and continuous improvement.



Best practice 1: VISION.

A global vision of innovation is established and shared throughout the organisation.

Criterion 1

The Executive Committee defines and shares its vision of innovation with the company, including its appetite for the risks caused.

- ▶ General Management must encourage employees to surpass themselves and get out of their comfort zones.
- ▶ It must communicate that the company is aware that failure is part of the innovation process.
- ▶ It also regularly communicates on the importance of innovation to the company's long-term success.
- ▶ General Management establishes the appetite for risk inherent in innovation.

Criterion 2

The Executive Committee sponsors and guarantees a culture of innovation.

- ▶ The company implements management techniques and mechanisms intended to create the most favourable conditions for developing concrete innovation.
- ▶ Innovation is the result of transversal work: various departments and teams are involved, and the IT department is consulted as an expert and contributor for issues related to innovation.

Best practice 2: ORGANISATION.

A body coordinates innovation efforts.

Criterion 1

A body in charge of the innovation effort exists with clearly defined roles and responsibilities.

- ▶ The roles and responsibilities for innovation must be defined.
- ▶ This body's mandate is clear and consists of promoting and facilitating innovation. This mandate is formally enacted by and with the strong support of General Management.
- ▶ Suggestions for this body's responsibilities:
 - ▶ Managing the innovation process, alignment with the company's strategy
 - ▶ Selecting innovation projects
 - ▶ Allocating resources
 - ▶ Tracking performance
- ▶ This body can be comprised of IT department or business unit employees and, possibly, outside members.

Criterion 2

Using a Project Management Office (PMO) makes innovation driven by emerging technologies easier.

- ▶ The PMO helps create a secure place that fosters conceptualisation and experimentation by including conceptualisation exercises in the portfolio planning process.
- ▶ The PMO can also reserve a portion of the portfolio for innovation.
- ▶ The PMO works in close collaboration with all stakeholders to involve the right people at the right time.

Criterion 3

The body in charge of the innovation effort organises and tracks the ideas retained.

- ▶ A system is used to collect innovative ideas in the organisation. The initiatives can take the shape of an idea box, digital platform, competition, etc.
- ▶ The body ensures that the right resources are allocated according to the innovation's objective.

- ▶ The innovation effort uses funds that are separate from standard projects.
- ▶ An approach using pilots with a limited scale is adopted to show the innovative idea's potential.
- ▶ When an idea has demonstrated its potential in a pilot, it is selected and joins the portfolio of standard projects.

Criterion 4

An inspection body exists to confirm that innovation projects are conducted responsibly in regards to General Management and the company's technology guidelines in architecture, security and standards.

- ▶ Not only is this to confirm the respect of certain norms but also to raise teams' awareness.
- ▶ These 'inspector-coaches' must represent General Management, business units and the IT department.
- ▶ This also helps avoid allowing a shadow IT to develop.

Criterion 5

Space for innovation (for example, time specifically set aside) is given to employees exclusively for topics of innovation.

- ▶ Create dedicated environments that foster creativity and innovation while ensuring that best IT practices (sandbox, innovation lab, co-working rooms, etc.) and security are respected.
- ▶ Employees are able to dedicate a percentage of their working time or workweek to innovation activities or project development.
- ▶ Centres of Excellence are used to centralise skills and experience, act as depositories of best practices, implement POCs and pilots as well as train employees.

Criterion 6

Actions are organised to encourage working in mixed business unit/IT teams: workshops, project collaboration, learning approaches (e.g. test and learn).

- ▶ The company implements management techniques and mechanisms intended to create the most favourable conditions for developing concrete innovation.

Best practice 3: TECHNOLOGY WATCH.

Organise the technology watch (as well as regulations, environment, ecosystem, etc.) to enlighten innovation efforts and the company's strategy.

Criterion 1

Business intelligence and innovation activities are organised at the company level. They are co-led by the IT department and business units based on a shared roadmap with sufficient resources.

- ▶ This organisation can be more or less formal (strategic partnership between the IT and Marketing departments to identify innovations that could help the company stand out from its competitors).
- ▶ Without needing to be heavily explicit, the 'rules of the game' are clear: the objectives and limits to this watch activity, positioning *vis-à-vis* PoCs and other projects.
- ▶ The IT department and business units identify the risks and opportunities of the main technological evolutions.

Criterion 2

The IT department is part of a business intelligence network within the company that includes other business functions.

- ▶ The IT department participates in global business intelligence to anticipate and incorporate IT impacts.
- ▶ The IT department has selected a certain number of technologies that it judges to be strategic in agreement with business units and where it decides to conduct these activities.

Criterion 3

The IT department has expanded its technology scope to its eco-system by participating in networks outside the company (clubs, organisations, etc.).

- ▶ Experts are called on to give feedback on their experiences and share their knowledge at events organised by renowned organisations in France and abroad.
- ▶ The company participates in changing standards in strategic technical sectors.
- ▶ The information gathered at these events are made available to IT people as well as identified business unit contacts.

Criterion 4

These business intelligence and innovation activities can lead to create proofs of concept (PoC) and demonstrations in order to improve the company's processes.

- ▶ There are technology demonstrations and communication campaigns within and outside the company.
- ▶ Some companies set up 'sandboxes' to encourage innovation. Demonstrations and PoCs are practical applications of these technology watch and demonstrate ideas' feasibility to improve the company's processes.

Best practice 4: ORGANISATION'S SPEED.

The company is organized in such a way as to quickly acknowledge and take actions on innovation initiatives in the given time frame.

Criterion 1

The company is able to muster resources (financial, human, etc.) to complete initiatives and projects within a given time frame.

- ▶ The innovation portfolio is tracked.
- ▶ Initiatives' progress and the use of allocated resources is documented.

Criterion 2

The company has implemented an agile innovation process.

- ▶ Agile methods allow small, cross-functional teams to work in small increments to build and test a product or a feature through a proof of concept followed by, potentially, a small-scale pilot.

Criterion 3

The company anticipated the appropriate legal process to minimise the time to execute the contract establishment process and mobilise external resources.

Criterion 4

Innovation is taken into account in human resource management, in particular in the skills development plan. (See VECTOR 8 - HUMAN RESOURCES)

Criterion 5

The company sets up and organises partnerships with its ecosystem (higher education institutions, incubators, competitiveness clusters, associations, clubs, etc.).

- ▶ The partnerships with its ecosystem allow the company to foster a spirit of innovation and attract talent.
- ▶ See the Cigref publication in French: 'Open Innovation, réponse aux challenges de l'entreprise' (Open innovation, a response to business challenges)

Best practice 5 : COMMUNICATION AND PERFORMANCE.

Innovation is the subject of clearly defined communications, assessments of its effectiveness and continuous improvement.

Criterion 1

Communication on innovation is structured according to an internal and external communication plan. Actions are shared and company's actors highlighted.

- ▶ This communication is established between the various actors and coordinated by the company's communication department.
- ▶ This criterion is in line with the [VECTOR 12 - MARKETING AND COMMUNICATION](#).

Criterion 2

The innovation process's progress and results are shared within the company.

- ▶ The innovation's managing body creates and updates a scorecard to gather and share key innovation metrics.

Criterion 3

Effectiveness evaluation criteria are defined in line with the company's performance needs.

- ▶ These indicators can be defined in quantitative (financial, resources, etc.) and qualitative terms.

Criterion 4

These criteria are analysed to identify the innovation's impact on the organisation, employees, clients and users.

Criterion 5

The various assessment criteria are reviewed by General Management.

RISKS

TAKE INTO ACCOUNT DIGITAL RISKS (CYBER AND TECHNOLOGICAL) IN THE STRATEGIC STAKES AND BUSINESS PROCESSES

STAKES FOR THE COMPANY

1

Include digital risks (technological and cyber) in the company's global risk management and its business risk mapping, and therefore helping make strategic decisions.

2

And vice versa, include business impacts in the digital risk management by considering the severity and probability of these impacts.

3

Reduce the risk factors inherent in using digital technologies that support critical and business processes with regards to the continuous operation and execution of the company's (and business units') strategy.

THREATS TO THE COMPANY

1

A lack of reliability, compliance, integrity, availability and confidentiality of critical or sensitive company information (financial, sales, personal, or strategic data or data related to the company's expertise).

2

A lack of ability for the company to deal with digital risks to major applications, key infrastructure and critical data.

RELATED RISK FACTORS

1

A lack of systematic risk identification and management processes.

2

A lack of communication and discussion with business units and General management.

BEST PRACTICES

1

Digital risks management framework integrated in risk global management.



2

Strategic and business stakes of risks.



3

IT process controls for prevention, detection and reaction.



4

Embedded application controls with business units.



5

Frequent IT controls evaluation in regards to the stakes.



6

Reactions to major incidents implementation of effective and tested processing scenarios.



7

Risks reporting towards the General Management to make the appropriate decisions.



Best practice 1: DIGITAL RISKS MANAGEMENT FRAMEWORK.

The company steers digital risk management by using the company's global risk management framework.

Criterion 1

The company considers risk management as an essential part of the company's governance and includes it in its communication.

- ▶ Internal and external communication from management is carried out on risk management with a clear definition of objectives.
- ▶ Risk management is an integral part of the company's annual activity report.
- ▶ Information, awareness and training programs are provided.

Criterion 2

Top management has implemented a risk management policy and organisation covering all the company's critical processes and integrated it into the business units and IT function.

- ▶ There are ad hoc risk management committees that include participants from business units and the Executive Committee.
- ▶ A risks network that includes all business units is included in the company's organisational chart. The risk network's mission is specified and communicated. The risk network includes a business intelligence section on business unit, IT and emergent risks. A risks expert is appointed within the IT department. A risk management policy document is shared within the company.

Criterion 3

The level of appetite and tolerance for risk is defined and shared with all actors at each level where it is relevant. Risk reduction action plans are coordinated by the risks department or, if not, by the management board.

- ▶ Measurement units and frequency are defined and shared among the entire company.
- ▶ Management has set reasonable thresholds of residual risks for the company and the maximum acceptable financial impact.
- ▶ This system allows us to answer the question: what are the methods to transfer and/or reduce risk?

Criterion 4

The approach in place to identify the main risks includes business units and IT department participants. The latter evaluates the risks to its own processes (projects, changes, operations, incidents, security, data management, etc.).

- ▶ An inventory of risks has been drafted with business units and consolidated. This inventory includes IT risks. It is reviewed annually through interviews. It is regularly presented to management and inspection bodies. The inventory can also base itself on recognised IT risk reference documents (Risk IT Framework, COBIT5 for Risk, ISO 27005).

Criterion 5

The company has risk management steering and tracking tools to help make strategic decisions.

- ▶ There are dashboards for managing technology and cyber risks for the Executive Committee and Board of Directors (see the Cigref publication "[Cybersecurity: Visualize, Understand, Decide](#)").
- ▶ There are databases of significant incidents whose impact on business in financial terms is measured.
- ▶ The analysis and reports of incidents' likely evolution, in frequency and impact, is considered in risk management.

Criterion 6

The IT department considers the priorities set in the risk reduction plan for the IT section of the company's strategic plan.

- ▶ The IT component generally considers aspects such as availability, business continuity, data theft protection, poor project selection, projects that do not reach their objectives, and non-mastery of technologies that the company could need to grow and remain competitive.
- ▶ Risks regarding integrity and confidentiality criteria must also be evaluated and reviewed periodically.

Best practice 2: STRATEGIC AND BUSINESS STAKES.

The IT department identifies and evaluates digital risks in conjunction with General Management, the risks department and business units in consideration of the company's key stakes.

Criterion 1

The scope of IT risk analysis relies on the scope of business processes identified as critical for the company.

- ▶ The following are generally taken into account: applications that support key financial flows (accounting, consolidation, and reporting systems), invoicing systems (purchase, order and stock management), transversal repository management applications (clients, contracts, etc.), user access management applications, critically confidential applications, applications considered as 'core business'.
- ▶ Special attention is paid to personal data processing.

Criterion 2

The IT department inventories the IT resources that support business unit processes identified as critical. The risks are evaluated in terms of frequency and impact, and are compared to the risk tolerance threshold for the supported business process.

- ▶ Resources include applications, servers, infrastructure and the key roles associated with them.

Criterion 3

The company has defined a list of "key data" or "master data" with the IT department and business units and identified them as such in a single data dictionary. (See VECTOR 4 - DATA)

- ▶ Knowing which data is considered "sensitive" allows a company to adjust its risk management approaches.
- ▶ This includes the processing of sensitive data (implementing traces, conservation, period review of access rights, etc.).
- ▶ For example, banking data can be considered as sensitive data, and a specific inspection system should be set up.

Criterion 4

The IT department takes into account changes in the internal and external organisation of the company (mergers, new businesses, new locations, etc.).

- ▶ When an information system is being integrated or coming under management, the technical reference framework should be redefined or aligned on the existing framework.
- ▶ Regular meetings with business units are set up to take these changes into account.
- ▶ Business unit requests are formalised, and the IT department creates reorganisation plans and updates service level agreements to take them into account.

Criterion 5

Events that have or may occur (threats) with a frequency and potential negative impact that are sufficiently significant for the company are identified. The events that have occurred are archived.

- ▶ Incident databases are set up to trace and list major incidents.
- ▶ A monitoring system is in place to anticipate emergent risks (online security monitoring, emergent business unit risks, etc.).
- ▶ An SOC (Security Operation Centre) supervises information systems to provide real-time tracking and protect against cyber attacks.

Criterion 6

Risk scenarios are identified from the events then categorised into IT risk families.

- ▶ An application can be made unavailable due to a variety of events such as a communications disruption, fire at the processing centre, or a server breakdown.

