MS4ICT – Official Method

Management System for ICT

Unified Risk-Based ICT Governance

An international ICT governance method based on risk,
linking events, risks, obligations, controls, and responsibilities
within a coherent, explainable, and sustainable framework.
Version 1.0

Normative method – tool-agnostic

ISBN: 978-99987-651-1-5

Legal deposit: May 2026
National Library of Luxembourg

Publisher: Didier BARELLA / BARELLA.APP®
Place of publication: Luxembourg

Status, Uses, and Governance of the MS4ICT Method

STATUS OF THE MS4ICT METHOD

The MS4ICT method (Management System for ICT) constitutes an original methodological framework for ICT governance, based on risk, coherence, traceability, and decision explainability.

This document defines the official reference version of the MS4ICT method, identified as:

"MS4ICT – Official Method – Version 1.0".

This version is authoritative for any use, reference, implementation, or interpretation of the MS4ICT method as of its date of publication.

The MS4ICT method is independent of any specific tool, technology, software solution, or organization.

Any implementation results from the voluntary application of the method by organizations and remains under their sole responsibility.

Any evolution of the MS4ICT method (new version, amendment, clarification, extension, or update) falls exclusively under the authority of its author and is subject to an explicitly identified official version.

Any adaptation, interpretation, implementation, or derivative application of the method shall not be considered a modification of the method itself, nor an official version of MS4ICT.

The principles, coherence rules, definitions, and concepts described in this document are normative within the MS4ICT method and prevail over any external interpretation.

MS4ICT is a governance method.

It is neither a legal standard, nor a certification, nor a software tool, nor an operational procedure.

EDITORIAL REFERENCE

This document is referenced under the following ISBN:

ISBN: 978-99987-651-1-5

The assignment of an ISBN serves solely as a bibliographic reference for the document.

It does not confer any external normative status on the method, nor does it in any way limit the version governance, controlled evolution, or the author's authority over the MS4ICT method.

AUTHORIZED USES OF THE MS4ICT METHOD

The MS4ICT method may be used by any organization, whether a natural or legal person, for the purposes of analyzing, structuring, implementing, or improving ICT governance, subject to strict compliance with the principles, rules, and definitions described in this document.

Authorized uses include, in particular:

- the use of MS4ICT as an ICT governance methodological framework;
- the application of the method within an internal organizational context, whether public or private;
- the implementation of the method through any tool, medium, or solution, in compliance with the principle of separation between the method and its implementation;
- explicit reference to the MS4ICT method in analysis, governance, audit, consulting, or research activities.

The following uses are not authorized without the prior written consent of the author:

- any modification, alteration, or adaptation of the principles, coherence rules, definitions, or concepts constitutive of the method;
- the dissemination of a modified version presented as “compliant”, “derived”, “equivalent”, or “adapted” to MS4ICT;
- the use of the name MS4ICT to designate a method, framework, tool, or offering that does not fully comply with the official method;
- the presentation of an implementation as an official, standardized, or normative version of the MS4ICT method.

Any use of the MS4ICT method implies explicit recognition of its author and respect for the methodological integrity of the method.

USE OF THE MS4ICT METHOD BY SOFTWARE PUBLISHERS

The MS4ICT method may be used by software publishers, platforms, or tool-based solutions for the purposes of implementing or facilitating ICT governance, subject to strict respect for the methodological integrity of the method.

In particular, a software publisher may:

- implement the MS4ICT method within a software solution or platform, provided that all the principles, coherence rules, and definitions of the method are fully respected;
- explicitly refer to MS4ICT as a governance methodological framework, subject to a clear distinction between the method and the tool;
- offer functionalities that support the application of the method, without modifying its structure, principles, or underlying logic.

Software publishers are not authorized to:

- modify, simplify, interpret, or circumvent the foundational principles of the MS4ICT method;
- present a tool as equivalent to, derived from, a substitute for, or an adaptation of the method;
- claim implicit, partial, or self-declared compliance with MS4ICT;
- present a solution as an "official version", a "certification", or an "MS4ICT standard".

Any reference to MS4ICT in a software context must explicitly acknowledge that the method is independent of the tool and cannot be equated with a technological solution.

COMPLIANCE FRAMEWORK AND FUTURE CERTIFICATION

The MS4ICT method may, in the future, be subject to a formal framework for recognition, compliance, or certification, in particular for software or organizational implementations.

Any such framework, potentially designated under a name such as *"MS4ICT Compliant"*, shall fall exclusively under:

- the definition,
- the governance,
- the criteria, and
- the formal attribution

by the author of the method or by an entity explicitly mandated to do so.

In the absence of such an officially published framework, no entity, tool, or implementation may claim to be MS4ICT-compliant, certified, or recognized, in any form whatsoever.

USE OF THE MS4ICT NAME AND LOGO

The name MS4ICT and the MS4ICT logo constitute identity elements of the method.

The use of the MS4ICT logo for commercial, promotional, marketing, institutional, or product-related purposes is strictly prohibited without the prior written consent of the author.

Any unauthorized use of the MS4ICT name or logo that may create confusion between the method, an implementation, a tool, or a commercial offering is prohibited.

TABLE OF CONTENT

1 INTRODUCTION

For more than a decade, the management of information technologies has evolved within an environment marked by a proliferation of standards, regulations, and compliance requirements. ISO/IEC standards, NIS2, DORA, the AI Act, the NIST Cybersecurity Framework, as well as ENISA publications - each framework brings its own logic, vocabulary, and obligations. This growing complexity has gradually fragmented organizations, creating silos between ICT, cybersecurity, compliance, legal, risk management, and executive teams.

In light of this situation, an evident conclusion has emerged: all these frameworks are built upon a common denominator - risk management. It is from this fundamental convergence that the MS4ICT method (Management System for ICT) was developed: a pragmatic framework designed to simplify, harmonize, and unify ICT governance within organizations.

MS4ICT provides a structured approach that enables organizations to:

- align standards and regulations on a common foundation;
- establish a shared language across disciplines;
- eliminate information duplication;
- strengthen coherence between responsibilities, risks, events, and controls;
- and deliver an integrated view of ICT governance.

Based on international reference frameworks (ISO/IEC), ENISA publications, and European regulatory requirements, the method relies on a modular architecture structured around coherent reference frameworks: context, responsibilities, risk events, risks, and controls. It enables the linkage of causes, impacts, and obligations, while offering role-specific views tailored to ICT, risk, compliance, legal, DPO, and executive functions.

MS4ICT is not a tool, but a methodological engine — an engine capable of creating multidimensional links, revealing dependencies, and providing a unified reading of the entire ICT management system.

2 CONTEXT AND CHALLENGE OF ICT GOVERNANCE

2.1 A CONSTANTLY EVOLVING DIGITAL ENVIRONMENT

Organizations operate in a digital landscape that is constantly evolving.

Dependence on technologies has increased, information systems have become more interconnected, more exposed, and more critical to business operations.

At the same time, risks associated with ICT have intensified: cyber threats, service failures, dependencies on third parties, and incidents affecting the availability, integrity, or confidentiality of information.

ICT governance is no longer a purely technical matter; it has become a strategic issue for the continuity, compliance, and resilience of organizations.

Proliferation of Normative and Regulatory Frameworks

Normative and regulatory requirements have multiplied significantly.

Organizations must now contend with numerous national, European, and international frameworks, including:

- information security standards;
- cybersecurity and resilience regulations;
- data protection requirements;
- frameworks specific to emerging technologies, particularly artificial intelligence.

Each of these frameworks provides a partial response to a legitimate need.

However, when considered individually, they do not provide a comprehensive and coherent view of ICT governance.

2.2 FRAGMENTATION OF RESPONSIBILITIES AND SILOED WORKING

In this context, organizations are often structured in silos.

ICT, cybersecurity, compliance, legal, data, AI, and executive teams operate with:

- distinct reference frameworks;
- sometimes diverging priorities;
- different languages and levels of interpretation.

This fragmentation complicates coordination, dilutes responsibilities, and makes it difficult to clearly assign decisions and actions.

It also fosters duplication of efforts and the emergence of grey areas within ICT governance.

2.2.1 The Paradox of Modern ICT Governance

A paradox emerges:

never have organizations needed ICT governance so much, and never has it been so difficult to structure it in a coherent manner.

Frameworks exist, obligations are known, and controls are often in place, yet the overall system lacks global coherence.

As a result, governance becomes difficult to explain, to justify, and to manage, both for operational teams and for executive management.

2.2.2 Challenges for Organizations

In response to this situation, organizations are facing several major challenges:

- ensuring coherence between risks, obligations, controls, and responsibilities;
- making governance understandable and explainable to all stakeholders;
- avoiding duplication and inconsistencies between normative and regulatory frameworks;
- improving the traceability of decisions and their justifications;
- enabling effective and sustainable steering of ICT governance over time.

These challenges constitute the starting point for any methodological reflection on ICT governance.