Criterion 7

IT risks take into account regulatory, legal, contractual and social constraints.

- ▶ The main regulatory constraints to consider are the General Data Protection Regulation (GDPR), the transposition of the NIS directive, tax and legal archiving, SOX if required, sector regulations (Basel 2, Solvency 3, Healthcare, Pharmaceutical, etc.).

Best practice 3: IT PROCESS CONTROLS.

The IT department has implemented controls systems for IT processes to reduce cyber risks in accordance with business units' constraints. These systems include preventive and detection controls as well as appropriate reaction capabilities.

Criterion 1

The IT department has identified and implemented a reference document of risk controls objectives through an IT process approach (COBIT or other).

- ▶ COBIT, distributed in France by AFA-ISACA, is a recognised reference of IT governance and management in terms of inspections, value creation, and IT risks through a process-based approach (examples of COBIT processes: Optimise risks, manage programmes and projects, manage the identification and building of solutions, manage changes, etc.).

Criterion 2

The IT department identifies its key controls to prevent and detect digital risks and react in case of an incident and rebuilt the information system.

- ▶ The goal is to have a reference of key controls, including general IT controls.
- ▶ Examples of key controls: an IT access management procedure, logging mechanisms for IT activity and log reviews, change management procedure, etc.
- ▶ Audits are conducted independently, particularly for critical projects and cyber stakes.

Criterion 3

The IT department formalises its key controls by applying the inspection documentation template defined by the company (i.e. risk department).

- ▶ These models are used to provide standardised classification and descriptions throughout the company.
- ▶ The various domains such as infrastructure, the network, data, etc. are to be considered.
- ▶ This approach should consider if automated controls are relevant compared to manual inspections to optimise processes and reduce residual risks.

Criterion 4

The IT department regularly studies projects that can reduce IT risks significantly. These projects can be proposed for inclusion in the IT plan with other projects, the arbitration to be done in conjunction with the business units.

- ▶ For example, a project to save critical data in real-time can help reduce disruption to business activity by allowing for a fast recovery in case of an incident. It is up to the business units, risks department and General Management to decide if the additional costs under consideration are acceptable given the impact of the interruption of business.

Criterion 5

When implementing application controls (new or adjustments), the IT department ensures that the tests of their effectiveness are carried out and communicated.

- ▶ The tests are specified, communicated to stakeholders, tested and validated.

Best practice 4: EMBEDDED APPLICATION CONTROLS.

The IT department, in conjunction with business units, takes into account controls embedded in applications.

Criterion 1

The controls embedded in the applications are identified and documented.

- ▶ The inspections repository includes embedded controls. These are described as for all controls.

Criterion 2

The controls embedded in the applications are tested and effective.

Criterion 3

The business unit, as data owner, remains responsible for the data it processes and shares responsibility for controls, be they manual or automated, with the IT department. (See VECTOR 4 - DATA)

- ▶ Everyone should keep their level of responsibility for manual or automated processing. The business unit keeps a share of responsibility even if the control is automated by the IT department.

Criterion 4

The controls embedded in the applications are analysed starting in the project design stage (application or infrastructure) to optimise control of the business process and strengthen internal controls ('Control by design').

- ▶ There are several types of embedded controls: access controls and task separation, system configuration, configuration of exceptional statuses or event reports (IPE, Information Produced by the Entity), interface controls.

Best practice 5: IT CONTROLS EVALUATION.

The company performs regular evaluations of the effectiveness of IT controls regarding the strategic, financial, business, regulatory, industrial or innovation stakes.

Criterion 1

The relevancy of the key controls identified, whether automatic or manual, must be evaluated and justified.

- ▶ The number of key controls should be appropriate for the organisation.
- ▶ These controls should be integrated into the processes.

Criterion 2

The evaluation of residual risks is based on tests of the effectiveness of key controls within the major IT function processes such as logical and physical security, managing operations, managing development, and managing change.

Criterion 3

Key controls must be evaluated by teams independent of the operations under evaluation.

- ▶ In this regard, certifications from independent firms are expanding, in particular for cyber risks (cyber-resilience) as well as around the concepts of companies having critical infrastructure called OIV (*Opérateur d'Importance Vitale* - Operators of Vital Importance) and OSE (*Opérateur de Services Essentiels* - Operators of Essential Services) in France.

Criterion 4

The IT department tracks the implementation and effectiveness of key controls.

Criterion 5

The documented evaluation includes recurring controls of surveillance identified with business units.

Best practice 6: REACTIONS TO MAJOR INCIDENTS.

The company is able to react effectively and within the set time to major incidents with a significant impact for the business unit.

Criterion 1

The crisis management plan is formalised and maintaining in operational condition. It must be connected to the business continuity and business resumption plans.

- ▶ A crisis plan review campaign is conducted regularly.
- ▶ We must distinguish between business continuity and business resumption plans as well as IT continuity and IT resumption plans, which do not concern the same actors (Business units/General Management and the IT department).
- ▶ Make sure that each of these plans is maintained in operational condition.

Criterion 2

The trigger conditions are defined and approved according to the type of event or incident.

- ▶ For example, a loss or theft of data, destruction of the information system, intrusion, or natural or industrial catastrophe.

Criterion 3

The processing scenarios are defined, approved, and tested regularly.

- ▶ The reaction and decision-making structure for confronting major incidents is regularly implemented.

Criterion 4

A review of major incident management is done, shared, and communicated.

- ▶ General Management's review confirms a commitment towards risk management by assigning the authority and responsibility to the appropriate levels of the company and ensuring that the necessary resources are allocated to risk management.

Best practice 7: RISK REPORTING.

The risk steering stakeholders share their risk exposure to General Management so it can make the right decisions within the right timeframe.

Criterion 1

IT risks are reviewed regularly in conjunction with the review of business unit risks.

Criterion 2

Controls review actions are organised in conjunction with the internal control reviews within the business unit processes.

Criterion 3

Reduction plans are established in conjunction with the evaluation of risks and business stakes, tracked by the risk department and steered in coordination with the business units.

- ▶ Set up additional inspections or adjust existing ones (design/formalization).
- ▶ Share objectives and the controls methods to put in place ahead of time.

Criterion 4

The company has risk indicators that highlight the events or situations that can have significant negative impacts on the business function.

- ▶ These indicators easily warn of events and situations, measure the impact, and the upwards or downwards trend.
- ▶ For example:
 - ▶ Project risks: needs not approved by management, deadlines not respected, lack of project risk tracking, etc.
 - ▶ Compliance risk: deliverables or release approval procedures not respected, deliverables not published, etc.
 - ▶ Security risk: server unavailability rate, number of major incidents per application/infrastructure, number of malicious external acts (viruses, hacking, etc.), number of weak passwords, number of restoration tests performed in the year, number of external audits, number of generic accounts, number of accounts with several incompatible functions, etc.
 - ▶ Internal inspection risk: user satisfaction levels, number of production releases not connected to a work order, number of urgent, non-standard changes (change to production data), etc.

Criterion 5

Regular reports to managers are made to track the main risks and appropriate decisions that could be evaluated during internal audits.

DATA

MANAGE, CAPITALISE AND
PROTECT COMPANY DATA

STAKES FOR THE COMPANY

1

Manage data as a strategic asset for the company.

2

Leverage data to develop new projects and services.

3

Give the company a competitive advantage by standing out from the competition.

4

Develop trust in the company's use of collected data (internal and external).

THREATS TO THE COMPANY

1

Harm to reputation and image.

2

Systems blockage.

3

Loss of systems control and management.

4

Financial costs and/or lower turnover.

RELATED RISK FACTORS

1

A lack of organisation and skills to align data knowledge, strategy and business operations.

2

Insufficient internal control system to ensure data protection (non-alteration) and compliance to regulations.

3

Data loss or leak (theft, involuntary leak, intrusion, sabotage, etc.).

BONNES PRATIQUES

1

A data repository to manage them as a major asset.



2

Capitalisation, data use to create value for the company.



3

Security implemented to protect data.



4

Regulations concerning data are respected.



5

Ethics on the actions taken for creating sustainable digital behaviour.



Best practice 1: DATA REPOSITORY.

The company must identify data and manage them as a major company asset.

Criterion 1

There is a coherent data use strategy.

- ▶ This strategy concerns all types of data from strategic data, sales data, industrial data, personal data to critical data.
- ▶ Data use issues are included in the digital section of the company's strategic plan (see VECTOR 1 · STRATEGY).

Criterion 2

The company creates and maintains a repository of important data for the company, specifying the applications that use them, access policies, the duration of conservation, the required level of security, etc.

- ▶ A repository is an inventory of data representing an object (client, organisation, product repository, etc.) and the characteristics and relationships between them.
- ▶ The description of business unit processes includes a data map.

Criterion 3

Reference data (used by several business unit applications or processes) is identified, and the risks of conflicting updates by the various applications are highlighted.

- ▶ If it exists, the data dictionary should specify the data's master application and/or identify any conflicts or duplicates with other applications.
- ▶ The dictionary defines each key data for the company (structured and unstructured data).

Criterion 4

The data dictionary is shared and understood by the business units and the IT department: the data owners are identified, and the data is categorised according to security and regulatory compliance.

- ▶ The dictionary is used to list sensitive and critical data to meet regulatory (CNIL/GDPR/Solvability 3) and security constraints.
- ▶ The roles and responsibilities of dictionary managers have been identified.
- ▶ Examples of actors: the Data Protection and Chief Data Officers as well as the IT department and functional and technical administrator.

Criterion 5

There is governance of the use and update of the data repository and dictionary, and it includes all of the parties concerned (business units, functions).

- ▶ A comitology (a set of committees) has been set up with all stakeholders (data repositories and dictionaries). With a regular frequency as part of a continuous improvement approach. These committees' minutes are traced.

Criterion 6

An inspection is held to check that data repositories and dictionaries are used in new projects.

- ▶ All new projects use the data dictionary and inform the managers — for example, the project committee or systems architect.

Criterion 7

The company expresses and implements processes to verify data quality.

- ▶ Possible data quality criteria: Traceability/Integrity/Freshness (regularly updated) /Exact/Duplication/Exhaustiveness/Coherence/Availability, etc.

Best practice 2: CAPITALISATION.

Data is used to create value for the business (new business units and/or optimisation).

Criterion 1

The company has created the competencies for data use (Chief Data Officer, Data Privacy Officer, Data Scientist, Data Manager, Project Manager, etc.).

- ▶ Job or role descriptions are available.

Criterion 2

The company has implemented initiatives or tools to capitalise on data.

- ▶ Examples of tools: data lakes, big data, analytics, machine learning, business intelligence and customer relationship management, etc.
- ▶ The initiatives and tools concern both structured and unstructured data.

Criterion 3

Company departments know of these initiatives and tools and make use of them.

Criterion 4

Business units use these tools and skills in their operations and projects, particularly for innovation.

Criterion 5

Use of these initiatives and tools is measured periodically.

Criterion 6

Data is used to anticipate events and make projections.

- ▶ Predictive models are created based on the data used.

Criterion 7

Companies who are required to make certain data available as open data (in compliance with the Lemaire law) have identified the impacts on the capitalisation of their data.

- ▶ Verify that there is a formalised analysis of the impact on the company's business.

Best practice 3: SECURITY.

The company has put in place a data protection system.

Criterion 1

According to the stakes, a risk map is based on the data's criticality (confidentiality, integrity, availability, traceability).

- ▶ There is a risk management methodology that is known and shared by the company.

Criterion 2

Risk coverage systems are put in place according to the criticality and the assessment of the threat to data (see VECTOR 3 · RISKS)

- ▶ There is an action or remediation plan.

Criterion 3

The company raises awareness among employees, including General Management, of data protection and risk coverage systems.

- ▶ There is a communication plan.

Criterion 4

The 'data aspect' is integrated into the company's business continuity and resumption plans.

Criterion 5

The company considers security aspects when using cloud computing (data ownership, contracts, the type of cloud, data criticality, reversibility, auditing, data location, etc.).

- ▶ These measures also concern sub-contractors.

Best practice 4: REGULATIONS.

The company seeks to comply with data regulations that apply to its business (GDPR, BCBS 239, NIS, LPM, Solvency 3, e-privacy, etc.).

Criterion 1

The company has identified and manages its regulatory obligations.

- ▶ This means verifying the sustainability and management over time of regulatory obligations (legal and contractual aspects, management of sub-contractors, personal consent, technical implementation, crisis management, inspection points, information campaigns, personal data protection management, request management portal, etc.).

Criterion 2

The company has put in place a system to meet new regulatory obligations.

- ▶ Project management is set up to create a governance framework for new regulations. If possible, the company relies on the company process map.

Criterion 3

The company has implemented compliance inspections for regulations.

- ▶ The company establishes inspection plans (internal inspections and risk management) and can identify the impacts of regulatory obligations on its processes.
- ▶ The system inspects both existing and incoming data (especially customer data).

Best practice 5: ETHICS.

Beyond the regulatory framework, the company values the actions taken in favour of responsible digital technology.

Criterion 1

The company makes commitments to its ecosystem (customers, employees, suppliers and partners) through a data use charter.

- ▶ Legal, IT, and business units participate in drafting the charter. General Management approves it and ensures it is applicable.

Criterion 2

The company trains and informs its employees, including General Management, of the data use charter.

- ▶ The communications department can be contacted for copies of the charter.

Criterion 3

The company checks that the charter has been implemented properly within the company.

- ▶ Check that communication media exists and that the charter is accessible. Respect for the charter can be inspected through questionnaires or training results, for example.
- ▶ The company can appoint a manager for rolling out this charter (for example, the Data Privacy Officer or Ethics Manager).