2.3 Positioning of the MS4ICT Method

2.3.1 A Method, Not an Additional Standard

MS4ICT is not intended to create a new standard, a new norm, or a competing framework alongside those that already exist.

Today, organizations have access to numerous regulatory and normative reference frameworks that are widely recognized and legitimate.

The challenge they face is not the absence of frameworks, but their unharmonized coexistence.

MS4ICT is positioned as a method of unification and coherence, capable of linking these frameworks together without replacing them.

2.3.2 A Methodological Response to the Challenges of ICT Governance

In response to the growing complexity of ICT governance, MS4ICT proposes a structured, explainable, and sustainable approach.

The method is designed to address the identified challenges directly:

- lack of coherence between reference frameworks;
- difficulty in explaining and justifying decisions;
- fragmentation of responsibilities;
- absence of a global and cross-functional view.

MS4ICT provides a methodological framework that enables ICT governance to be structured, interconnected, and steered in a clear and controlled manner.

2.3.3 Governance Based on Risk

Risk is both the entry point and the endpoint of the method.

MS4ICT adopts a risk-driven governance approach, in which:

- obligations are analysed through their impacts;
- controls are justified by the risks they are designed to cover;
- responsibilities are assigned based on the decisions to be made.

This approach makes it possible to move beyond a purely documentary or declarative form of governance, in favour of governance oriented toward prioritisation, impact, and action.

2.3.4 A Unified and Modular Method

MS4ICT is based on a deliberately simple structure, composed of clearly defined and interconnected reference frameworks.

Each reference framework addresses a specific need, while remaining fully consistent with the overall structure.

The method is modular:

- each component can be enriched or adapted,
- without calling into question the overall balance,
- nor the coherence of governance.

This modularity ensures the durability of the method within a constantly evolving normative and technological environment.

2.3.5 An Explainable and Traceable Method

One of the core objectives of MS4ICT is to make ICT governance explainable.

Each decision, each control, and each responsibility must be understandable, justified, and defensible.

MS4ICT promotes full traceability:

- why a risk exists;
- why an obligation applies;
- why a control is selected;
- why a responsibility is assigned.

This traceability is essential for internal steering, audits, and strategic decision-making.

2.3.6 A Universal Framework Independent of Tooling

MS4ICT is deliberately independent of any technology.

The method can be applied in a wide range of contexts:

- GRC tools,
- wikis,
- spreadsheets,
- specialised platforms,
- or dedicated solutions.

It defines **what** must be done and **why**, never the technical **how**.

Any implementation pertains to tooling and must not influence or constrain the method itself.

2.3.7 Global Positioning of MS4ICT

In summary, MS4ICT is positioned as:

- an ICT governance method;
- a unified, risk-based framework;
- a common language shared by ICT, cybersecurity, compliance, legal, executive management, and AI governance;
- a coherence engine that connects existing frameworks without replacing them.

MS4ICT therefore provides a stable, explainable, and sustainable methodological foundation upon which organizations can build coherent and controlled ICT governance.

3 FOUNDING PRINCIPLES OF THE MS4ICT METHOD

The MS4ICT method is based on a set of **founding principles** that structure the entirety of ICT governance.

- These principles are neither theoretical nor optional;
- they constitute the invariant rules upon which
- the coherence, readability, and durability of the method are built.

They apply to all reference frameworks, decisions, and uses of MS4ICT.

3.1 PRINCIPLE 1 – COHERENCE

ICT governance can only be effective if the elements that compose it are coherent with one another.

Within MS4ICT, no element exists in isolation:

- a control never exists without a risk;
- a risk never exists without an event;
- an obligation is never addressed without justification;
- a responsibility is never assigned without intent.

Each element must have:

- an identifiable origin;
- an explicit rationale;
- a clear destination.

Coherence is the primary condition for governance that is understandable and defensible.

3.2 PRINCIPLE 2 – TRACEABILITY

Every governance decision must be traceable.

MS4ICT requires full traceability of the links between:

- events,
- risks,
- obligations,
- controls,
- responsibilities,
- context.

This traceability makes it possible to answer, without ambiguity, the following questions:

- why this risk exists;
- why this obligation applies;
- why this control was selected;
- why this responsibility was assigned.

Traceability is not a documentary objective; it is a tool for steering, auditing, and sustainable governance.

3.3 Principle 3 – Explainability

Governance that cannot be explained can neither be applied nor accepted.

MS4ICT promotes an explainable approach, accessible to all stakeholders:

- executive management,
- ICT,
- cybersecurity,
- compliance,
- legal,
- DPO,
- AI governance.

Concepts are clearly defined, relationships are understandable, and decisions can be justified without relying solely on highly technical or purely normative language.

Explainability is an essential condition for acceptance, accountability, and informed decision-making.

3.4 Principle 4 – Normative Alignment

MS4ICT does not create new obligations.

The method aims to harmonize and align existing normative and regulatory frameworks.

A single risk may be subject to multiple obligations, and a single control may simultaneously address:

- international standards;
- European regulations;
- sector-specific or contractual requirements.

MS4ICT makes these alignments visible, coherent, and justifiable, without artificially multiplying controls or reference frameworks.

3.5 Principle 5 – Risk-based Governance

Risk is both the entry point and the exit point of the method.

Within MS4ICT:

- events constitute the objective foundation;
- risks are constructed based on context;
- obligations are analysed through their impacts;
- controls are selected to reduce risks;
- responsibilities are assigned according to the decisions to be made.

This approach enables governance oriented toward:

- prioritisation,
- impact,
- action.

It avoids purely declarative governance or governance exclusively focused on documentary compliance.

3.6 SCOPE OF THE FOUNDING PRINCIPLES

The founding principles of MS4ICT:

- apply to the method as a whole;
- are independent of any tool;
- are non-negotiable;
- do not vary according to organizational context.

They constitute a stable framework, ensuring the coherence of the method over time and across diverse environments.

Any implementation of MS4ICT must comply with these principles, without adapting, circumventing, or weakening them.

4 MS4ICT ARCHITECTURE

4.1 OVERALL VIEW OF THE MS4ICT ARCHITECTURE

4.1.1 Objective of the MS4ICT Architecture

The MS4ICT architecture defines the logical structure of the method.

Its purpose is to provide a clear, coherent, and explainable organization of the elements required for ICT governance.

This architecture is neither technical nor tool-based.

It describes how methodological concepts are articulated with one another, independently of any implementation.

4.1.2 A Deliberately Simple and Structuring Architecture

The MS4ICT architecture is based on a fundamental principle:

ICT governance can only be mastered if its components are clearly identified and coherently interconnected.

To achieve this objective, MS4ICT relies on:

- distinct reference frameworks, each fulfilling a specific role;
- a coherence engine ensuring the links between these reference frameworks;
- a clear separation between content, relationships, and views.

This structural simplicity is an essential condition for the explainability and long-term sustainability of the method.

4.1.3 Structural Components of the Architecture

The MS4ICT architecture is composed of three major elements:

- the reference frameworks, which carry governance information;
- the coherence engine, which connects this information together;
- the views, which enable role-appropriate perspectives.

These components are inseparable: none of them can fulfil its role without the others.

4.1.4 Reference Frameworks as the Foundation of Governance

Reference frameworks constitute the informational foundation of MS4ICT.

They make it possible to explicitly structure:

- the organizational context;
- responsibilities;
- risk events;
- risks;
- controls.

Each reference framework is autonomous in its content, yet dependent in its meaning: it fully takes on its significance only when it is connected to the others.

4.1.5 The Coherence Engine as the Central Element

At the heart of the architecture lies the coherence engine.

Its role is to ensure systematic and traceable links between the different reference frameworks.

The coherence engine ensures that:

- each risk is linked to an event;
- each obligation is justified by a risk;
- each control is selected to address both a risk and an obligation;
- each responsibility is assigned with explicit intent.

4.2 MS4ICT Architecture – Logical Layers

4.2.1 Objective of the Logical Layers

The MS4ICT logical layers make it possible to structure ICT governance into distinct conceptual levels, each fulfilling a specific role.

They ensure a clear separation between the different types of governance information, while guaranteeing their overall coherence through the coherence engine.

These layers are neither technical nor organizational in nature.

They provide a methodological reading of ICT governance.

4.2.2 Principle of Layered Separation

ICT governance often fails when it conflates:

- context and impacts;
- causes and consequences;
- obligations and solutions;
- responsibilities and actions.

MS4ICT introduces a strict separation into logical layers in order to:

- reduce complexity;
- prevent confusion;
- strengthen explainability;
- ensure the traceability of decisions.

Each layer has its own specific function and does not substitute for the others.

4.2.2.1 Layer 1 – Context

The context layer constitutes the starting point of all ICT governance.

It describes the environment in which the organization operates.

This layer makes it possible to structure:

- the organizational scope;
- critical assets;
- entities and roles;
- applicable obligations;

- internal and external dependencies.

The context gives meaning to events, risks, and decisions.

Without context, no governance analysis is relevant.

4.2.2.2 Layer 2 – Risk Events

The risk events layer describes what may occur, independently of context or impacts.

A risk event is a factual occurrence that may affect the organization, for example:

- a service outage;
- a system compromise;
- a human error;
- a supplier failure.

This layer provides an objective and stable foundation, which is essential to avoid a purely subjective risk analysis.

4.2.2.3 Layer 3 – Risks

The risk layer transforms events into analysable and actionable objects by contextualizing them.

A risk is constructed through the combination of:

- an event;
- a context;
- impacts;
- associated obligations.

This layer enables:

- prioritisation;
- justification of decisions;
- alignment with normative and regulatory requirements.

Risk constitutes the central element of MS4ICT governance.

4.2.2.4 Layer 4 – Obligations

The obligations layer groups together requirements arising from:

- standards;
- laws and regulations;
- contracts;
- internal commitments.

Obligations are never addressed in isolation.

They are analysed through the risks to which they relate, in order to avoid purely declarative or documentary-driven governance.

This layer makes it possible to link compliance and risk management within a coherent and integrated approach.

4.2.2.5 Layer 5 - Controls

The controls layer translates governance decisions into concrete measures aimed at reducing risks and addressing obligations.

A control exists only if it:

- covers one or more identified risks;
- responds to one or more obligations;
- fits within the context of the organization.

This layer makes it possible to justify each control and to avoid redundant, unnecessary, or non-prioritized controls.

4.2.2.6 Layer 6 – Responsibilities

The responsibilities layer defines who is responsible for what, how, and with what intent.

Each responsibility is associated with:

- controls;
- risks;
- obligations;
- an explicit objective.

This layer puts an end to grey areas, implicit responsibilities, and unmanaged overlaps.

4.3 VIEWS AS A TRANSVERSAL PROJECTION

MS4ICT views do not constitute an additional layer.

They are transversal projections of the logical layers, tailored to the needs of different roles.

A view selects and organizes relevant information drawn from the existing layers, without creating new data or modifying the structure of the method.

4.4 ROLE OF THE LAYERS IN OVERALL COHERENCE

The MS4ICT logical layers never operate in isolation.

They are connected by the coherence engine, which ensures that each element:

- has a clearly identifiable origin;
- is justified;
- and fits within an explainable chain.

This layered structuring enables governance that is:

- readable;
- traceable;
- explainable;
- sustainable.

4.5 SYNTHESIS OF THE LOGICAL LAYERS

The logical layering enables MS4ICT to:

- clarify the roles of each governance component;
- avoid conceptual confusion;
- facilitate explanation and governance steering;
- prepare coherent implementations, without constraining them.

The logical layers constitute a stable reference framework that is essential to understanding and applying the MS4ICT method.

5 REFERENCE FRAMEWORKS

5.1 CONTEXT REFERENCE FRAMEWORK

5.1.1 Role of the Context Reference Framework

The context reference framework constitutes the mandatory starting point of all ICT governance within the MS4ICT method.

It makes it possible to describe the environment in which the organization operates and to give meaning to all the other reference frameworks.

Without a clearly defined context, it is neither possible to analyse risks in a relevant manner nor to justify governance decisions.

The context reference framework addresses a central question: in which environment is ICT governance exercised?

5.1.2 Purpose of the Context Reference Framework

The purpose of the context reference framework is to:

- define the scope of ICT governance;
- identify what is critical for the organization;
- make explicit the applicable constraints and obligations;
- provide a shared baseline of understanding for all stakeholders.

It is not intended to be an exhaustive inventory, but rather a methodological structuring of the context that is relevant for governance.

5.1.3 Constituent Elements of the Context

The context reference framework brings together the elements required to understand the governance environment, including in particular:

- the organizational scope covered by ICT governance;
- the entities, functions, and roles involved;
- critical assets, whether informational, technical, human, or third-party related;
- applicable normative, regulatory, and contractual obligations;
- significant internal and external dependencies;
- processes and services that are critical to the organization.

These elements are described at the level necessary for governance purposes, without going into technical or operational detail

5.1.4 The Context as the Foundation of Coherence

Within MS4ICT, the context feeds all other reference frameworks:

- it makes it possible to determine which events are relevant;
- it conditions the analysis and prioritisation of risks;
- it justifies the applicability of specific obligations;
- it influences the selection of controls;
- it informs the assignment of responsibilities.

The context therefore constitutes the foundation of the method's overall coherence.

5.1.5 Boundary Between Context and Implementation

The context reference framework is deliberately tool-independent.

It describes *what* must be considered, never *how* it must be implemented.

It is not intended to:

- replace a CMDB;
- provide a detailed technical inventory;
- document configurations or technical architectures.

Any concrete implementation of the context falls within the scope of tooling and must remain compliant with the methodological principles defined by MS4ICT.

5.1.6 Evolution of the Context Reference Framework

The context is not static.

It evolves with:

- organizational changes;
- regulatory developments;
- the emergence of new services or dependencies;
- technological transformations.

Any evolution of the context must be documented in order to preserve the traceability and coherence of governance decisions over time.

5.1.7 Position of the Context Reference Framework Within the Method

The context reference framework:

- is the first reference framework to be established;
- conditions the overall quality of ICT governance;
- serves as a common reference point for all stakeholders.

It constitutes the methodological foundation on which risk analysis and all coherence mechanisms of MS4ICT are built

5.2 RESPONSIBILITIES REFERENCE FRAMEWORK

5.2.1 Role of the Responsibilities Reference Framework

The responsibilities reference framework is one of the structuring pillars of the MS4ICT method.

It addresses a fundamental question that is too often neglected in ICT governance:

who is responsible for what, how, and with what intent?

The absence of clearly defined responsibilities is a major source of dysfunctions, grey areas, duplication of efforts, and conflicts within ICT governance.

5.2.2 Purpose of the Responsibilities Reference Framework

The purpose of the responsibilities reference framework is to:

- clarify responsibilities related to ICT governance;
- make accountability for decisions and actions explicit;
- eliminate implicit or assumed responsibilities;
- ensure coherence between responsibilities, risks, controls, and obligations.

It is not an organizational tool, but a methodological reference framework for governance.

5.2.3 The MS4ICT Responsibility Model

MS4ICT is based on a responsibility model structured around four inseparable dimensions:

5.2.3.1 Who

The “who” identifies the responsible role or entity.

It may refer to:

- a business role;
- an ICT role;
- a cybersecurity role;
- a compliance or legal role;
- an executive or management role.

MS4ICT prioritises roles rather than individuals, in order to ensure the sustainability and transferability of governance.

5.2.3.2 What

The “what” corresponds to the responsibility being exercised, that is, the expected action or decision.

Examples of responsibilities include:

- analysing a risk;
- validating a control;
- maintaining a reference framework;
- supervising a supplier;
- notifying an authority.

The “what” must be formulated in a clear, explicit, and unambiguous manner.

5.2.3.3 How

The “how” describes the means or methods used to exercise the responsibility.

It may refer to:

- processes;
- procedures;
- internal practices;
- methodological guidelines or frameworks.

The “how” remains deliberately tool-independent.

It describes an approach, never a technical implementation.

5.2.3.4 With What Intent

Intent is the differentiating element of the MS4ICT responsibility model.

It makes explicit why a responsibility exists:

- to reduce a risk;
- to address an obligation;
- to ensure a level of compliance;
- to ensure continuity or resilience;
- to protect critical assets.

Without explicit intent, a responsibility can neither be understood nor justified.

5.2.4 Responsibilities and Overall Coherence

Within MS4ICT, a responsibility never exists in isolation.

It is always associated:

- with one or more controls;
- which are themselves linked to risks;
- arising from events;
- contextualised;
- and associated with obligations.

The responsibilities reference framework directly feeds the coherence engine and ensures that each decision is assigned in a traceable and explainable manner.

5.2.5 Elimination of Grey Areas

The responsibilities reference framework makes it possible to explicitly address situations of overlapping or conflicting responsibilities.

When multiple roles are involved in the same subject matter, MS4ICT requires clarification of:

- the exact scope of each role;
- the nature of the responsibility exercised;
- the associated intent.

This clarification reduces tensions, avoids duplication of efforts, and strengthens accountability.

5.2.6 Boundary Between Responsibilities and Organization

The responsibilities reference framework is not:

- an organizational chart;
- a job description;
- an operational RACI matrix.

It describes governance responsibilities, not hierarchical structures.

Any organizational or operational instantiation falls within the scope of tooling or implementation and must remain compliant with the principles of the MS4ICT method.

5.2.7 Evolution of the Responsibilities Reference Framework

Responsibilities evolve with:

- organizational changes;
- new obligations;
- the emergence of new risks;
- changes in the ICT scope.

Any evolution must be documented in order to preserve the traceability and coherence of governance over time.