Criterion 4

In managing its data and hardware, the company measures and considers its environmental costs and seeks to reduce its environmental footprint.

- ▶ For example, concrete actions to save energy in data centres, optimise printing, purchasing and recycling hardware, raising awareness among staff, etc.

Criterion 5

The company communicates on the best ethical practices put in place.

- ▶ The company verifies that a corporate social responsibility -oriented communication plan is in place and that standards are met, possibly even applying for certification.

ARCHITECTURE

ALIGN IT ARCHITECTURE WITH STRATEGIC STAKES

STAKES FOR THE COMPANY

1

Make the IT section of the company's strategic plan a reality in business unit processes to encourage management's involvement and maximise the chances of reaching the targets set.

2

Identify the trajectory and main steps to reach the strategic plan's IT target considering the resources and investments required for each of them.

3

Provide an architectural framework to the project portfolio to make sure it helps reach the IT target.

4

Reduce IT costs and increase its adaptability through streamlining, simplification, encouraging the reuse of features, and taking advantage of opportunities to outsource services.

THREATS TO THE COMPANY

1

Not reaching the strategic target due to a poor resource (finance, organisation, skills, etc.) identification or planning.

2

Not taking advantage of innovations, offers of products and services and technology opportunities.

3

Incur extra costs and limit IT's ability to evolve through a lack of streamlining or increased complexity.

4

Expose the company to security incidents and non-compliance (CNIL, GDPR, traceability, etc.).

5

Lose control of the information system (for example, widespread 'shadow IT', uncontrolled use of cloud computing and SaaS offers, etc.).

RELATED RISK FACTORS

1

A lack of knowledge of the company's strategy.

2

A lack of communication and coordination between the IT department and business units.

3

A lack of required skills within the IT department and business units.

4

A lack of organisation and methodology needed to manage IT.

BEST PRACTICES

1

Mapping of application, data, flows and infrastructure.



2

IT roadmap breaking down the company's digital strategy.



3

Core IT et Fast IT cohabit with the integration of multiple cloud computing systems.



4

Communication with business units to share challenges, stakes and impacts.



5

Rules and principles of architecture with application conditions.



6

Architectural governance based on a reference framework taking changes into account.



Best practice 1: MAPPING.

List the applications, infrastructure, data and data flows between applications. Connect this IT map to the company's business unit processes and update it during projects.

Criterion 1

The IT department maintains maps of applications (catalogues of applications and services), technologies (infrastructure and technical components) and data covering all IT. They are updated during projects.

- ▶ Maps are only beneficial if they are used for operations. It is vital that they be correct (i.e. maintained), that they contain relevant information (particularly the links between the various components ([see criterion 2](#))), that they and the tools used to manage them be as widely accessible as possible.
- ▶ Means to judge the maps' quality must be put in place alongside them. 'Liveliness' indicators are in place to measure the effective use of the map and the relevance and accuracy of data.
- ▶ In particular, maps should always be used in the impact analysis for any IT changes (applicative or infrastructure project).

Criterion 2

Maps highlight the connections between the various components listed: the application data's connections, flows between applications, applications' connection to the technical components used, the link between technical components. They are also links to business unit processes.

- ▶ The flow descriptions should detail the technical protocol or solution, the key data exchanged and the exchange's direction.
- ▶ The description of the links between the various components should be updated regularly to remain beneficial. For this, avoid static versions like PowerPoint files that are difficult to update in favour of dynamic versions. For example, a dynamic model with centralised descriptions of applications and their dependencies in the same database of components of several types (designed from a meta-model) will allow for an appropriate vision for each of the IT department's functions (design, operations, support, etc.).
- ▶ The description of business unit processes includes a data and processing map.
- ▶ The application and technical maps show the connections to the data repository ([see VECTOR 4 - DATA](#)). The maps must describe the ends of maintenance/support for hardware and software architecture components.

Criterion 3

The maps are made consistent with the business unit processes through tools that make it easy to find connections between the users, processes, and IT component, and to classify these according to their criticality for business units.

- ▶ Certain tools offer an approach based on the process maps to which we then attach the IT components.
- ▶ The process description should also be as independent as possible from the organisation (describe 'roles' instead of 'users').

Criterion 4

A process of creation, maintenance and communication of maps involving all stakeholders is formalised and in place.

- ▶ The maps can be managed by specialised tools to make them easier to use and maintain and to connect to other repositories (i.e. processes).

Criterion 5

The organisation in charge of developing, maintaining and communicating the various maps is defined.

- ▶ In principle, the responsibility for maps management lies with the team in charge of the IT architecture, which ensures that they are aligned or converge with the information system with the architecture repository.

Best practice 2: IT ROADMAP.

The digital section of the company's strategic plan is translated into an IT roadmap or blueprint that is based on the map, systems architecture schema and the organisation of data.

Criterion 1

The IT roadmap describes the 3-5-year target organisation for the various IT functions and the connections between them to reach the objectives of the strategic plan's IT section. IT managers and business units are aware of it.

- ▶ The systems architecture schema summarises (often as an 'outline') the target position of the main IT components according to a structure and level of granularity consistent with those in the data dictionary and process map.

Criterion 2

The maps describe the current and target position of each of the map's components compared to the systems architecture schema.

- ▶ It should specify if components with a discrepancy should be adjusted, replaced, or simply decommissioned.

Criterion 3

The IT roadmap details the projects to align IT with the company's strategic plan with roadmaps for components in discrepancy.

- ▶ The impact of discrepancies on reaching strategic objectives is evaluated to justify the investments needed to reach the target IT.

Criterion 4

The IT roadmap is updated at least annually to take into account technological, strategic and regulatory evolutions.

- ▶ The changes should be limited and justified with a medium- or long-term approach.

Best practice 3: *FAST IT*.

The IT roadmap provides an architecture that allows Core and Fast IT to exist together and integrate multiple cloud computing systems.

Criterion 1

The IT roadmap defines the target scopes and interactions between Core IT and the various Fast IT applications.

- ▶ Since Fast IT does not have the same constraints or objectives as Core IT, it is important to set the boundary between the two to be able to manage them separately when necessary.

Criterion 2

The IT roadmap integrates external cloud-computing components (SaaS, PaaS, IaaS, etc.), for example, by means of internal platforms.

- ▶ Using an EIP-type exchange platform (Enterprise Integration Platform) allows IT to control all the types of flows exchanged between the internal IT and cloud computing solutions, not just from a service performance or quality point of view (load decoupling) but from a security (stronger authentication, flow encryption) and maintainability (single standardised point of passage for reversibility, [see criterion 3](#)) standpoint.

Criterion 3

The reversibility principles of external cloud computing components and the related architecture rules are defined.

- ▶ By design, cloud computing introduces a potentially strong dependency on an outside supplier that must be limited from the contract and design stage of the cloud computing service's integration with the internal IT (see [criterion 2](#)).
- ▶ There are means to detect and avoid structurally captive cloud computing offers (proprietary offers in SaaS mode that manage the company's repositories).

Criterion 4

Recurring dependencies in the support and operations chain (including maintenance) are taken into account in the technical and contractual levels. Any technical dependencies are also taken into account.

- ▶ The IT department should avoid connecting technical operations between different cloud computing services since this is unmanageable in practice.

Best practice 4: COMMUNICATION WITH BUSINESS UNITS.

Explain and share architecture challenges with simple vocabulary and with explanatory diagrams. Involve business units and give them the responsibility to help them choose investments by identifying impacts on their business processes.

Criterion 1

The architectural principles and rules describe the underlying business unit impacts and the related benefits and risks (performance, robustness, impact on operating efficiency, the IT use cost, time to market, etc.).

Criterion 2

The analysis of existing IT solutions' and projects' compliance with the architecture reference with an explanation of the impact of discrepancies is shared with business units.

Criterion 3

IT architecture objectives are included when communicating the strategic plan's digital section to business units.

- ▶ Architecture objectives must be aligned with the strategic business stakes.

Criterion 4

Business units are made aware of the architectural stakes and challenges via communities that meet regularly: the constraints, risks, and key factors of success in implementing the various technologies and the impacts (short- and long-term) of not applying principles and rules are explained.

- ▶ Educate on the architectural stakes and challenges through concrete, innovation-fostering use cases related to business stakes.
- ▶ Share project feedback with business units highlighting the risks, strengths and limits of the technologies used or the architectural principles applied.

Best practice 5: RULES AND PRINCIPLES.

The architectural rules and principles are formalised with application methods appropriate to the stakes and risks. They allow for previously developed components and functions to be reused systematically. They are a framework for project teams to use as a basis.

Criterion 1

The IT department has established a set of principles, standards, technical standards, procedures and rules for implementation and use combined with services that take advantage of technological innovations while considering the constraints of legacy systems.

- ▶ The framework, also referred to as a "technical reference framework", is updated during projects (in particular when it is not applicable or incomplete) and based on technology monitoring (definition of the scope of application of new technology, an update related to an obsolete technology).

Criterion 2

Architectural rules provide areas of freedom to promote time-to-market and innovation while limiting the risk of losing control of the IT (security, resilience, maintainability, compliance, etc.).

- ▶ More than rules as such, it is about leaving the possibility of deviating from the rules in particular contexts (according to precise criteria).

Criterion 3

Previously developed functions have been identified as reusable. They are duly noted so that new projects can easily include them in their developments.

- ▶ A good practice is to create and maintain a dictionary of reusable services and set up service governance to determine the service reusability requirements from the outset.

Criterion 4

This framework is known, accepted and applied by all the stakeholders (the different components of the IT departments and business units involved in the projects).

- ▶ The framework must be kept up-to-date and easily accessible (Intranet + search engine) by all project stakeholders.

Criterion 5

This framework is regularly updated, and changes are communicated to all stakeholders, including the impacts of developments on legacy systems.

- ▶ Repository changes take into account their impact on legacy systems. Using maps ([see best practice 1](#)) helps to measure this impact and target adjustments of migrations of the software base to the future standard.

Criterion 6

Applying and changing the architecture framework is supervised and inspected by IT department management. The architecture repository's compliance is an indicator on the IT dashboard.

Criterion 7

A general policy approved by IT department management governs changes to and the application of the framework: description of the life cycle, the operation of decision-making bodies, deliverables and related quality control procedures.

- ▶ Ideally, the framework update process should be defined and integrated with architecture and project governance to make it easier to implement.

Best practice 6: ARCHITECTURE GOVERNANCE.

An organisation is in place to ensure the reference scope is applied and guide its evolution to meet projects' needs and take into account technological developments.

Criterion 1

IT governance allows It department to control the application of rules and principles at all stages of the IT solution lifecycle.

- ▶ This inspection is carried out as soon as the solution is defined (alignment with the IT architecture schema), at the various stages of initial implementation projects (respect of the frame of reference), during maintenance (obsolescence management) and when decommissioning solutions.
- ▶ Monitoring at the various stages of the life cycle also makes it possible to use our experience to validate or invalidate the framework and to make changes if necessary.

Criterion 2

An organisation and governance are in place to study and approve the changes to the architecture repository, taking into account feedback, new project needs and changing technologies.

- ▶ The resources are specific to each company's organisation.
- ▶ It is absolutely essential to ensure that the framework's evolution and application correspond to a transversal global optimum that includes multiple factors: the cost of applying the standard, supporting suppliers for the technologies used (at least for critical applications), the ability to deploy and use the technical prerequisites that projects need, the benefits of the new standard's technological contributions, etc.

Criterion 3

Understandable criteria accepted by all stakeholders (business units and IT) are identified to adjust the architecture's level of support and inspection for each project.

- ▶ The architecture objectives must be formalised based on the project's business unit objectives. They are tracked in the same vein as business unit objectives throughout the duration of the project.

Criterion 4

The project portfolio steering process inspects the continuous application of the architecture's frame of reference.

- ▶ An indicator of projects' alignment with the frame of reference is defined and tracked at the project portfolio level (see criterion 6). Related objectives are set and tracked (minimum project alignment level, global level of IT alignment to be reached, etc.).

Criterion 5

An IT obsolescence management process ensures that all IT components comply with the obsolescence management rules defined by the architecture. It also defines the remediation plans to be implemented in case of discrepancy.

- ▶ Managing obsolescence is an important issue for IT durability and cost control but difficult to "sell" to business units.
- ▶ Setting up a dedicated process, governance and means within the IT department is often necessary to ensure the obsolescence frame of reference is applied.

Criterion 6

IT management dashboard includes indicators related to the IT architecture (measurement of the alignment with the frame of reference and the level of obsolescence in particular). The IT department directors review these indicators, and action plans are in place to correct discrepancies.

- ▶ Objectives of alignment of the IT with the architecture's frame of reference are defined and tracked.

NOTES...

PROJECT PORTFOLIO

OPTIMISE THE VALUE OF IT
LEGACY AND MANAGE ITS
EVOLUTIONS

STAKES FOR THE COMPANY

1

Cover all needs in terms of IT development in a balanced way, taking into account the company's stakes and strategic objectives.

2

Ensure that the portfolio is realistic and based on an overall estimate of the resources needed, the changes to be made and the new skills to be developed.

3

Find an optimal balance between value creation, risks, and resources.

4

Allocate the company's resources to the projects that contribute most to value creation.

5

Set concrete value creation objectives through a sufficient level of commitment from executives throughout the project stages (launch, development, release).

THREATS TO THE COMPANY

1

Miss out on strategic projects for the company.

2

Waste company resources on projects that do not create to significant value, are poorly steered, or compete with each other.

3

Increase IT costs by not keeping new applications' recurring costs under control.

4

Not realising projects' expected benefits due to insufficient involvement of business units or General Management.