5.2.8 Position of the Responsibilities Reference Framework Within the Method

The responsibilities reference framework:

- builds upon the context reference framework;
- is fed by risks and controls;
- constitutes the link between governance and action.

It ensures that ICT governance is not abstract, but rather carried by clearly identified roles, accountable and aligned with the organization's strategic and operational challenges.

5.3 Risk Events Reference Framework

5.3.1 Role of the Risk Events Reference Framework

The risk events reference framework constitutes the objective foundation of risk analysis within the MS4ICT method.

It describes what may occur, independently of context, impacts, or applicable obligations.

This reference framework makes it possible to anchor ICT governance on observable and recognised facts, rather than on perceptions or subjective assumptions.

5.3.2 Why Distinguish Between an Event and a Risk

In many approaches, the notions of event and risk are conflated.

MS4ICT introduces a clear methodological distinction:

an event describes a fact that may occur;

a risk results from the contextualisation of that event, its impacts, and the associated obligations.

This separation is essential in order to:

- guarantee the objectivity of the initial reference base;
- ensure the stability of the reference framework over time;
- facilitate the coherence and traceability of risk analysis.

5.3.3 Origin of Risk Events

MS4ICT relies on recognised and neutral sources to define risk events, in particular the publications of ENISA, which are widely used at the European level.

These sources offer several advantages:

- institutional neutrality;
- regular updates;
- broad coverage of ICT threats;
- compatibility with European frameworks such as NIS2 and DORA.

The risk events reference framework is therefore designed as a reusable, sustainable, and organization-independent foundation.

5.3.4 Definition of a Risk Event

A risk event is a fact that may affect the organization, without presuming:

- its likelihood;
- its impacts;
- the applicable obligations;
- the existing controls.

Examples of risk events include:

- system compromise;
- service unavailability;
- loss or alteration of data;
- human error;
- supplier failure;
- malicious manipulation;
- technical compliance failure.

These events constitute potential causes, not fully-fledged risks.

5.3.5 Structure of a Risk Event

Within MS4ICT, each risk event is described in a structured and explainable manner, including in particular:

- an explicit name;
- a clear and neutral description;
- possible causes;
- potential sources;
- illustrative examples.

This structuring enables a shared understanding among the different ICT governance stakeholders.

5.3.6 Role of Risk Events in Overall Coherence

The risk events reference framework directly feeds the MS4ICT coherence engine.

Each event:

- may generate one or more risks;
- serves as an anchoring point for contextual analysis;
- ensures traceability between causes, risks, and decisions.

By separating the event from the risk, MS4ICT avoids analyses that are biased by premature organizational or normative considerations.

5.3.7 Boundary Between Risk Events and Implementation

The risk events reference framework is independent of any technical implementation.

It is not intended to:

- detect incidents;
- monitor systems;
- replace a SOC or a SIEM.

It provides a methodological foundation upon which detection, monitoring, or incident management tools may rely, without influencing the method itself.

5.3.8 Evolution of the Risk Events Reference Framework

Risk events may evolve with the emergence of new threats, new usages, or new technologies.

Any evolution of the reference framework must:

- be documented;
- remain consistent with the reference sources;
- preserve the stability and comparability of risk analysis over time.

5.3.9 Position of the Risk Events Reference Framework Within the Method

The risk events reference framework:

- builds upon the context reference framework;
- feeds the risk reference framework;
- constitutes the objective foundation of risk-based governance.

It is an essential element for ensuring coherent, explainable ICT governance, aligned with European and international frameworks.

5.4 Risk Reference Framework

5.4.1 Role of the Risk Reference Framework

The risk reference framework constitutes the analytical core of the MS4ICT method.

It transforms risk events, initially described in an objective manner, into contextualised, analysable, and actionable risks.

This reference framework enables the transition from a factual observation to a structured governance decision.

5.4.2 Definition of Risk within MS4ICT

Within MS4ICT, a risk is neither a simple descriptive statement nor a subjective assessment.

It is defined as the structured combination of several elements:

- an event that may occur;
- a given organizational context;
- potential impacts;
- applicable obligations;
- controls designed to reduce the risk.

This definition ensures that each risk is understandable, justifiable, and traceable.

5.4.3 Structure of an MS4ICT Risk

Each risk is constructed from the following components:

5.4.3.1 Event

The event constitutes the potential cause of the risk.

It originates from the risk events reference framework and describes what may occur, independently of any analysis.

5.4.3.2 Context

The context explains why the event is relevant to the organization.

It builds upon the context reference framework and makes it possible to identify the assets, processes, roles, or dependencies concerned.

5.4.3.3 Impacts

Impacts describe the potential consequences should the risk materialise.

They may be:

- operational;
- financial;
- legal and regulatory;
- reputational;
- strategic.

Impacts make it possible to assess the criticality of the risk and to guide prioritisation.

5.4.3.4 Obligations

Obligations correspond to the **normative, regulatory, contractual, or internal requirements** linked to the risk.

They allow risk management to be connected to compliance, **without conflating the two**.

5.4.3.5 Controls

Controls represent the measures decided to reduce the risk or limit its impacts.

They are never defined in isolation: a control exists only if it responds to an identified risk and an applicable obligation.

5.4.4 Role of Risk in Overall Coherence

Within MS4ICT, risk is the pivot between the different reference frameworks.

It makes it possible to link:

- events to obligations;
- obligations to controls;
- controls to responsibilities;
- decisions to context.

The risk reference framework directly feeds the coherence engine, ensuring coherent and explainable governance.

5.4.5 Risk-Based Prioritisation and Steering

The risk reference framework enables prioritisation-driven governance.

By analysing risks through their impacts and obligations, the organization can:

- focus efforts on the most critical risks;
- avoid a purely exhaustive approach;
- justify its choices to management and auditors.

Risk thus becomes a steering instrument, rather than a mere documentary artefact.

5.4.6 Boundary Between Risk and Implementation

The risk reference framework is independent of any technical implementation.

It does not describe:

- detailed attack scenarios;
- technical configurations;
- automated calculations.

Any quantification, automation, or tooling falls within the scope of implementation and must remain compliant with the MS4ICT methodological framework.

5.4.7 Evolution of the Risk Reference Framework

Risks evolve with:

- changes in context;
- the emergence of new events;
- the evolution of obligations;

- organizational transformations.

Any evolution must be documented in order to preserve decision traceability and coherence over time.

5.4.8 Position of the Risk Reference Framework Within the Method

The risk reference framework:

- builds upon the context and events reference frameworks;
- feeds the controls reference framework;
- constitutes both the entry point and the exit point of MS4ICT governance.

It is the central element of ICT governance oriented toward impact, prioritisation, and decision-making.

5.5 Controls Reference Framework

5.5.1 Role of the Controls Reference Framework

The controls reference framework constitutes the decision-making translation of ICT governance within the MS4ICT method.

It addresses a central question: what must the organization do to reduce the identified risks and respond to the applicable obligations?

Controls represent the concrete expression of governance choices, grounded in risk and justified by obligations.

5.5.2 Definition of a Control within MS4ICT

Within MS4ICT, a control is a measure decided in order to reduce a risk or limit its impacts, while responding to one or more obligations.

A control never exists in isolation.

It is systematically linked:

- to one or more risks;
- to identified obligations;
- to a given context;
- to clearly defined responsibilities.

This definition ensures that every control is explainable, traceable, and defensible.

5.5.3 Normative Origin of Controls

MS4ICT primarily relies on recognised normative frameworks, notably ISO/IEC standards, as well as on European regulatory requirements such as NIS2, DORA, or the GDPR.

The method does not create new controls.

It selects, structures, and justifies existing controls, aligning them with a risk-based governance logic.

5.5.4 Structure of an MS4ICT Control

Each control is described in a structured manner in order to ensure its understanding and coherence:

- Objective: what the control aims to achieve;
- Description: the nature of the decided measure;
- Covered risks: the risks addressed by the control;
- Associated obligations: the relevant normative or regulatory requirements;
- Responsibilities: the roles responsible for its implementation and monitoring.

This structuring enables readable and auditable governance.

5.5.5 Controls and Overall Coherence

The controls reference framework is closely linked to the MS4ICT coherence engine.

Each control is justified by:

- an identified risk;
- originating from an event;
- contextualised;
- associated with explicit obligations.

This chain ensures that controls are neither arbitrary nor redundant, but rather the result of coherent and traceable decisions.

5.5.6 The Statement of Applicability (SoA)

Within MS4ICT, the Statement of Applicability is not an isolated or purely normative document.

It is a generated view of the controls reference framework, in which:

- each control is justified;
- each exclusion is explained;
- each link is traceable.

The SoA thus becomes a tool for explanation and steering, rather than a mere documentary requirement.

5.5.7 Boundary Between Controls and Implementation

The controls reference framework is independent of any technical implementation.