RELATED RISK FACTORS

1

A lack of a formal IT roadmap approved by business units and General Management.

2

A lack of methodology in drafting business cases appropriate to the types of projects.

3

A lack of methodology in managing project launch priorities.

4

Launching projects other than Fast IT type without a business case.

5

A lack of organisation or definition of steering responsibilities for the project portfolio throughout their lifespan.

BEST PRACTICES

1

A single project repository for global management.



2

Business case for each project elaborated with business units and the IT department.



3

Innovation integrated into the project portfolio.



4

Managing launch priorities based on business cases.



5

Tracking and steering launched project based on reliable, exhaustive reports.



6

Business end-of-project assessment to learn any necessary lessons.



Best practice 1: PROJECT REPOSITORY.

All projects are references in a single repository that can be structured in a programme to make global project management easier.

Criterion 1

There is a single repository for all projects.

- ▶ Projects are presented in a company-wide standard framework to be able to compare them.
- ▶ Project ideas and innovation initiatives are included in the portfolio in a specific category, even if the project is not yet formalised.

Criterion 2

All projects are referenced in this repository, from the idea stage to launched projects being worked on.

- ▶ The business case is the deliverable of a progressive project approval process from the initial idea to the launch decision.
- ▶ The process typically includes the following approval steps: declaration of intent or opportunity, functional business unit design scoping, prototyping (if needed), business case, scoring, and launch decision.
- ▶ All projects are declared in the repository, including projects underway.

Criterion 3

The repository is structured to categorise projects by their type to make decision making easier.

- ▶ Project portfolio segmentation can be based on the following types:
 - ▶ Programmes: where relevant, projects are assigned to programmes
 - ▶ Regulatory and compliance projects
 - ▶ Innovation projects (typically technology)
 - ▶ Projects to support business development
 - ▶ Projects to improve performance (quality, reduced lead times, process standardisation),
 - ▶ Cost reduction projects,
 - ▶ Infrastructure or systems optimisation projects,
 - ▶ Projects for maintaining in operational condition,
 - ▶ Decommissioning projects,
 - ▶ Etc.
- ▶ Another segmentation system classifies projects according to their stage of progress:
 - ▶ Declaration of intention approved,
 - ▶ Business unit functional framework approved
 - ▶ Pre-project approved,
 - ▶ Business case approved
 - ▶ Projects launched (by project stage, [see VECTOR 7 - PROJECTS](#))
- ▶ To verify that projects are in line with the company's strategy, it is essential to specify which part of the strategic plan each project refers to.
- ▶ Dependencies between projects must be identified and described.

Criterion 4

The project repository is managed by an organisation for which it is the main task.

- ▶ Formal portfolio management is typically the responsibility of a Project Management Office (PMO) which prepares decisions for Executive Committee.
- ▶ The projects are evaluated based on their contribution to value creation and the inherent risks and difficulties in implementation.
- ▶ This evaluation can be introduced when structuring the repository to classify projects from 'high value/low risk' to 'low value/high risk'.

Best practice 2: *BUSINESS CASE*.

Business units prepare a business case with help from the IT department for each business unit project with a significant IT aspect.

Criterion 1

The business case presents the benefits the company expects in terms of process improvement and value creation.

- ▶ These business cases explain the expected business benefits and the conditions needed to obtain them:
 - ▶ What? (Project objectives)
 - ▶ Why? (Expected opportunities and benefits)
 - ▶ Who? (Human resources and necessary skills)
 - ▶ How much? (Costs and ROI)
 - ▶ When? (Development objective, speed of execution, short/long-term perspective)
- ▶ The project's benefits are identified with qualitative and/or quantitative criteria.
- ▶ The impacts for business units (organisation, processes, skill levels to implement) are clearly evaluated.

Criterion 2

The business case assesses projects' profitability given the expected gains and overall estimated costs.

- ▶ When the IT aspect is significant, the costs (project and recurring) are estimated based on prototypes, if necessary.
- ▶ Drafting a load plan refines the business case's vision of time.
- ▶ Recurring costs must be estimated for a three- to five-year period (or according to the application's estimated life span).

Criterion 3

The business case includes a risk analysis (not seeing the expected benefits, deviation in costs and deadlines, risks not to take, etc.).

- ▶ Identify the project's conditions for success (prefer prototypes when the stakes justify it) ([see VECTOR 7 - PROJECTS](#))
- ▶ Identify interdependencies between projects since this is a risk factor that is often underestimated. Make sure to measure the impact on business cases.
- ▶ Consider alternative solutions (i.e. overhauling the business unit process) or working in a downgraded mode.

Criterion 4

Business units lead the development of business cases in collaboration with the IT department.

- ▶ For purely technical and infrastructure projects, the business case can be drafted by the IT department and approved by the Executive Committee.
- ▶ Drafting business cases is too often limited to projects with the highest costs without considering their stakes.

Criterion 5

The business unit that owns the project is responsible for both achieving the expected benefits and managing risks optimally.

- ▶ Business cases identify business managers (including sponsors) who will be responsible for generating business profits. For this, they are involved in the project for its entire lifespan.
- ▶ The managers of the business units concerned, in collaboration with the business unit project manager, take all measures (in terms of staff, information, training, organisation, etc.) needed to make the expected benefits a reality.

Criterion 6

The IT department checks that the business case is consistent with the IT roadmap.

- ▶ This consistency check is essential to:
 - ▶ Control changes to IT (for example, generalised 'shadow IT', uncontrolled use of cloud computing and SaaS offers, etc.),
 - ▶ Guarantee IT security (security incidents, cyber attacks, etc.) and compliance (CNIL, GDPR, traceability, etc.),
 - ▶ Streamline IT changes and maintain control of the technologies needed for them,
 - ▶ Control technical debt (hardware and software obsolescence) (see [VECTOR 5 · ARCHITECTURE](#))

Best practice 3: INNOVATION.

The project portfolio includes projects to scale innovation initiatives (PoC, MVP, Labs and other R&D work)

Criterion 1

The IT department gathers a list of initiatives to scale from the company's innovation actors. (see [VECTOR 2 · INNOVATION](#)).

- ▶ These innovation actors can be found in the IT department (the innovation team and community), the business units, the innovation department, etc.
- ▶ The IT department works with those driving these initiatives, sometimes called 'digital champions'.
- ▶ The IT department should be involved ahead of any decision to scale to make sure it is feasible (choice of architecture, security, etc.).

Criterion 2

There is appropriate portfolio governance to manage these innovation initiatives in accordance with their specificities (such as their speed - Fast IT).

- ▶ These initiatives are regularly reviewed to decide whether to continue them, reorient them, or stop them.
- ▶ The method of analysis takes inspiration from the fast development method (Agility).
- ▶ The decision-making process is quick.
- ▶ When a project is judged to be promising, fast development methods are allocated to it, and it joins the 'Core IT' project portfolio.

Best practice 4: MANAGING LAUNCH PRIORITIES.

An inter-project launch priority management process based on business cases is in place and involves business units in the Executive Committee for key projects.

Criterion 1

To prioritise their launches, the portfolio's projects are evaluated according to the expected benefits for the company, the inherent risks, and the predefined budgetary scope estimated over time.

- ▶ A decision and arbitration framework is defined, shared and pre-established.
- ▶ Benefits and risks are assessed based on the business case.
- ▶ Dependencies with existing projects or projects near launch are identified and their impacts analysed.

Criterion 2

Decisions to launch projects are made by the Executive Committee.

- ▶ Project launch permissions take into account operational constraints: the human resources available, the production capacity, financial resources.
- ▶ The evaluation results and their consequences in terms of hierarchy are formalised and communicated to the teams concerned.
- ▶ An alerting process for General Management is in place for final arbitration if needed.

Criterion 3

Project launch decisions are adjusted according to the company's strategic stakes and competitive environment (Time-to-Market).

- ▶ In this case, a 'time-driven project' or agile approach can be put in place ([see VECTOR 7 - PROJECTS best practice 3 criterion 3](#))

Best practice 5: TRACKING AND STEERING LAUNCHED PROJECTS.

A project management process involving the business units is used to monitor, steer (review the priority or even stop) ongoing projects on the basis of reliable and exhaustive reports, if necessary, by updating the business case.

Criterion 1

Projects' advancement is regularly tracked and summarised by PMO which reports to the Executive Committee.

- ▶ Project managers update projects' progress (quality, costs, delays, risks, remainder, etc.) in the project tracking tool to draft summaries.
- ▶ This information is confirmed in conjunction with the business unit in a project committee.
- ▶ This vector is connected closely to [VECTOR 7 - PROJECT](#), which describes the tracking of ongoing projects and the reports to be sent to steering bodies (including the Executive Committee).

Criterion 2

Based on this tracking, the Executive Committee makes decisions to allocate resources, re-prioritise and update business cases, if necessary.

- ▶ Resources can be allocated among various projects.

Criterion 3

A project portfolio management tool that works with the operational tracking of projects makes it easier to steer the overall portfolio.

- ▶ The portfolio management tool acts as a tool that consolidates the elements used in projects' operational management.
- ▶ It includes key elements of steering, such as resource allocation, dependencies with other projects, unified indicators, etc.
- ▶ This tool is made available to business units.

Best practice 6: BUSINESS END-OF-PROJECT ASSESSMENT.

General Management has business unit project assessment carried out when the project has reached a nominal state of operation to learn the lessons needed to optimise the decision-making process concerning projects.

Criterion 1

For projects that contribute greatly to value creation and/or are costly, the resulting business benefits are analysed to verify that they are in line with the initial business case.

Criterion 2

These analyses must include all stakeholders (project team, end users, clients, etc.).

- ▶ Calling on a third party (in-house or outside the company) for an independent viewpoint can be useful.

Criterion 3

The analyses and feedback on the project's progress are formalised. Action plans to improve the project portfolio management process, as well as launching or implementing projects, are put in place to secure the expected benefits.

- ▶ Business unit project reports feed into a shared knowledge base made available to all business units and the IT department. We recommend using a single template to make it easier to capitalise on the data gathered in project reports.

Criterion 4

General Management makes sure that the concerned business units managers take all corrective measures in terms of staff, information, training, organisation, etc. or launching another project.

- ▶ General Management monitors the proper implementation of the corrective actions decided.

NOTES...

PROJECTS

CONTROL PROJECT AND SOLUTION IMPLEMENTATION

STAKES FOR THE COMPANY

1

Fit into the project portfolio defined by the company, which should guarantee alignment with the company's business needs and strategic plan

2

See the project as a business unit project with a digital component (and not the other way around) by defining properly the involvement, the roles and the responsibilities of the business units and the IT department in steering and driving the project, including the business unit's processes and the skills to develop (change management).

3

Put in place the conditions for successful project completion with regards to the business case's objectives (opportunity study) in terms of costs, deadlines, features developed, expected benefits and user take-up.

4

Make sure that various project methods (for example, 'agile' vs more traditional 'V-model') cohabit. This approach must include the criteria for deciding to use one method over others.

THREATS TO THE COMPANY

1

A lack of company resource optimisation.

2

An inability to generate the expected business unit benefits.

3

A loss of competitiveness due to a dysfunction of the company.

RELATED RISK FACTORS

- 1** Not respecting the IT and project portfolio strategy.
- 2** Undefined roles and responsibilities (IT and business units).
- 3** A lack of project management methodology.
- 4** Insufficient understanding of the different project management methodologies.

BEST PRACTICES

- 1** Business objectives for projects that are explicit, consistent, and shared. ✓
- 2** Project governance that is clear, legitimate, and recognised. ✓
- 3** Project methods related to expected objectives. ✓
- 4** Project compliance and security by design. ✓
- 5** Managing milestones to track drifts from objectives. ✓
- 6** Technical and user acceptance tests are carried out before the production release. ✓
- 7** IT end-of-project assessment drafted and shared. ✓

Best practice 1: BUSINESS UNIT OBJECTIVES FOR PROJECTS.

The projects' strategic business unit objectives are clear, coherent with each other, and shared.

Criterion 1

The key issues or objectives of the business units to be achieved during the course of the project are clearly identified when the project is launched and then updated.

Criterion 2

The strategic objectives (financial, operational, technical, etc.) are explained by the management to the various stakeholders.

Criterion 3

These objectives are coherent with each other.

Criterion 4

These objectives are understood and shared by all project actors.

Criterion 5

These objectives are ordered, and an arbitration procedure is in place to resolve conflicts between objectives that might become incompatible or even contradictory.

Best practice 2: PROJECT GOVERNANCE.

The project's mode of governance is clear, shared, legitimate and recognised.

Criterion 1

There is a single, legitimate leading unit.

- ▶ The leading unit is the department, unit or entity that is the solution's end user. In most cases, this will be a business unit (except for technical projects).
- ▶ For projects of a transversal nature, the leading unit is the entity that is the most concerned, most legitimate, or most driving.

Criterion 2

The sponsor is named and known by all. Their real availability allows them to fulfil their role.

- ▶ The sponsor's role is as a facilitator to make important decisions and ensure the whole is coherent.

Criterion 3

A strategic steering committee (chaired by the sponsor and led by the project manager/scrum master) and an operational project committee are formed and effective.

- ▶ Each of the two effective committees is made up of participants representing the various activities and subjects covered (business units, IT, change management, etc.). They meet regularly and adapt to the topics. They make decisions and guide the project. A record of decisions is systematically and quickly drafted at the end of each committee meeting.
- ▶ The steering committee produces a report for a committee made up of representatives of General Management, the IT department and the business units in a standardised format so it can exercise its role of consolidated management of the project portfolio (see VECTOR 6 · PROJECTS PORTFOLIO).

Criterion 4

The project's steering mode is completely defined. It includes additional committees to the steering and project committees. These additional committees are known (objectives, frequency, dashboards and indicators, etc.).

- ▶ Examples of additional committees for business unit, feature arbitration, batch or works monitoring, IT integration, acceptance test for completed developments, etc.
- ▶ In difficulties are encountered on critical projects, the company may call for independent audits.

Criterion 5

The project's operational, financial and human stakes and risks are identified and known to all. The criticality of these risks must be evaluated, tracked and communicated regularly to all stakeholders.

- ▶ Project costs are identified and quantified. These costs include all those attributable to the project.
- ▶ The "support" component is planned upstream in the project and is dimensioned correctly in order to overcome resistance to change.
- ▶ A risk map is maintained and communicated at regular intervals.

Best practice 3: PROJECT METHODS.

The project steering method is evaluated upstream in its consistency with other projects and in reaching the expected objectives. It must include stakes related to change management.

Criterion 1

An evaluation of different project management methods recognised within the IT department ("V-model" or "agile" methods) is conducted during the project design process.

- ▶ Digital transformation requires a lifecycle management model for IT applications separating core applications, those that differentiate the company, and those that foster innovation. Depending on their level, the projects' complexity/criticality, the size of the project team, the chosen project management process should be more or less continuous.
- ▶ In some cases (Fast IT), projects can be time-driven, and arbitrations are made on these projects' functional content.

Criterion 2

Choosing the project management method must take into account the synchronisation needed with other ongoing projects and the IT department's ability to cope with it, as well as the elements specific to the project (cost, delay, the teams' skills).

- ▶ The duality of processes (historical or continuous) requires the IT department to be able to ensure unified governance.

Criterion 3

There is a single project manager/scrum master, and they have a business unit-oriented skills profile. They have real authority over a team and a dedicated budget.

- ▶ Setting up pairs of user/IT department project managers is possible.

Criterion 4

Project participants are assigned appropriately according to the project types ("V-model" or "agile" methods).

- ▶ In some cases (particularly in agile projects), the DevOps technique brings together development and production teams leading to shorter development cycles, increased release frequency and continuous delivery.
- ▶ See the Cigref publication '[Agile at scale](#)'.

Best practice 4: PROJECT COMPLIANCE.

In addition to the essential involvement of end-users, security, compliance and internal controls must be integrated since the beginning of the project design phase.

Criterion 1

Compliance is considered from the project design stage.

- ▶ Beyond the self-interest of avoiding additional costs related to late consideration, "*security & privacy by design*" is a regulatory constraint in the General Data Protection Regulation (RGDP) and potentially other applicable regulations.

Criterion 2

Internal inspections are included in the project design stage.

- ▶ In order to limit the difficulties of monitoring the project's (regulatory and security) compliance, you must take into account the constraints related to internal inspection as early as possible.

Criterion 3

The ability to ensure the security of the project when part of IT must be planned ahead.

- ▶ To guarantee the IT's security coherence and the ability of the SOC to respond to it, compliance with the standards of IT technical consistency must be taken into account from the design stage.

Best practice 5: MANAGING MILESTONES.

Regular milestones are planned to monitor the drifting of objectives, costs, deadlines, technical feasibility, and business requirements in relation to the initial objectives.

Criterion 1

Relevant indicators are defined to track project progress and anticipate difficulties. These indicators are measured regularly.

- ▶ These indicators track workloads, planning and production (in work units). For example, they can measure the actual rate of resource allocation and consumption, the number or percentage of requirements added or modified which may indicate a drift from the original objectives. Some of these indicators should be used to monitor that business stakes continue to be considered as the project progresses.
- ▶ In agile projects, the development cycle is shorter, adaptive and iterative, and appropriate indicators should be identified at the Sprint, Epic or other levels.

Criterion 2

These indicators are shared and act as criteria for steering and decisions in the committees.

Criterion 3

Alerting and arbitration procedures are defined.

- ▶ If alerting procedures have been activated, they result in an effective decision.
- ▶ In agile projects, alerts can be raised much more quickly than in tradition V-model projects.

Criterion 4

The most operational monitoring body regularly examines drifting indicators and makes arbitrations or, if necessary, raises alerts to the steering committee which decides as a last resort.

- ▶ In agile projects, there may be only one operational structure that brings stakeholders together.

Criterion 5

The steering committee confirms that milestones have been reached.

- ▶ There are frequent milestones to approve options that structure the project and for which it is difficult to roll back without significant consequences. All too often, passing milestones is left to the IT function which takes on a business unit responsibility.
- ▶ In agile projects, the operational structure can approve the choices and priority of user stories in the backlog to be included in the next sprint.

Best practice 6: TECHNICAL AND USER ACCEPTANCE TESTS.

The project is subject to technical and user acceptance tests before being released into production.

Criterion 1

The IT department performs technical and functional unit tests.

- ▶ The IT department can also perform functional non-regression tests subject to final approval by a panel of users.
- ▶ In agile projects and DevOps, new appropriate test techniques are spreading (such as Test-Driven Development, Acceptance Test-Driven Development or Behaviour-Driven Development).

Criterion 2

The business unit user acceptance test stage is planned and done.

- ▶ The business unit user acceptance test stage is essential no matter the project management method used.
- ▶ In agile projects, if the product owner (PO) is knowledgeable and available, there can be continuous approvals. Otherwise, a batch approval is performed essentially as a demo with the business units at the end of a sprint.

Criterion 3

Validating user acceptance tests is subject to formal approval.

- ▶ This approval is based on a detailed report of the results of each test, including the cases remaining in anomaly considered non-blocking. The test committee minutes produces a signed and documented user acceptance test report (a list of remaining anomalies and justification of their non-blocking character).
- ▶ In agile projects, this approval can be simply an email from business units confirming that the software fulfils the user stories of this sprint.

Criterion 4

The steering committee gives the green light based on clear and shared GO/NO GO criteria.

- ▶ The GO/NO GO criteria must cover all aspects used to decide on launch: user acceptance test results are an essential criterion of GO/NO GO as is training, documentation and launch support (a support team, etc.). The GO / NO GO criteria and their acceptability threshold must be defined prior to decision making.
- ▶ In an agile project, sprints only last a few weeks, so this step is not necessarily applicable.

Best practice 7: IT END-OF-PROJECT ASSESSMENT.

An end-of-project assessment is carried out and shared.

Criterion 1

A project assessment is planned and actually carried out with all stakeholders once the start/break-in phase is complete.

Criterion 2

This assessment must check that there are no residual tasks remaining (thus additional cost): uninstallations, decommissioning, training, etc.

Criterion 3

The assessment allows all project stakeholders to share the same vision of the project costs, deadlines, and respect for announced features.

Criterion 4

The assessment should also allow stakeholders to establish and share a common understanding of the lessons to be learned from the project.

- ▶ **Examples of lessons learned: the difficulties encountered and mistakes not to be reproduced, methodological and other gains, good practices, etc.**

NOTES...

HUMAN RESOURCES

ORGANISE AND MANAGE TALENT AND SKILLS

STAKES FOR THE COMPANY

1

Anticipate the company's needs by investing in the skills needed to complete future projects.

2

Maintain employees' motivation and employability by capitalising on their skills.

3

Make the company's digital and IT business units attractive to new talent.

4

Have people of different generations and skills work together to ensure proper IT development dans roadmap.

THREATS TO THE COMPANY

1

Harm motivation of IT people and lose skills due to uncontrolled turnover.

2

Not be able to hire resources that the company needs.

3

Uncontrolled ageing of the IT department's average age.

4

A loss of the company's competitiveness.

RELATED RISK FACTORS

1

A mismatch between the company's projects and objectives on the one hand and the evolution in resources on the other.

2

A lack of knowledge and steering of skills and resources.

3

A lack of knowledge of technologies and appealing modes of organisation.

4

A lack of arbitration between the technological benefits (which is attractive) and relevance to the company, a lack of communication on attractive projects and modes of organisation.

5

A lack of change management (modes of operation, different generations).

BEST PRACTICES

1

HR objectives that anticipate the IT department's future needs.



2

Framework of competency is formalised.



3

Strategic workforce planning adequated with company forecasted needs.



4

Skills evaluation is carried out.



5

Hiring plan set to meet IT needs.



6

Skills development through IT training programs.



Best practice 1: HR OBJECTIVES.

The management of IT human resources must anticipate the IT department's future needs, develop internal skills and manage talent.

Criterion 1

An HR plan for the IT department in line with the IT strategy and the company's HR rules is defined to identify future needs and an availability schedule for the resources and the means in place to acquire them (school partnerships, trade shows, direct approaches, etc.).

Criterion 2

An IT skills management approach is formalised to ensure the IT department's HR plan is applied and that skills evolve in line with needs and contributes to the development of the digital section of the company's strategic plan.

Criterion 3

The adequacy of IT resources is regularly assessed, and trajectory correction measures are regularly developed and presented to IT department and HR executives.

Criterion 4

In line with its approach to innovation, the company monitors future skills and anticipates its needs.

- ▶ For example, DevOps, Internet of Things, Artificial intelligence, Data Science, Blockchain, etc.

Criterion 5

An approach in favour of women in digital trades has been taken.

- ▶ For example, the 'Femmes@Numérique' (a French group of associations and business foundations with government support) and 'She Leads Tech' (AFAI-ISACA) approaches.

Best practice 2: FRAMEWORK.

A framework of required skills has been formalised.

Criterion 1

An IT and digital business unit jobs framework is established in coherence with the standards of the profession and is shared with stakeholders. Potential bridges between job classes are identified and described.

- ▶ Make sure that digital business units are included in the approach. The digital business unit and IT jobs framework also covers jobs outside the IT department.
- ▶ See the Cigref publication (in French): '[Nomenclature RH des métiers du numérique](#)'

Criterion 2

Job descriptions are formalised and attached to the jobs in the framework. During hiring, these job descriptions are shared with and known to all IT people.

- ▶ Each employee must have a job description that is based on the digital business units' framework.

Criterion 3

There is a mapping of the IT and digital business unit jobs including the necessary skills. Critical and/or key positions are identified.

- ▶ The map must describe the existing situation faithfully.

Criterion 4

The framework is regularly maintained with the best practices on the market, technological changes and the company's strategy.

Best practice 3: STRATEGIC WORKFORCE PLANNING.

A plan to match the skills with the company's current and future needs is formalised and in place.

Criterion 1

An analysis of discrepancies to the needs expressed is performed.

- ▶ In conjunction with the HR and digital sections of the company's strategic plan. ([See best practice 1](#)).
- ▶ The needs are derived from the company's strategic plan.

Criterion 2

The skills approach helps identify key skills and those with (great) potential, including digital jobs. The skills approach feeds into succession plans.

- ▶ The results must be traced, monitored, and be the subject of action plans if needed.

Criterion 3

A discrepancy resorption plan is drafted, formalised, and implemented (training, hiring and supplier and start-up partnerships). The summary is presented to the IT department's management board.

- ▶ The action plan is compared to and adjusted in line with the market's best practices.

Criterion 4

The skills management approach feeds into the company's next strategic plan.

- ▶ This criterion is in line with [VECTOR 9 - PROVIDERS/SUPPLIERS](#).

Criterion 5

A hiring plan is set and shared with the human resources department.

- ▶ This criterion is in line with [VECTOR 9 - PROVIDERS/SUPPLIERS](#).

Best practice 4: SKILLS EVALUATION.

Skills are evaluated.

Criterion 1

There is a skills evaluation process in the IT department based on the skills framework.

- ▶ The process is carried out at least once a year (for example, during the annual reviews).

Criterion 2

The IT department uses the company's HR assessment tools in compliance with regulatory constraints (security, GDPR, etc.).

Criterion 3

The evaluation process is monitored with indicators and, if necessary, is subject to an action plan.

- ▶ Check that all employees have been evaluated at least once a year.

Criterion 4

A capitalisation process has been put in place. The indicators used are analysed for their relevance.

- ▶ The results of this analysis are used to improve the skills evaluation process for the following year.

Best practice 5: HIRING PLAN.

A hiring plan is set and implemented to meet the IT department's resource requirements.

Criterion 1

In conjunction with supplier sourcing (see VECTOR 9 · PROVIDERS / SUPPLIERS) and the IT department's current skills, a hiring plan is defined to take into account the IT department's current and future needs.

Criterion 2

Job vacancies are presented in such a way as to make them attractive (a description of the company and its strategy, its international activities, the position's field of responsibility, etc.).

Criterion 3

Job vacancies are systematically published internally, and applicants are received by recruiters. Responses are systematically sent to them.

Criterion 4

Various media are used to fill the open positions externally (social networks, sponsorship, relationships with schools and universities, ecosystem relationships, head-hunters, etc.)

Criterion 5

Position filling reviews are regularly conducted with the IT and HR departments. In particular, this should allow to anticipate the time needed to fill positions.

Best practice 6: SKILLS DEVELOPMENT.

Digital training programs make it possible to match the skills to the company needs and helps keep the skills in-house (IT department attractiveness).

Criterion 1

A training offer is published and made visible to all employees.

- ▶ The training offer must be updated regularly (for example, using MOOCs, partnerships with schools, etc.).

Criterion 2

Sharing internal skills and capitalising on technical know-how is organised.

- ▶ A knowledge management approach, company social networks, topical communities, etc.

Criterion 3

Management must ensure that the training plan is in line with its activities and employees' objectives.

- ▶ Employees must be able to take advantage of training that is in line with their current and future assignments.

Criterion 4

The training offer's effectiveness is measured and formalised.

- ▶ The training offer's effectiveness at the IT department level is formalised. The training offer evolves as needed.

Criterion 5

Managers regularly review their employees' skills gains with them.