It does not describe:

- configurations;
- detailed procedures;
- specific tools or technologies.

Any concrete implementation falls within the scope of tooling and must remain compliant with the MS4ICT methodological framework.

5.5.8 Evolution of the Controls Reference Framework

Controls may evolve in response to:

- changes in risks;
- new obligations;
- organizational evolutions;
- technological transformations.

Any evolution must be documented in order to preserve the traceability, coherence, and justifiability of governance decisions.

5.5.9 Position of the Controls Reference Framework Within the Method

The controls reference framework:

- builds upon the risk reference framework;
- feeds the responsibilities reference framework;
- constitutes the direct link between governance and action.

It is the final expression of structured, coherent, and risk-driven ICT governance.

6 COHERENCE ENGINE

6.1 PRINCIPLES

6.1.1 Role of the Coherence Engine

The coherence engine constitutes the core of the MS4ICT method.

It transforms a set of distinct reference frameworks into an integrated, coherent, and explainable governance system.

Without a coherence engine, the reference frameworks remain silos.

With it, they become a structured whole, in which each element has its place, its justification, and its relationship with the others.

6.1.2 Purpose of the Coherence Engine

The purpose of the coherence engine is to:

- systematically link governance elements;
- guarantee coherence between risks, obligations, controls, and responsibilities;
- ensure traceability of decisions;
- make governance explainable at all levels.

It does not generate new information.

It structures the relationships between existing information.

6.1.3 Principle of Systematic Linking

The coherence engine is based on a fundamental principle:

no governance element exists in isolation.

Within MS4ICT, the engine ensures that:

- each event may generate one or more risks;
- each risk is linked to an explicit context;
- each risk is associated with applicable obligations;
- each obligation calls for one or more controls;
- each control is assigned to identified responsibilities.

This chain constitutes the foundation of overall coherence.

6.1.4 Principle of Complete Traceability

The coherence engine enforces end-to-end traceability of the relationships between the reference frameworks.

It makes it possible to answer, unambiguously, the following questions:

- why this risk exists;
- why this obligation applies;
- why this control was selected;
- why this responsibility is assigned.

Traceability is a structuring principle, essential for steering, auditing, and defending governance decisions.

6.1.5 Principle of Explainability

Coherence has value only if it is explainable.

The MS4ICT coherence engine is designed to produce relationships that are understandable, even for non-technical stakeholders.

Each link must be explainable:

- in a logical manner;
- using a shared vocabulary;
- without relying on in-depth knowledge of standards or tools.

Explainability is an essential condition for stakeholder buy-in and governance effectiveness.

6.1.6 Principle of Methodological Neutrality

The coherence engine is independent of any implementation.

It does not rely on:

- any specific tool;
- any particular technology;
- any imposed data model.

It describes a methodological logic, applicable in diverse contexts and transposable across different tooling environments.

Any implementation must respect the principles of the engine, without altering or simplifying them.

6.1.7 Principle of Non-Circumvention

Within MS4ICT, the coherence engine is not optional.

No governance decision may be taken outside the coherence chain:

- no control without a risk;
- no risk without an event;
- no responsibility without an explicit intent;
- no obligation without justification.

This principle protects the method against arbitrary decisions and documentary drift.

6.1.8 Principle of Sustainability

The coherence engine is designed to remain valid over time.

It enables the integration of:

- new obligations;
- new risks;
- new contexts;
- new reference frameworks;

without calling into question the overall structure of the method.

Coherence is maintained even in a constantly evolving environment.

6.1.9 Position of the Coherence Engine Within the Method

The coherence engine:

- links all MS4ICT reference frameworks;
- determines the quality of governance;
- forms the foundation of MS4ICT views;
- acts as the guarantor of overall coherence.

It is the differentiating element of MS4ICT and the central point around which the entire method is structured.

6.2 Coherence Engine -Rules

6.2.1 Purpose of the Coherence Rules

The coherence rules define the mandatory relationships between the various reference frameworks of the MS4ICT method.

They constitute a normative framework ensuring that every ICT governance decision is:

- justified;
- traceable;
- explainable;
- coherent with the method as a whole.

These rules do not describe technical mechanisms, but non-negotiable methodological constraints.

6.2.2 Rule 1 – No Control Without a Risk

A control cannot exist within MS4ICT unless it is explicitly linked to one or more identified risks.

This rule ensures that:

- controls are not arbitrary;
- controls are justified by real issues;
- governance is not reduced to a normative checklist.

Every control must be able to answer the question:

which risk is this control intended to reduce?

6.2.3 Rule 2 – No Risk Without an Event

Every risk must be linked to a risk event identified in the risk events reference framework.

This rule makes it possible to:

- anchor risk analysis in objective facts;
- avoid abstractly formulated risks;
- ensure the stability of the risk reference framework.

A risk without an event constitutes a methodological coherence breach.

6.2.4 Rule 3 – No Risk Without Context

A risk has meaning only in relation to an explicit context.

Each risk must be contextualised through elements from the context reference framework:

- concerned assets;
- critical processes;
- dependencies;
- applicable obligations.

This rule prevents generic or reality-disconnected risk analysis.

6.2.5 Rule 4 – No Obligation Without Risk Justification

Normative or regulatory obligations are never handled in isolation within MS4ICT.

Every obligation must be linked to one or more risks it addresses.

This rule makes it possible to:

- align compliance with risk management;
- avoid purely documentary governance;
- make compliance explainable and prioritised.

6.2.6 Rule 5 – No Control Without Obligation or Explicit Intent

A control must respond to an identified obligation or to an explicit risk-reduction intent.

This rule ensures that:

- each control has a clear purpose;
- controls are defensible during audits;
- exclusions are justifiable.

A control without an obligation or intent constitutes a governance anomaly.

6.2.7 Rule 6 – No Responsibility Without an Associated Control

A governance responsibility must always be linked to one or more controls.

This rule makes it possible to:

- avoid abstract responsibilities;
- clarify accountability;
- connect governance with action.

Every responsibility must be able to answer:

what is this responsibility concretely accountable for?

6.2.8 Rule 7 – No Responsibility Without Explicit Intent

Each responsibility must be associated with a clearly defined intent.

Explicit intent defines:

- the purpose of the responsibility;
- its link with risks and obligations;
- the justification of the decision.

Without intent, a responsibility can neither be understood nor assessed.

6.2.9 Rule 8 – Continuity of the Coherence Chain

The MS4ICT coherence chain must be continuous, with no breaks or logical shortcuts:

Context → Event → Risk → Obligation → Control → Responsibility

Any break in this chain compromises overall coherence and governance explainability.

6.2.10 Rule 9 – Uniqueness and Non-Contradiction of Links

The relationships established by the coherence engine must be:

- non-contradictory;
- explicit;
- understandable.

Two elements cannot be linked incoherently or conflictually without documented justification.

This rule protects the method against internal inconsistencies.

6.2.11 Rule 10 – Primacy of the Method Over Tooling

Coherence rules prevail over any tooling constraints.

No technical, organizational, or operational limitation may justify a breach of MS4ICT methodological rules.

Tooling adapts to the method, never the reverse.

6.2.12 Role of the Rules in MS4ICT Governance

The coherence rules:

- frame all governance decisions;
- guarantee alignment between reference frameworks;
- make the method defensible and audit-ready;
- protect MS4ICT against drift and arbitrariness.

They constitute the normative foundation of the coherence engine and must be respected in any implementation of the method.

7 MS4ICT VIEWS

7.1 ROLE OF MS4ICT VIEWS

MS4ICT views make ICT governance readable, explainable, and usable for the various actors within the organization.

They constitute the interface between the methodological structure of MS4ICT, and the concrete needs of the roles involved in ICT governance.

Views do not create any new information.

They project the existing reference frameworks through the coherence engine.

7.1.1 Why Views Are Essential

In many organizations, ICT governance fails not due to a lack of information, but due to excessive complexity.

Even well-structured reference frameworks quickly become unreadable when presented in a raw form.

MS4ICT views address this challenge by enabling:

- targeted and relevant reading;
- role-appropriate language;
- immediate understanding of responsibilities and priorities.

7.1.2 Principle of Projection, Not Duplication

An MS4ICT view is a filtered projection of the reference frameworks, not an additional framework.

It selects, organises, and presents existing information without creating new data, without modifying it, and without breaking overall coherence.

This principle guarantees information uniqueness and prevents divergence between views and their source reference frameworks.

7.1.3 Principle of Coherence by Design

Views are generated from the MS4ICT coherence engine.

This guarantees that every piece of information displayed in a view is:

- linked to a risk;
- justified by an obligation;
- associated with a control;
- assigned to a responsibility.

No view may present isolated or unjustified information.

7.1.4 Principle of Role-Based Adaptation

Each view is designed according to the needs of a specific role.

A view must enable its user to:

- understand what concerns them;
- identify their responsibilities;
- visualise priorities;
- make informed decisions.