- ▶ At the least, this is done as part of the annual performance review.

Criterion 6

An annual training report is presented to the IT and HR departments, then published.

- ▶ It is presented to social partners.

PROVIDERS & SUPPLIERS

STEER RELATIONSHIPS WITH DIGITAL BUSINESS SOLUTIONS AND SERVICE PROVIDERS

STAKES FOR THE COMPANY

1

Have an effective process and the elements required to decide rather "make or buy".

2

Guarantee good governance of outsourced activity in ~~the~~ all stages, from choice decision, launch, daily monitoring and closing.

3

Manage the customer/supplier relationship effectively by involving all stakeholders (business units, the IT department, subcontractors).

4

Acquire appropriate solutions to speed up the time-to-market of the company's projects in consideration of internal resources (HR, finance, business lines, etc.).

THREATS TO THE COMPANY

1

Loss of control and dependency on certain suppliers.

2

Information leaks to competitors.

3

Legal and financial risks related to the steering of outsourcing contracts.

4

Impacts to company staff and management due to poor management of outsourcing actions.

5

Harm to the company's image.

RELATED RISK FACTORS

1

Not having certain shared criteria to identify and select 'make or not make' opportunities.

2

A lack of understanding of the ecosystem of digital solutions and service providers; A lack of methodology in steering the customer/supplier relationship.

BONNES PRATIQUES

1

Strategy and governance of outsourced services are defined. ✓

2

Study for opportunity and feasibility. ✓

3

Outsourcing approach includes a transition and change management. ✓

4

Management of services is organised on a daily basis. ✓

5

Closure and reversibility defined as a function of business stakes. ✓

6

Supplier relationships are organised and monitored. ✓

Best practice 1: STRATEGY AND GOVERNANCE.

An outsourced services strategy and its associated governance have been defined.

Criterion 1

The IT outsourcing strategy includes the "make or buy" policy. The IT department evaluates opportunities to outsource each of the activities/IT with business units based on the criticality of the activities concerned. It must be approved by the appropriate level of the hierarchy.

- ▶ Such an evaluation:
 1. Includes the mapping of the company's activities and the corresponding IT activities (including shadow IT),
 2. Leads to sifting through the following criteria: alignment with the business unit strategy, alignment with the IT strategy, market maturity and provider offerings, operational requirements, the number and quality of internal skills,
 3. Imposes privacy, security, and regulatory constraints,
 4. Considers workforce, industrial, supplier dependency, legal, financial and image risks.

Criterion 2

A management system for outsourced services has been put in place, including a risk management aspect.

- ▶ An organisation and processes of outsourced services are in place to meet business needs.
- ▶ Business units must be aware of the exposure to risk and the measures taken. The following risks are frequently considered: reliability/integrity of third parties, data privacy and protection, cybersecurity, regulatory compliance, corporate social responsibility (CSR), ethics and sustainable development, quality and safety.

Criterion 3

An outsource-related human resources management has been put in place.

- ▶ Identify key resources (including new skills) to be maintained within the organization (for example, a contract manager, a project manager expert in managing subcontracting, an architect able to evaluate subcontractors' proposals). Verify that roles and responsibilities associated with outsourced services have been assigned. Ensure that the management of jobs and skills is in place ([see VECTOR 8 - HUMAN RESOURCES](#)).

Criterion 4

Indicators have been defined and put in place to measure the added value to business units when outsourcing services.

- ▶ Examples of value provided: financial gains, velocity, risk reduction, etc.

Criterion 5

Knowledge management has been organised.

- ▶ Capitalise on and develop knowledge of managing outsourced services to:
 - ▶ Steer contracts,
 - ▶ Audit the services purchased,
 - ▶ Exercise service reversibility ([see best practice 5](#)).

Best practice 2: STUDY.

There is an opportunity/feasibility study for each service that is a candidate for outsourcing.

Criterion 1

There are market studies and potential service providers identified for the service to be outsourced.

- ▶ Including benchmarks.

Criterion 2

There is a strength/weakness analysis of the existing.

- ▶ Analysis of documentation, the skills level, system obsolescence, technical debt, etc.

Criterion 3

There is a business case for outsourcing an activity.

- ▶ Purpose, tangible and intangible gains/costs: the quantifiable and non-quantifiable financial implications of the integration, interoperability, and reversibility of the offers as well as the additional costs related to the necessary level of security must be taken into account.
- ▶ The business plan must also show the gains generated within the business units, relevant elements of comparison (internal/external) and an estimate of ROI.

Criterion 4

There is a risk analysis for the activity to be outsourced.

- ▶ Risks are mapped (including cybersecurity). A risk reduction plan exists and is implemented and maintained.
- ▶ For cloud computing offers, the risks should be split according to the sensitivity of the data concerned and whether it is a public cloud, external private cloud or hybrid cloud computing system. (see [VECTOR 4 - DATA](#))

Criterion 5

The business unit makes the decision to outsource a business activity, always in consultation with the IT department. The decision to outsource an activity specific to the IT department is made by the IT department in consultation with the business units.

- ▶ Based on the business case and risk analysis.

Best practice 3: OUSTOURCING APPROACH.

An approach including a transition and change management is set up for each of the IT activities to be outsourced.

Criterion 1

For the activity to be outsourced, the services concerned have been defined clearly within the specifications (a needs assessment and results requirements).

- ▶ The business unit and IT department directors have formally approved the specifications.

Criterion 2

A procedure, including supplier evaluation criteria, is developed in parallel to the specifications.

- ▶ The evaluation criteria must take into account the various risks of dependency, loss of control, etc.

Criterion 3

The service transfer plan to a supplier has been defined and includes any HR impacts (transfer of staff to the service provider)

- ▶ To be done as early as possible before launching the call for tenders.

Criterion 4

A knowledge and data transfer process to the service provider has been defined.

- ▶ The knowledge transfer is formalised (document database, best practices, etc.).
- ▶ In particular, the contract states that the supplier can only use the company's data to execute the contract.

Criterion 5

In the outsourcing contract, there are definitions of the security commitments that the supplier is to respect (in particular, the supplier drafts a plan to guarantee security to be approved by the client).

- ▶ For example, when using cloud computing or company data.

Criterion 6

In the outsourcing contract, there are elements to measure the quality of the service provided.

- ▶ These contractual elements cover aspects such as defining a service level agreement (SLA), identifying obligations of means and results, reporting measures and audit clauses.

Criterion 7

Drafting the contract and the ability to modify it during execution are the result of collaboration between all the stakeholders (business units, IT department, purchasing and legal).

- ▶ There are inspections to check that all stakeholders have been involved in drafting the contract. The contract must allow the service to evolve subject to the agreement of the parties (review clause).

Best practice 4: MANAGEMENT.

The day-to-day management of services is organised.

Criterion 1

Formal management reviews of outsourced services are held regularly with the service provider.

- ▶ After an analysis of the contract's strengths, weaknesses, opportunities and threats:
 - ▶ Inspection points were defined (for example, the certification of the service provider's staff),
 - ▶ An appropriate steering approach is in place to execute the contract as close as possible to its terms (contractual milestones, invoicing, etc.) alongside an associated report.
- ▶ There are always minutes after each service management review meeting.

Criterion 2

Discrepancy resorption plans are identified and implemented. Incident and problem tracking inspections are organised with the service provider.

- ▶ Any event or contractual discrepancy that could have an impact on the schedule, the contract amount or project costs must be the subject of an appropriate level of communications for decision making.

Criterion 3

There is a periodic review (at least annual) of the contract with all stakeholders (business units, IT department, purchasing department). A service evolution process has been defined, understood and shared with the service provider.

- ▶ Evolutions of services must occur within the contract's framework.

Criterion 4

The measure provides for a method of preventing and handling potential problems through:

- A process defined and understood by the parties for managing conflicts,
- A glossary to overcome differences of vocabulary,
- A defined and understood process to reduce the impact of cultural differences.

► This is a real need with all service providers and is essential in case of offshoring.

Criterion 5

The analysis of the service's value is assessed at an appropriate frequency (given the initial objectives and contract duration). The decision to prolong outsourced services is studied and made with the business unit.

- A report of outsourced services.
- The realisation of expected savings (compared to the business plan and initial return on investment).

Best practice 5: CLOSURE AND REVERSIBILITY.

Service closure and reversibility management have been defined according to the business stakes.

Criterion 1

A clause describing the detailed conditions of service closure and reversibility have been defined in the contract.

- From the start of the project, how reversibility operations must be studied, demonstrated, and defined in the clauses of the contract. The ability to manage reversibility from one partner to another supplier or in-house must be checked and preserved.
- The elements allowing the reversibility option must be updated (annually with the service provider).
- Reversibility that integrates the restitution of company-owned data and its deletion at the end of the contract must be provided for.

Criterion 2

The transfer of the service provider's resources has been anticipated in accordance with the changes to the scope of service.

- See the HR impacts as part of re-internalisation.

Criterion 3

The business continuity plan must include the interdependencies of the service with the company's IT environment (interfaces, other applications concerned, etc.)

- A business continuity plan has been drafted to mitigate any failures during the reversibility phase.

Criterion 4

The knowledge and data transfer process has been defined.

- Within the framework of the contract, the reversibility plan provided by the external service provider includes:
 - A description of the training required for the company or the buyer to use the returned data (including documentation),
 - The assurance of the destruction of the data once the transfer is made.

Criterion 5

Closure and reversibility procedures are reviewed regularly.

- ▶ This includes data retrieval, documentation (updated operational procedures) and materials as appropriate.
- ▶ Once per year, the IT department checks that the reversibility plan (including a data recovery mechanism) is up-to-date. Reversibility tests and audits are scheduled and carried out periodically (frequency defined in the contract).

Best practice 6: SUPPLIER RELATIONSHIPS.

The management of hardware and software suppliers is organised and tracked.

Criterion 1

The purchasing and legal departments are included at key moments when purchasing hardware and software.

- ▶ They are involved in the various steps, including choosing a supplier, drafting contracts, reviews with the supplier, ending contracts, etc.

Criterion 2

In projects, the choice of hardware and software suppliers follow recommendations in terms of the company's technical and systems architecture ([see VECTOR 5 - ARCHITECTURE](#))

- ▶ When purchasing hardware and software, technical validation points must be in place to ensure that they are consistent with existing elements.

Criterion 3

There is hardware fleet management.

- ▶ At the least, this means that:
 - ▶ Configuration management is regularly updated.
 - ▶ The fleet is inventoried at least once a year.
 - ▶ Hardware maintenance is optimised.
 - ▶ Exits from the hardware fleet are traced.

Criterion 4

There is software asset management.

- ▶ Resources are allocated to this function.
- ▶ At the least, this means that:
 - ▶ The software fleet inventory is kept up-to-date and optimised to make sure that the number of licences purchased matches use (discrepancies are corrected, and software maintenance is optimised).
 - ▶ Exits from the software fleet are traced.
 - ▶ Licences must be managed to limit legal risks.
- ▶ See the Cigref publication '[Software Asset and Cloud Management](#)'.

Criterion 5

Versioning and anticipation of hardware and software obsolescence are organised.

- ▶ There is an upgrade process, and suppliers are involved when the operation is considered critical.

NOTES...

SERVICES

PROVIDE DIGITAL
SERVICES THAT MEET
CLIENT EXPECTATIONS

STAKES FOR THE COMPANY

1

Understand the needs of business units and their evolution.

2

Guarantee a level of service that meets business units' needs considering the budget constraints.

3

Offer a catalogue of services that responds to the changing needs of customers or users.

THREATS TO THE COMPANY

1

A mismatch between the services provided and the needs of business units and employees.

2

Unsuitable allocation of resources (under- or over-allocation) causing a loss of competitiveness of poorly served operational functions.

3

Degrade the execution of business unit processes in terms of availability, integrity and privacy.

RELATED RISK FACTORS**1**

A lack of communication with the business units and the Executive Committee resulting in a lack of understanding of their needs.

2

Lack of understanding of and reaction to changing business unit needs.

3

A lack of structured processes and methodology to deliver the expected level of effectiveness.

BEST PRACTICES**1**

Catalogue for IT client services is offered and understandable.

**2**

Client requests are implemented on existing services.

**3**

Service agreements are in place and managed.

**4**

Continuous improvement of the user-perceived quality of service.

**5**

Production activity is steered using dashboards.



Best practice 1: CATALOGUE.

The IT department has set up a catalogue of client services.

Criterion 1

The service catalogue was established with clients.

- ▶ The IT department co-builds the service catalogue with its clients.

Criterion 2

The catalogue presents the services and work units to quantify them.

- ▶ This description must be understandable and drafted in concertation with the client.

Criterion 3

The service catalogue is regularly updated.

- ▶ This update must be done in collaboration or consultation with the client.

Criterion 4

The elements that make up the cost structure of each service are known and tracked, and their changes are regularly communicated to the customers.

- ▶ This criterion is linked to [VECTOR BUDGET & PERFORMANCE](#).
- ▶ The quality of this communication is a key element in an internal contractual relationship.

Criterion 5

The IT department is able to link the services delivered and the business unit processes to which they are attached.

- ▶ Here, the goal is to co-build a map - potentially simplified - of the processes and services associated with the client.

Best practice 2: CLIENT REQUEST.

The IT department has put in place a client request management process on existing services (run).

Criterion 1

The IT department regularly meets its clients to identify and update their needs and expectations.

- ▶ The minimum frequency for these meetings should be twice a year.

Criterion 2

The business units have a clear view of the services rendered to them.

- ▶ The business units verify that the services rendered match the service level agreement, and they have an end-to-end view of these services.

Criterion 3

The business units have a documented view of each service's cost.