Views may vary in level of detail, terminology, and angle of interpretation, without ever altering the methodological structure.

7.1.5 Principle of Readability and Pedagogy

MS4ICT views prioritise clarity and pedagogy.

They must be understandable without in-depth knowledge of standards, regulatory frameworks, or internal mechanisms of the method.

Readability is an essential condition for stakeholder engagement, accountability, and governance effectiveness.

7.1.6 Principle of Technological Neutrality

MS4ICT views are technology-independent.

The method defines the content and logic of the views, but does not prescribe any format, tool, or interface.

Any visual or operational implementation falls within the scope of tooling and must respect the methodological principles of the views.

7.1.7 Principle of Non-Contradiction Between Views

MS4ICT views must never contradict one another.

Different views may present different information, but never incoherent information.

This rule ensures shared understanding and a common language across organizational roles.

7.1.8 Evolution of MS4ICT Views

Views may evolve according to role needs or organizational maturity.

Any evolution must:

- remain compliant with the coherence engine;
- respect methodological rules;
- preserve traceability;
- maintain decision explainability.

7.1.9 Position of Views Within the Method

MS4ICT views:

- are based on the reference frameworks;
- are generated by the coherence engine;
- constitute the primary support for decision-making.

They are the visible expression of structured, coherent, and risk-driven ICT governance.

7.2 MS4ICT VIEW – EXECUTIVE MANAGEMENT

7.2.1 Objective of the Executive Management View

The Executive Management view aims to provide a strategic, synthetic, and explainable reading of ICT governance.

It enables executive management to understand:

- the major risks facing the organization;
- the critical obligations that must be met;
- the governance decisions that have been taken;
- the associated responsibilities.

This view supports decision-making, prioritisation, and accountability at the highest level.

7.2.2 Positioning of the Executive Management View

The Executive Management view is not intended to present all technical or operational details.

It focuses on what is essential for strategic steering.

It is built from:

- the MS4ICT reference frameworks;
- the coherence engine;
- the rules of traceability and explainability.

No information displayed in this view is isolated or unjustified.

7.2.3 Main Content of the Executive Management View

The Executive Management view highlights, in a prioritised manner:

- strategic risks with a significant impact on continuity, compliance, or reputation;
- the critical regulatory and normative obligations associated with those risks;
- the key controls decided to address them;
- the governance responsibilities associated with decisions and controls.

The level of detail is deliberately limited in order to preserve readability and clarity.

7.2.4 Risk-Based Reading

In the Executive Management view, risk is the entry point.

All information is organised around simple questions:

- what are the priority risks?
- why are these risks critical?
- which obligations result from them?
- what decisions have been taken to address them?
- who is responsible for these decisions?

This approach enables executive management to directly link ICT governance to business and strategic challenges.

7.2.5 Explainability and Justification of Decisions

The Executive Management view must make it possible to explain every governance decision without resorting to technical or normative language.

Each element displayed in the view must be justifiable through the MS4ICT coherence chain:

context → event → risk → obligation → control → responsibility

This explanatory capability is essential for executive committees, boards of directors, and interactions with external stakeholders.

7.2.6 Responsibilities and Accountability

The Executive Management view highlights governance responsibilities without entering into organisational details.

It enables the identification of:

- the roles responsible for key decisions;
- areas of accountability;
- points requiring arbitration or validation.

The view promotes clear governance, in which responsibilities are explicit and assumed.

7.2.7 Boundary of the Executive Management View

The Executive Management view does not present:

- technical configurations;
- detailed procedures;
- fine-grained operational metrics;
- raw data originating from tools.

These elements belong to other views or to tooling and are not necessary for strategic decision-making.

7.2.8 Evolution of the Executive Management View

The Executive Management view may evolve depending on:

- the maturity of ICT governance;
- the expectations of executive management;
- the regulatory or strategic context.

Any evolution must nevertheless:

- remain compliant with the coherence engine;
- preserve traceability;
- guarantee the explainability of decisions.

7.2.9 Value of the Executive Management View within MS4ICT

The Executive Management view is an essential lever for transforming ICT governance into a matter of strategic steering, rather than a technical or documentary exercise.

It enables executive management to rely on a clear, coherent, and defensible view of ICT-related challenges and the associated decisions.

7.3 MS4ICT VIEW – ICT

7.3.1 Objective of the ICT View

The ICT view aims to provide an operational, structured, and coherent reading of ICT governance, tailored to teams responsible for information systems, services, and infrastructures.

It enables ICT teams to understand:

- the risks that directly affect ICT services and assets;
- the obligations applicable to their scope;
- the controls to be implemented or maintained;
- the responsibilities associated with the expected actions.

7.3.2 Positioning of the ICT View

The ICT view is positioned at the interface between governance and operations.

It does not replace technical tools, ITSM processes, or architecture reference frameworks.

It provides a coherence framework that makes it possible to link ICT actions to risk and compliance challenges.

All information presented originates from the MS4ICT reference frameworks and is linked through the coherence engine.

7.3.3 Main Content of the ICT View

For the relevant scope, the ICT view highlights:

- critical services, systems, or assets derived from the context reference framework;
- relevant risk events likely to affect those assets;
- associated ICT risks, analysed and prioritised;
- normative or regulatory obligations impacting ICT activities;
- ICT controls to be implemented, maintained, or improved;
- ICT responsibilities associated with controls and decisions.

The level of detail is adapted to the needs of ICT teams, without overloading the view with non-relevant elements.

7.3.4 Service- and Asset-Oriented Reading

In the ICT view, the reading can be initiated from critical services or assets.

This approach makes it possible to answer key operational questions:

- which risks affect this service?
- which obligations apply to it?
- which controls must be in place?
- who is responsible for their implementation?

Governance thus becomes directly actionable for ICT teams.

7.3.5 Coherence Between Governance and Operations

The ICT view makes it possible to link operational activities with governance decisions.

Each control visible in the view:

- is justified by an identified risk;
- responds to an explicit obligation;
- is associated with a clear responsibility.

This coherence avoids:

- controls applied “out of habit”;
- actions disconnected from real challenges;
- misunderstandings between governance and operational teams.

7.3.6 ICT Responsibilities and Accountability

The ICT view highlights responsibilities falling within ICT teams, without substituting for the internal organisation.

It enables identification of:

- the roles responsible for ICT controls;
- the expected actions;
- areas requiring coordination with other functions (cybersecurity, compliance, suppliers).

Accountability is thus clarified, without rigidifying the organisation.

7.3.7 Boundary of the ICT View

The ICT view does not present:

- detailed technical configurations;
- step-by-step procedures;
- data directly originating from tools (monitoring, tickets, logs).

These elements fall within tooling and operational processes.

The ICT view provides the governance framework within which those elements take meaning.

7.3.8 Evolution of the ICT View

The ICT view may evolve depending on:

- the maturity of ICT teams;
- changes in the technical scope;
- the emergence of new risks or obligations.

Any evolution must remain:

- compliant with the coherence engine;
- aligned with the MS4ICT reference frameworks;
- explainable and traceable.

7.3.9 Value of the ICT View within MS4ICT

The ICT view enables ICT governance to be transformed into a useful operational lever.

It helps ICT teams to:

- understand the rationale behind controls;
- prioritise actions;
- engage in effective dialogue
- with executive management, compliance, and cybersecurity functions.

It is a key element for coherent, applicable, and sustainable ICT governance.

7.4 MS4ICT VIEW – CYBERSECURITY

7.4.1 Objective of the Cybersecurity View

The Cybersecurity view aims to provide a **clear, structured, and prioritised** reading of cybersecurity challenges, risk-based and aligned with overall ICT governance.

It enables cybersecurity functions to understand:

- relevant cyber risk events;
- the organisation's priority cyber risks;
- applicable cybersecurity obligations;
- the expected security controls;
- the associated responsibilities.

7.4.2 Positioning of the Cybersecurity View

The Cybersecurity view is positioned at the intersection of ICT governance, risk management, and cybersecurity operations.

It does not replace:

- detection or monitoring tools;
- SOCs, SIEMs, or incident response platforms;
- operational security processes.

It provides a methodological coherence framework that links cybersecurity activities to governance and compliance challenges.

7.4.3 Main Content of the Cybersecurity View

The Cybersecurity view highlights:

- cyber risk events derived from the events reference framework (e.g. compromise, unavailability, data breach);
- contextualised cyber risks affecting critical assets, services, or processes;
- cybersecurity obligations stemming from normative and regulatory frameworks (e.g. ISO/IEC, NIS2, DORA, sector-specific requirements);
- security controls selected to reduce those risks;
- cybersecurity responsibilities associated with the implementation, monitoring, and supervision of controls.

Information is presented in a prioritised manner, based on impacts and governance stakes.

7.4.4 Threat- and Risk-Oriented Reading

In the Cybersecurity view, the reading is centred on the question:

which cyber events and risks threaten the organisation, and how should they be addressed?