- ▶ *Raising client business units' awareness of services' costs help them better understand their added value.*

Criterion 4

The IT department conducts benchmarks to compare its service offer with that of other companies in the same business sector and of comparable size, or even with offers from external service providers.

- ▶ This criterion is linked to **VECTOR BUDGET & PERFORMANCE**.
- ▶ In practice, this is about questioning the IT department's ability to control and self-evaluate costs.
- ▶ See the Cigref publication (in French) '[Modèle d'analyse et de benchmarking des coûts informatiques](#)'.

Best practice 3: SERVICE AGREEMENTS.

The IT department has set up service agreements.

Criterion 1

Services delivered to a particular business function or process are grouped together in a service agreement between the IT department and the entity concerned.

- ▶ In particular, the IT department has worked with users to set the acceptable time of interruption and the decision process for switching to a degraded mode in the event of a prolonged interruption in its service agreements. You should make sure that the service agreement is consistent with crisis management standards and the business continuity and resumption plans.
- ▶ This criterion is connected to [criterion 3 of this vector's best practice 5](#).

Criterion 2

Service agreements are drafted with business units, and the agreements formalise the respective agreements. They are written so as to be understandable by both parties.

- ▶ The goal is to formalise a collaboration agreement where each party understands the other's stakes and challenges and accepts their constraints.

Criterion 3

The contract includes the client's purpose and expectations as well as each stakeholder's duties and obligations.

- ▶ Regulatory aspects should also be taken into consideration and included.

Criterion 4

The contract is regularly updated in terms of both the types of services and cost structure.

Criterion 5

Monitoring indicators are defined and are the subject of regular, formal reports and discussions with business units.

- ▶ The contract's dashboard allows for constant communication with the client. Its frequency is appropriate to the service and must be regular to be a true companion steering tool.

Best practice 4: IMPROVEMENT.

The IT department has set up a continuous improvement process based on user-perceived quality.

Criterion 1

The IT department has put in place tools to measure the proper functioning and performance of its services with a process for collecting complaints and incidents relating to services rendered to customers.

- ▶ Collecting complaints is the start of the continuous improvement process.

Criterion 2

The claims/incidents reported and the discrepancies noted with respect to the commitments are the subject of regular analyses and resolution mechanisms to reduce future occurrences.

Criterion 3

A service quality monitoring dashboard is drawn up from the indicators mentioned in the service agreement (performance, incident resolution, etc.).

- ▶ The indicators are communicated through dashboards and distributed to the IT department managers and customers concerned.

Criterion 4

The IT department or a third party conducts regular satisfaction surveys among clients (i.e., *NPS*, *net promoter score*).

- ▶ It is preferable that these surveys be conducted by a third party.
- ▶ The dashboards and surveys are to be shared with client steering bodies.

Criterion 5

The measured quality indicators and satisfaction surveys help service agreements to evolve.

- ▶ The areas of improvement found in the satisfaction surveys are to be discussed with the business unit so as to adjust the service agreements.

Criterion 6

The IT department capitalises on the implementation of innovative approaches in delivering its services and integrates the benefits of the most significant innovations.

- ▶ Innovation is integrated into the continuous improvement process. Innovation challenges or hackathons can be co-initiated in such a manner as to improve services or create new ones. Clients can be called on to test innovative ideas.

Best practice 5: PRODUCTION.

The IT department uses a dashboard to steer production and support activities.

Criterion 1

The IT department has implemented resources and tools to manage and supervise production, changes, configurations, incidents and problems, data, environments, etc.

- ▶ The IT department has described its organisation and mapped its internal processes in these fields. It must be able to justify how it steers its activities through dashboards, indicators, or steering committees. Furthermore, it must ensure that it complies with the required certifications in its sector.

Criterion 2

The IT department controls the scheduled works and planned service interruptions.

- ▶ The IT department is able to analyse the impact of degraded performance or interrupted service on its clients' activities. Scheduled works are agreed with the business unit.

Criterion 3

The IT department communicates efficiently with its clients in case of incident.

- ▶ The IT department has up-to-date knowledge of the organisations and user networks that may be impacted by the incident. The means of communication should be appropriate for the type of incident.

NOTES...

BUDGET & PERFORMANCE

STEER IT BUDGET AND PERFORMANCE

STAKES FOR THE COMPANY

1

Align IT's performance objectives with the company's objectives.

2

Ensure that IT performance objectives are reached by providing the best resource allocation at the lowest cost.

3

Control the IT budget (recurring operations and projects).

4

Involve the various stakeholders (Executive Committee, business units, IT department) in managing IT by communicating on its performance.

THREATS TO THE COMPANY

1

Make poor decisions due to a lack of control over all cost elements.

2

No control over factors leading to projects "slippage".

3

Causing misunderstandings between General Management, the finance department, business unit directors and the IT departments over the IT budget and the costs of the services the IT department provides to its clients, which can result in a loss of trust that hinders reaching the company's objectives.



RELATED RISK FACTORS

1

A lack of understanding of the company's objectives and business units' expectations.

2

A lack of understanding of IT's contribution to the company's objectives.

3

Absence of IT roadmap or project portfolio management.

4

A lack of a structured process to track IT performance and budget.

5

A lack of business sense and skills in IT management control.

BEST PRACTICES

1

IT performance objectives aligned with those of the company.



2

Indicators to measure performance and reach objectives.



3

Budget is managed with a General Management arbitration process.



4

Service costs are calculated to share responsibility with the business units.



5

Projects are tracked in terms of costs, deadlines and features.



Best practice 1: IT PERFORMANCE OBJECTIVES.

The steering of the IT department relies on all IT performance objectives aligned with those of the company.

Criterion 1

The IT department has identified priority objectives, highlighting their contribution to those of the company (see [VECTOR 1 -STRATEGY](#)) and structuring them according to the six aspects of the *AFAI IT Scorecard*.

1. Contribution to business unit value creation
2. Control of IT-related risks
3. Consideration for IT client expectations
4. Performance of IT processes (build, run, changes)
5. Cost control of services rendered by IT to its clients
6. Management of IT skills and preparing for the future

Criterion 2

The IT department's objectives are communicated to all stakeholders (IT department employees, digital or external clients, top management of other departments, Executive Committee, partners, etc.).

- ▶ Objectives must be SMART (Simple, Measurable, Achievable, Realistic and Time-based).
- ▶ The objectives are documented to be understood by all stakeholders.
- ▶ Some objectives may be derived from external certification requirements (ISO 9001, ISO 2700x, etc.).

Criterion 3

The objectives are reviewed at least annually based on the measures observed, their level of achievement and the company's strategy.

Best practice 2: INDICATORS.

Indicators for measuring IT performance and the level of achievement of IT department objectives are defined, monitored and shared regularly with stakeholders.

Criterion 1

Performance measurement indicators (quantitative and qualitative) are formalised in dashboards. They measure the level of achievement of the IT department's objectives (see [best practice 1](#)).

- ▶ The IT Scorecard published by AFAI can be used to find examples of indicators.
- ▶ These indicators are formally defined. For quantitative aspects, the data used to measure the indicator should be extracted, if possible, in an automated way from existing IT.

Criterion 2

Improvement objectives are associated with performance measurement indicators.

- ▶ The service commitments negotiated with business units are measured by these indicators.

Criterion 3

Means of measuring and controlling the achievement of objectives (definition of indicators, regular measurements) are in place at the IT department level.

- ▶ The IT department analyses the results of these indicators and their discrepancies from the objectives to implement any corrective actions.

Criterion 4

Performance measurement indicators are reviewed and updated as necessary (changes in strategy or company or IT department objectives) to allow for improvements in measuring performance.

- ▶ The rules for managing indicators must result from shared management rules.

Criterion 5

The performance indicators are consolidated into dashboards that are regularly shared with stakeholders and General Management in a suitable format that shows everyone's contribution.

- ▶ With a view to transparency and improved communication, the IT department publishes and periodically shares dashboards with stakeholders and General Management summarising the levels and trends of these indicators.
- ▶ These should be published 'as it happens' to give the most up-to-date view of performance.
- ▶ These dashboards can also be shared with IT department employees for management purposes.

Best practice 3: BUDGET.

The IT department has implemented a budget management process to manage arbitrations with General Management and the business units relating to projects, changes and recurring operations.

Criterion 1

There is a budget consolidating all IT costs (in and outside IT department).

- ▶ This budget consolidates not only the costs placed under the responsibility of the IT department but also those of IT entities or IT representatives that report to operational or functional departments.

Criterion 2

The IT sector's budget is built on the basis of types of expenditures that are adapted to IT and of responsibility centres.

- ▶ [Cigref's model of analysis and benchmarking of IT costs \(in French\)](#) indicates the list of types of expenses to be taken into account (including amortisation, premises, etc.)
- ▶ Centres assigned to IT managers should group together all the expenses for which they have the initiative.
- ▶ Distributed costs (structure, premises, etc.) may also be included in the responsibility centres to obtain a full cost of centres' activities, but they must be clearly separated from direct expenses.

Criterion 3

The IT budget identifies the resources allocated to projects (transformation), ongoing maintenance and other recurrent costs, especially IT production.

- ▶ This split into at least three parts is essential because each one is steered in a different way:
 - ▶ For projects, this is an investment that must be "profitable" for the company,
 - ▶ For recurring costs, we are closer to a "factory" (placed under the organisational or functional responsibility of the IT department) for the production of IT services whose costs must be optimised,
 - ▶ Changes, in turn, must fall within a budgetary framework negotiated based on the application's domain.

Criterion 4

The IT department's budget drafting process has been formalised. The roles and responsibilities of the budget process are formally assigned (drafting, tracking discrepancies, updates, etc.). There is a clearly defined arbitration process.

- ▶ Setting up an IT management control system is recommended for this process to work.
- ▶ The management control helps elaborate the budget and its revisions, tracks achievements by cost centres and expenses type by comparing them both to the budget and to previous years.
- ▶ Spending is also tracked 'on commitment' to anticipate any drifts.

Best practice 4: SERVICE COSTS.

The IT department calculates the complete cost of the IT services in the catalogue provided to its clients by breaking it down into unit costs and volumes to share IT cost responsibilities with business units.

Criterion 1

A customer services catalogue has been defined with IT department clients and covers all the services provided.

- ▶ The catalogue is client-oriented (the business unit can read and understand it).
- ▶ It includes the provision of workstations, application and any changes and projects.
- ▶ It can also include services such as consulting, expertise, etc.
- ▶ It is placed at a level where making service-level agreements is possible.

Criterion 2

The IT department has identified all of its activities.

- ▶ [Cigref's model of analysis and benchmarking of IT costs \(in French\)](#) provides a typical list of activities that can be found in almost all IT departments.

Criterion 3

The unit cost of services rendered to IT clients is calculated with a recognised Activity-Based Costing (ABC) method which allows us to clearly explain its changes and to steer them.

- ▶ By applying the ABC method, the calculation of justifiable unit costs should allow to:
 - ▶ Ask questions with IT department clients such as the cost of SLA requirements, potential decommissioning of certain applications based on cost per user,
 - ▶ Bill IT department clients for the cost of services,
 - ▶ Make benchmarking easier,
 - ▶ Highlight the IT department's productivity (change in the unit cost according to services rendered).
- ▶ For this, IT department managers must understand their contribution to the complete cost of the services provided to be able to steer them by acting on the levers for which they are responsible.

Best practice 5: PROJECTS.

For the aspects of costs, deadlines, and features delivered, and for each project, the IT department tracks, activities under its control that may impact the business case.

Criterion 1

Projects' economic monitoring is linked to their operational management.

- ▶ Ideally, the operational and business monitoring use a shared tracking tool or, at the very least, a shared repository.

Criterion 2

A consolidation of the tracking of costs, deadlines and delivered features is linked to the project portfolio management (See VECTOR 6 - PROJECT PORTFOLIO).

Criterion 3

There is a project monitoring dashboard that is shared with the executives of the business units concerned.

Criterion 4

The discrepancies between real and estimates are flagged to the steering committees and, for strategic projects, to the Executive Committee.

Criterion 5

The business case is updated if discrepancies require it.

NOTES...

MARKETING & COMMUNICATION

SHOWCASE SERVICES AND COMMUNICATE
ON THE TECHNOLOGICAL CHALLENGES

STAKES FOR THE COMPANY

1

Evolve the IT department's image to one strategic actor with high added value.

2

Be transparent about IT performance to foster business units' understanding of the IT department's work and stakes.

3

Encourage employees engagement to digital transformation plans.

4

Anticipate and be able to communicate during crisis situations.

THREATS TO THE COMPANY

1

A lack of transparency and loss of information that could encourage the developpement of Shadow IT and harm the IT department's image among its internal clients.

2

A negative 'black box' or 'ivory tower' effect toward end users.

3

A lack of attractiveness for talent to join the IT department and the company.

RELATED RISK FACTORS

1

A misunderstanding of the company's strategy, and a misalignment of the IT and the company's strategies.

2

No communication process with business units.

3

Underestimating the cultural impact of transformation projects.

4

A lack of crisis communication and crisis management methodology.

BEST PRACTICES

1

The IT department's marketing function is organised and IT client-oriented.



2

Communication plan formalised and shared.



3

Internal IT department communication.



4

Internal company communication.



5

Crisis situation communication is anticipated.



Best practice 1: IT DEPARTMENT'S MARKETING FUNCTION.

The IT department markets its services to its clients.

Criterion 1

The IT department has a marketing function and implements a structured communication strategy.

- ▶ 'User clubs' and events around the IT department's projects and services are organised and held.
- ▶ IT projects have support for change management and in operational communications to users.

Criterion 2

The IT department's marketing function builds a relationship with its clients.