This approach makes it possible to:

- align cybersecurity with real risks;
- avoid purely technical or exhaustive security approaches;
- focus efforts on critical scenarios.

Risk acts as the guiding thread between threat, obligation, and control.

7.4.5 Coherence Between Cybersecurity, ICT, and Compliance

The Cybersecurity view makes visible the coherence between:

- cyber risks;
- regulatory requirements;
- security controls;
- stakeholder responsibilities.

It facilitates dialogue between cybersecurity teams, ICT teams, compliance functions, and executive management, based on a shared language.

7.4.6 Cybersecurity Responsibilities and Steering

The Cybersecurity view highlights cybersecurity-related responsibilities, without detailing internal organisational structures.

It enables identification of:

- roles responsible for cybersecurity controls;
- domains requiring supervision or arbitration;
- coordination points with ICT;
- suppliers or compliance functions.

Cyber accountability is thus clarified and fully integrated into overall governance.

7.4.7 Boundary of the Cybersecurity View

The Cybersecurity view does not present:

- real-time alerts;
- raw technical logs or indicators;
- detailed incident response procedures;
- security configurations.

These elements fall within tooling and security operations.

The Cybersecurity view provides the governance framework within which those elements take meaning.

7.4.8 Evolution of the Cybersecurity View

The Cybersecurity view may evolve with:

- the emergence of new threats;
- changes in the regulatory context;
- the organisation’s cybersecurity maturity.

Any evolution must:

- remain aligned with the coherence engine;
- preserve decision traceability;
- guarantee explainability of priorities.

7.4.9 Value of the Cybersecurity View within MS4ICT

The Cybersecurity view positions cybersecurity as a governance lever, rather than an isolated discipline.

It helps cybersecurity functions to:

- prioritise security efforts;
- justify controls;
- engage in effective dialogue with executive management, ICT, and compliance.

It is a key element of coherent, defensible, and sustainable cybersecurity governance.

7.5 MS4ICT VIEW – COMPLIANCE

7.5.1 Objective of the Compliance View

The Compliance view aims to provide a structured, explainable, and defensible reading of the normative and regulatory obligations applicable to the organization.

It enables compliance functions to understand:

- which obligations truly apply;
- which risks they are linked to;
- which controls address them;
- which responsibilities are assigned.

The Compliance view transforms compliance into a risk-based governance lever, rather than an isolated documentary exercise.

7.5.2 Positioning of the Compliance View

The Compliance view is positioned at the intersection of governance, risk management, and normative requirements.

It does not merely list obligations or controls.

It highlights the justification logic behind compliance decisions.

All information presented is derived from the MS4ICT reference frameworks and linked through the coherence engine.

7.5.3 Main Content of the Compliance View

The Compliance view highlights:

- the normative and regulatory obligations applicable to the given scope;
- the risks addressed by those obligations;
- the controls selected to ensure compliance;
- the responsibilities associated with the implementation and monitoring of controls;
- the justifications that explain the choices made.

Obligations are presented in a contextualised manner, not as an abstract checklist.

7.5.4 Obligation- and Risk-Oriented Reading

In the Compliance view, reading may begin from **obligations**.

For each obligation, it is possible to answer the following questions:

- why does this obligation apply?
- which risks does it address?
- which controls have been decided?
- who is responsible for their application?

This approach makes it possible to directly link compliance and governance, without conflating them.

7.5.5 The Central Role of the Statement of Applicability

The Compliance view naturally integrates the Statement of Applicability (SoA), not as a static document, but as a coherent and justified view of the controls reference framework.

Within MS4ICT:

- each applicable control is justified;
- each exclusion is explained;
- each relationship is traceable.

The SoA thus becomes a steering, audit, and communication tool, rather than a mere normative requirement.

7.5.6 Explainability and Auditability

The Compliance view is designed to meet audit requirements, both internal and external.

It makes it possible to explain:

- why a control is present or absent;
- how an obligation is covered;
- on what basis decisions were taken.

The MS4ICT coherence chain ensures compliance that is defensible, traceable, and explainable.

7.5.7 Compliance Responsibilities and Accountability

The Compliance view highlights compliance-related responsibilities, without substituting for the internal organizational structure.

It enables identification of:

- roles responsible for compliance;
- coordination points
- with ICT, cybersecurity, or legal functions;
- domains requiring arbitration or validation.

Compliance thus becomes a governed process, rather than a diffuse responsibility.

7.5.8 Boundary of the Compliance View

The Compliance view does not present:

- detailed operational procedures;
- raw technical evidence;
- specific configurations or tools.

These elements fall within tooling and implementation.

The Compliance view provides the methodological framework within which those elements take meaning.

7.5.9 Evolution of the Compliance View

The Compliance view may evolve depending on:

- the emergence of new obligations;
- changes in risks;
- changes in scope or context.

Any evolution must:

- remain aligned with the coherence engine;
- preserve decision traceability;
- guarantee the explainability of choices.

7.5.10 Value of the Compliance View within MS4ICT

The Compliance view enables a shift from imposed compliance to risk-driven compliance.

It helps compliance functions to:

- prioritise efforts;
- engage in effective dialogue
- with executive management, ICT, and cybersecurity;
- demonstrate governance coherence during audits.

It is a key element of structured, justifiable, and sustainable ICT governance.

7.6 MS4ICT VIEW – DPO (DATA PROTECTION OFFICER)

7.6.1 Objective of the DPO View

The DPO view aims to provide a structured, explainable, and defensible reading of personal data protection challenges within ICT governance.

It enables the DPO to understand:

- the events likely to affect personal data;
- the associated GDPR-related risks;
- the applicable obligations;
- the controls in place;
- the responsibilities related to data protection.

This view supports the DPO in their roles of advice, monitoring, and steering GDPR compliance.

7.6.2 Positioning of the DPO View

The DPO view is positioned at the intersection of compliance, risk management, and ICT governance.

It is not limited to a purely legal reading of the GDPR.

It links personal data protection to concrete risks, organizational context, and governance decisions.

All information presented is derived from the MS4ICT reference frameworks and linked through the coherence engine.

7.6.3 Main Content of the DPO View

The DPO view highlights:

- risk events that may affect personal data (e.g. breach, alteration, unavailability);
- contextualised GDPR-related risks (e.g. personal data breach, non-compliance, impact on rights and freedoms);
- applicable GDPR obligations (e.g. security, data minimisation, data subject rights, notification);
- controls selected to address those obligations;
- responsibilities associated with the DPO and other relevant roles (ICT, cybersecurity, legal, business functions).

Information is presented in a coherent and prioritised manner.

7.6.4 Risk- and Data Subject Rights-Oriented Reading

In the DPO view, reading is centred on the following question:

which risks threaten the rights and freedoms of data subjects, and how are they addressed?

This approach makes it possible to:

- link data protection to concrete risks;
- move beyond purely formal compliance;
- prioritise actions based on real impacts.

7.6.5 Articulation with DPIAs

The DPO view enables identification of risks requiring a Data Protection Impact Assessment (DPIA).

DPIAs are not isolated objects:

- they form part of the MS4ICT coherence chain, in relation to:
    - events;
    - risks;
    - obligations;
    - controls.

This articulation strengthens coherence between GDPR compliance and overall ICT governance.

7.6.6 Responsibilities and Role of the DPO

The DPO view highlights the specific role of the DPO, without conflating it with operational responsibilities.

It makes it possible to distinguish:

- advisory and monitoring responsibilities;
- operational responsibilities belonging to ICT or business functions;
- decision-making responsibilities belonging to executive management.

This clarification preserves the functional independence of the DPO, while ensuring coherent governance.

7.6.7 Boundary of the DPO View

The DPO view does not present:

- line-by-line detailed processing records;
- exhaustive operational registers;
- raw technical evidence;
- detailed internal procedures.

These elements fall within tooling and implementation.

The DPO view provides the methodological framework within which those elements take meaning.

7.6.8 Evolution of the DPO View

The DPO view may evolve depending on:

- changes in processing activities;
- the emergence of new risks or events;
- regulatory or case-law developments.

Any evolution must:

- remain aligned with the coherence engine;
- preserve decision traceability;
- guarantee explainability of choices.

7.6.9 Value of the DPO View within MS4ICT

The DPO view enables personal data protection to be fully embedded at the core of ICT governance, without isolating or diluting it.

It helps the DPO to:

- steer GDPR-related risks;
- engage in effective dialogue with ICT, cybersecurity, compliance, and executive management;
- demonstrate structured, coherent, and defensible compliance.

It is a key element of mature, aligned, and sustainable GDPR governance.

7.7 MS4ICT VIEW – LEGAL

7.7.1 Objective of the Legal View

The Legal view aims to provide a structured, explainable, and coherent reading of the legal challenges related to ICT governance.

It enables the legal function to understand:

- the legal risks associated with ICT;
- the applicable legal and contractual obligations;
- the controls decided to address them;
- the responsibilities associated with governance decisions.