- ▶ It is responsible for relationships with the IT department's clients.
- ▶ It has a precise understanding of users' needs for the IT department's services.
- ▶ It regularly measures and improves satisfaction among IT's users and clients (user surveys, support hot surveys, etc.).
- ▶ It develops its client and user knowledge (client and user knowledge bases, segmentation, profiling, etc.).

Criterion 3

The IT department's marketing function defines, capitalises on, streamlines, and markets/publishes the IT department's offer of services.

- ▶ The IT department's offer of services and services catalogue are promoted to clients and users. (See [VECTOR 10 - SERVICES](#))

Criterion 4

The IT department's marketing function manages user and client satisfaction.

- ▶ The quality of service and the customer experience are promoted to clients and users (satisfaction, respect for SLAs, incident communication, etc.).
- ▶ The development of project SLAs, the definition and tracking of service commitments and the publication of service monitoring can be put in place.

Criterion 5

Performance indicators for the IT department's marketing performance are defined.

- ▶ For example, client satisfaction index, number of client and user events held, uptake rate for new services.

Best practice 2: COMMUNICATION PLAN.

The IT department communicates according to a formal, structured, and shared communication plan.

Criterion 1

The IT communication plan is an important aspect of the IT department's strategy.

- ▶ The IT department must integrate issues related to the subject of IT communications as a required element and include it in its agenda.
- ▶ This criterion is in line with [VECTOR 1 - STRATEGY](#).

Criterion 2

A communication dedicated to IT is defined and materialised within the IT department's communication plan. The IT performance dashboards are used as communication tools, and their content is adapted according to the target population.

- ▶ The IT communication plan is shared with the company's communication department.

Criterion 3

The communication plan is approved by top management, distributed and updated once a year.

- ▶ An annual meeting is organised with top management to approve the communication plan and update it where necessary.

Criterion 4

The communication plan identifies and segments all the audiences to whom the IT department communicates.

- ▶ For example, employees, project managers, IT department actors, other company members including General Management, end users, etc.

Criterion 5

The IT department's communication plan is aligned with the company's overall and strategic communication strategy and, in particular, takes into account innovation ideas and cyber risks.

- ▶ IT communication must not come into conflict with the company's overall communication strategy, and it must be coherent so as to not be counter-productive.

Criterion 6

Crisis communication is a priority in the communication plan and is proportionate to the risks.

- ▶ Crisis situations give rise to special and exceptional communications that must be elaborated with the company's crisis communication teams and receive dedicated support.
- ▶ The scenarios must be anticipated and be subject to regular drills involving all stakeholders in the IT department.

Criterion 7

Actions are regularly implemented to measure the impact and effectiveness of communications, and these results are used in updating the communication plan.

- ▶ Feedback is used to improve communication.

Best practice 3: INTERNAL IT DEPARTMENT COMMUNICATION.

Communication within the IT department is regular and organised.

Criterion 1

The internal IT department communication actions have been defined.

- ▶ In-house IT department employees' awareness is raised through traditional internal communication channels, newsletters, emails, the intranet, and the company's social network on topics for which they should be informed such as regulations.

Criterion 2

Communications take the form a distribution of information to the various IT functions representatives. They must be proactive and qualitative.

- ▶ Communication seeks to be extra-transactional and go beyond the communication of figures related to incident resolution, for example.
- ▶ Communication is proactive since it should not take place only during crises or service interruptions.

Criterion 3

Various channels have been identified and are used according to the type of communication and target audience, prioritising the company's usual in-house communication channels.

- ▶ For example, emails, text messages, posters, flyers, videos, intranet, corporate social network, etc.

Criterion 4

Communication takes the form of a commitment to the various IT functions using presentation-based formats for individual, verbal communication.

- ▶ For example, presentation conferences, face-to-face discussions, presentations, workshops, IT department management road shows, etc.

Criterion 5

The managers of the various IT functions are involved in designing, creating and distributing communications. IT internal communication integrates digital clients' strategic objectives.

Criterion 6

Communications impacts towards the various IT functions is periodically analysed and improved.

- ▶ Resources such as satisfaction surveys can be used.

Best practice 4: INTERNAL COMPANY COMMUNICATION.

The IT department sends communications to other company actors in an organised and regular way.

Criterion 1

Communication actions to actors outside the IT department have been defined.

- ▶ Actors outside the IT department are business units, General Management, etc.

Criterion 2

The communications take the form a distribution of information to company executives. They must be proactive and qualitative.

- ▶ Communications share uses, security and cybersecurity practices concerning social networks, in particular, a guide to using new technologies and new legislation (for example, GDPR).
- ▶ Communication seeks to be extra-transactional and go beyond the communication of figures related to incident resolution, for example.
- ▶ Communication is proactive since it should not take place only during crises or service interruptions.

Criterion 3

Various channels have been identified and are used according to the type of communication and target audience.

- ▶ For example, emails, newsletters, TV screens, etc.

Criterion 4

Communication takes the form of a commitment from the various IT functions made aware of their roles as ambassadors and guarantors of the IT department's image to other stakeholders by using resources that allow for individual, verbal communication.

- ▶ For example, presentation conferences, face-to-face discussions, presentations, workshops, IT department management road shows, etc.

Criterion 5

The various IT representatives are involved in designing, creating and distributing communications. Communication integrates stakeholders' strategic objectives.

Criterion 6

Communications impacts is periodically analysed and improved.

- ▶ Resources such as satisfaction surveys can be used.
- ▶ An acknowledgement of innovation or cyber risks can lead to updates to this communication.

Criterion 7

The IT department communicates on its contribution to the company's CSR policy (diversity, disability, the environment, energy, etc.).

Best practice 5: CRISIS SITUATIONS.

Communications in case of an IT-related crisis are formalised and shared ahead of time to anticipate the situation.

Criterion 1

IT-related crisis communications are based on a related procedure. Crisis communications must take into account the importance and speed of cyber attacks.

- ▶ By crisis, we mean any exceptional situation that can represent a real risk to the company or IT's operations.
- ▶ Given the speed of potential impacts in the case of cyber attacks, the company should have reflected on its speed of reaction.
- ▶ The communication on incidents outside the company is made according to established rules.
- ▶ This criterion and best practice are connected to [VECTOR 3 · RISKS](#).

Criterion 2

Major risks that could lead to a crisis situation have been identified and the subject of coherent crisis communication coordination among the various actors (IT, functional workers, operators, managers).

- ▶ For example, internet service interruption, intrusion into the information system, phishing, etc.

Criterion 3

Crisis communications are approved and sent to company actors and/or entities.

Criterion 4

Tools and/or resources that provide valid communication between actors in times of crisis have been defined.

- ▶ Appropriate tools and resources have been identified to make communication as efficient as possible.

Criterion 5

Crisis communication drills are held regularly.

- ▶ Crisis situations can be simulated to test the organisation's communications maturity during crisis situations.

Criterion 6

Feedback is gathered to learn lessons and improve reactions.

- ▶ One of the goals is to practice continuous improvement in the crisis management procedure.

BIBLIOGRAPHY

Reference frameworks

- ▶ [EN] [COBIT2019](#) / AFAI-ISACA
- ▶ COBIT5 for risk / AFAI-ISACA
- ▶ COBIT5 for security/ AFAI-ISACA
- ▶ Risk IT Framework / AFAI-ISACA
- ▶ ITIL Version 3 / ITIL Foundation
- ▶ [GTAGs – Global Technology Audit Guides](#) / IIA

Governance / Strategy

- ▶ [Digital ethics: a guide for professionals of the digital age](#)/ Cigref - 2018
- ▶ [Agile at scale](#) / Cigref – 2018
- ▶ [FR] [Open Innovation, réponse aux challenges de l'entreprise](#) (Open innovation, a response to business challenges) / Cigref - 2018
- ▶ [FR] [Entreprise, les clés d'une application réussie du GDPR](#) (Company, the keys to applying GDPR successfully / AFAI-ISACA, Cigref, TECH IN France - 2017
- ▶ [FR] [Gouvernance du numérique](#) (Digital governance) / Cigref - 2014
- ▶ [FR] Le pilotage du SI par l'entreprise - les nouveaux tableaux de bord de l'IT Scorecard (Steering your company's IT - the new IT Scorecard dashboards) / AFAI-ISACA- 2011

Risks

- ▶ [« Risk in focus » Survey](#) / IFACI – 2018
- ▶ [Cybersecurity: Visualize, Understand, Decide](#) / Cigref – 2018
- ▶ [FR] [Cyber-risques : Enjeux, approches et gouvernance](#) (Cyber-risks : Stakes, approaches, and governance) / IFACI – 2018
- ▶ [FR] [L'entreprise face à ses enjeux et risques numériques](#) (Companies' digital challenges and risks) / AFAI-ISACA, Cigref, Crowe Horwath, IFACI - 2015

Information system

- ▶ [EN] [Software Asset & Cloud Management](#) / Cigref – 2018
- ▶ [FR] La contribution du système d'information à la valeur de l'entreprise : démarche, cas concrets (IT's contribution to company value: approach and concrete cases / AFAI-ISACA.
- ▶ [FR] [Modèle d'analyse et de benchmarking des coûts informatiques](#) (IT cost benchmarking and analysis model) / Cigref – 2018.
- ▶ [FR] [Valorisation des données dans les grandes entreprises](#) (Valuable use of data in large companies) / Cigref – 2016
- ▶ [FR] [Cloud Computing et protection des données dans le cloud](#) (Cloud computing and protecting data in the cloud) / AFAI-ISACA, Cigref - 2013

ACRONYMS

- ▶ **ABC : Activity-Based Costing**
- ▶ **MVP: Minimum Viable Product**
- ▶ **PoC: Proof of Concept**
- ▶ **IT : Information Technology**
- ▶ **SOC: Security Operational Center**

GLOSSARY

- ▶ **Business Case:** a document whose goal is to justify investments of time or money in a new project. It must explain what company process, activity, or product is concerned and detail the project's objectives (Source : thebusinessplanshop).
- ▶ **Core IT:** IT inherited from all the changes that have occurred up to now, also called legacy system.
- ▶ **Cyber-risk:** there are 4 types of cyber-risks with various consequences that directly or indirectly affect individuals, administrations and businesses: cybercrime, image damage, espionage, and sabotage (Source: Gouvernement.fr)
- ▶ **Cybersecurity:** a key requirement for an information system, enabling it to withstand cyberspace events that may compromise the availability, integrity or compliance of stored, processed, or transmitted data, and related services provided or made accessible by these systems (Source: ANSSI).
- ▶ **DevOps:** mixing tasks performed by a company's application development (Dev) and systems operations (Ops, for operations) teams (Source: LeMagIT)
- ▶ **Fast IT:** agile computing using innovative technologies, exploiting (produced, stored, shared, analysed) data to respond to new uses, cultures and organisations (social, collaborative, connected, etc.)
- ▶ **Computer science:** the science of rational processing, especially by automated machines, of information considered as the support of human knowledge and communications in the technical, economic and social fields.
- ▶ **Agile method:** a project management method based on very short development cycles (called 'Sprints') for continuous improvement. An initial version of the expected deliverable called the Minimum Viable Product (MVP) is delivered quickly and then stabilised and refined over iterative development cycles.
- ▶ **"Digital":** all technologies beyond the company's IT that operates with it and that enriches it.
- ▶ **IT roadmap:** the operational version of the digital/IT section of the company's strategic plan.
- ▶ **IT:** a set of resources (staff, software, processes, data, hardware, computing science and telecommunications equipment, etc.) allowing the collection, storage, structuring, modelling, management, manipulation, analysis, transport, exchange and distribution of information (texts, images, sounds, video, etc.) within an organisation.

EVALUATION TOOL

free download



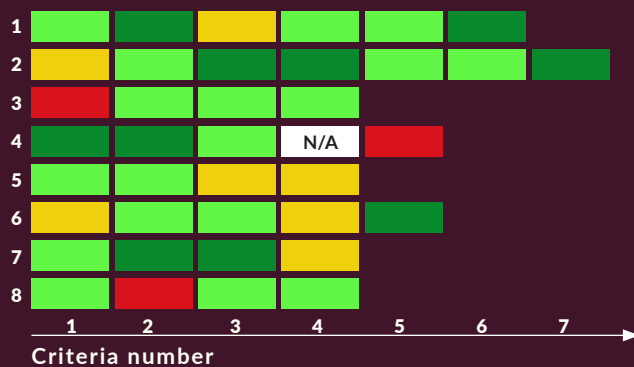
EVALUATION TOOL XLS

The evaluation tool (xls) offers a matrix with best practices on the horizontal axis and criteria on the vertical axis. The scale includes four colours without an 'average' option to force an evaluation. This does not give a final score but a 'wall of colours' giving a snapshot of a certain shade creating an overall scoring.

EVALUATION EXAMPLE

STAGE 1 EVALUATION OF EACH CRITERION

Best
Practices



STAGE 2 EVALUATION OF EACH PRACTICE



Low

Insufficient

Satisfactory

Good

Not applicable

STAGE 3 EVALUATION OF THE VECTOR



AFAI-ISACA

WWW.AFAI.FR

3 rue du Colonel Moll

75017 Paris

+33 1 40 08 47 81

afai@afai.fr

CIGREF

WWW.CIGREF.FR

21 avenue de Messine

75008 Paris

+ 33 1 56 59 70 00

cigref@cigref.fr

IFACI

WWW.IFACI.COM

98 bis boulevard Haussmann

75008 Paris

+33 1 40 08 48 00

institut@ifaci.com

IT GOVERNANCE AUDIT GUIDE FOR COMPANIES IN THE DIGITAL ERA