This view supports the legal function in its roles of risk mitigation, advisory support, and legal risk steering.

7.7.2 Positioning of the Legal View

The Legal view is positioned at the intersection of governance, risk management, and regulatory compliance.

It is not limited to a purely textual reading of legal obligations.

It links law to concrete risks, organizational context, and governance decisions.

All information presented is derived from the MS4ICT reference frameworks and linked through the coherence engine.

7.7.3 Main Content of the Legal View

The Legal view highlights:

- legal and regulatory obligations applicable to the ICT scope (laws, regulations, sector-specific requirements);
- contractual obligations related to suppliers, partners, or customers;
- legal risks associated with those obligations (sanctions, litigation, liability, contractual invalidity);
- controls selected to manage those risks;
- responsibilities associated with the management and monitoring of legal obligations.

Information is presented in a **contextualised manner**, not as an abstract list of legal texts.

7.7.4 Obligation- and Legal Risk-Oriented Reading

In the Legal view, reading is centred on the following questions:

- which legal obligations apply?
- which legal risks do they address?
- which decisions have been taken to manage them?
- who is responsible for their implementation?

This approach makes it possible to connect law with operational governance, without reducing it to a purely advisory role.

7.7.5 Articulation with Contracts and Third Parties

The Legal view makes it possible to identify risks and obligations related to third parties, including in particular:

- ICT suppliers;
- cloud service providers;
- critical partners.

It makes visible the articulation between:

- contractual requirements;
- ICT risks;
- regulatory obligations;
- governance controls.

This coherence is essential to secure contractual relationships in a complex digital environment.

7.7.6 Responsibilities and Role of the Legal Function

The Legal view highlights the specific role of the legal function, without conflating it with operational responsibilities.

It makes it possible to distinguish between:

- advisory and validation responsibilities;
- operational responsibilities belonging to ICT or business functions;
- decision-making responsibilities belonging to executive management.

This clarification promotes clear legal governance and stronger accountability.

7.7.7 Boundary of the Legal View

The Legal view does not present:

- detailed contractual clauses;
- complete legal documents;
- operational procedures;
- data originating from contract management tools.

These elements fall within tooling.

The Legal view provides the methodological framework that gives meaning to this information.

7.7.8 Evolution of the Legal View

The Legal view may evolve depending on:

- legislative or regulatory changes;
- the evolution of ICT-related risks;
- new contractual relationships.

Any evolution must:

- remain aligned with the coherence engine;
- preserve decision traceability;
- guarantee explainability of legal choices.

7.7.9 Value of the Legal View within MS4ICT

The Legal view enables law to be fully integrated into the core of ICT governance, without isolating or overloading it.

It helps the legal function to:

- anticipate risks;
- secure decisions;
- engage in effective dialogue with executive management, ICT, compliance, and cybersecurity functions.

It is a key element of coherent, defensible, and sustainable legal governance.

7.8 MS4ICT VIEW – ARTIFICIAL INTELLIGENCE

7.8.1 Objective of the AI View

The AI view aims to provide a structured, explainable, and governed reading of the challenges related to the use of artificial intelligence systems within the organization.

It enables stakeholders involved in AI (executive management, business functions, compliance, legal, DPO, ICT) to understand:

- the specific risks related to AI systems;
- the applicable obligations;
- the controls that have been decided;
- the associated responsibilities.

The AI view embeds AI within overall ICT governance, without treating it as an isolated or out-of-scope domain.

7.8.2 Positioning of the AI View

The AI view is positioned at the intersection of:

- ICT governance;
- risk management;
- regulatory compliance;
- protection of fundamental rights.

It does not treat AI as a mere technology, but as a **high-impact system** likely to affect:

- individuals;
- decision-making processes;
- compliance;
- the organization's reputation.

All information presented is derived from the MS4ICT reference frameworks and linked through the coherence engine.

7.8.3 Main Content of the AI View

The AI view highlights:

- AI systems or algorithmic uses falling within the governance scope;
- AI-related risk events (e.g. bias, lack of transparency, decision errors, model drift, excessive dependency);
- contextualised AI risks (e.g. discrimination, non-compliance, infringement of rights, loss of trust);
- applicable obligations arising from regulatory and normative frameworks (e.g. AI Act, ISO/IEC 42001, GDPR where applicable);
- the controls decided to manage these risks;
- the responsibilities associated with AI-related decisions.

Information is presented in a prioritised and explainable manner.

7.8.4 Impact- and AI Risk-Oriented Reading

In the AI view, reading is centred on the following question:

what impacts may AI systems have, and how are those impacts governed?

This approach makes it possible to:

- move beyond a purely technical view of AI;
- link AI to real risks;
- prioritise governance actions based on potential impacts.

Risk is the entry point for AI governance within MS4ICT.

7.8.5 Articulation with AI Compliance

The AI view makes it possible to link AI-specific requirements with the organization's other obligations.

It makes visible:

- alignment between the AI Act, AI standards, and ICT governance;
- the links between AI risks, data protection, and legal requirements;
- coherence between AI controls and existing controls.

AI governance is **not a silo**, but a coherent extension of **risk-based governance**.

7.8.6 Responsibilities and AI Governance

The AI view highlights responsibilities related to AI, without conflating them with purely technical responsibilities.

It makes it possible to distinguish between:

- design and usage responsibilities;
- validation and oversight responsibilities;
- decision-making and arbitration responsibilities.

This clarification is essential for responsible and explainable AI governance.

7.8.7 Boundary of the AI View

The AI view does not present:

- detailed algorithmic models;
- technical parameters;
- AI code or architectures;
- internal performance metrics.

These elements fall within tooling and operational practices.

The AI view provides the **methodological framework** within which these elements are governed.

7.8.8 Evolution of the AI View

The AI view is expected to evolve depending on:

- changes in AI uses;
- regulatory developments;
- societal and ethical expectations.

Any evolution must:

- remain aligned with the coherence engine;
- preserve decision traceability;
- guarantee explainability of choices.

7.8.9 Value of the AI View within MS4ICT

The AI view enables artificial intelligence to be integrated into coherent, responsible, and sustainable ICT governance.

It helps the organization to:

- anticipate AI-related risks;
- demonstrate structured compliance;
- make informed decisions;
- establish lasting trust in AI uses.

It constitutes a core pillar of modern AI governance, aligned with European challenges and the principles of MS4ICT.

8 IMPLEMENTATION OF THE MS4ICT METHOD

8.1 PRINCIPLES FOR IMPLEMENTING THE MS4ICT METHOD

8.1.1 Purpose of the Implementation Principles

The implementation principles define how to apply the MS4ICT method without altering its structure, founding principles, or overall coherence.

They constitute a methodological framework intended to guide organizations in adopting MS4ICT, independently of any tool or technical solution.

8.1.2 Principle of Method Primacy

The MS4ICT method takes precedence over any organizational, technical, or operational considerations.

No tooling constraint, existing limitation, or historical practice may justify adapting or simplifying the method.

Tooling adapts to the method, never the reverse.

8.1.3 Principle of Gradual Implementation

The implementation of MS4ICT is progressive.

It is neither necessary nor desirable to immediately cover the entire ICT scope.

The method may be applied:

- to a limited scope;
- to critical services;
- to priority risks;
- or to a specific regulatory domain.

This gradual approach enables controlled adoption and sustainable maturity growth.

8.1.4 Principle of Explicit Scope

Any implementation of MS4ICT must begin with the definition of a clear and documented scope.

This scope must specify:

- what is included;
- what is excluded;
- the assumptions adopted;
- the known limitations.

An implicit or vague scope is incompatible with explainable governance.

8.1.5 Principle of Coherence Before Exhaustiveness

MS4ICT prioritises coherence over exhaustiveness.

It is preferable to have a limited but coherent scope, in which all reference frameworks are properly connected, rather than a broad scope containing coherence gaps.

Coherence is a condition for governance credibility and sustainability.

8.1.6 Principle of Risk-Based Governance

The implementation of MS4ICT must always be risk-driven.

Risks constitute:

- the entry point;
- the prioritisation criterion;
- the exit point of governance.

Any implementation decision must be justifiable by an identified, contextualised, and analysed risk.

8.1.7 Principle of Continuous Explainability

The method must remain explainable at every stage of its implementation.

At any time, it must be possible to answer the following questions:

- why this scope?
- why this risk?
- why this control?
- why this responsibility?

An implementation that cannot be explained constitutes a methodological breach.

8.1.8 Principle of Method / Implementation Separation

The implementation of MS4ICT must never confuse:

- the method;
- the organization;
- the tooling.

Reference frameworks, the coherence engine, and views belong to the method.

Processes, tools, dashboards, and automation belong to the implementation.

This separation is essential to preserve the independence and longevity of the method.

8.1.9 Principle of Clear Accountability

Any MS4ICT implementation must clarify governance responsibilities.

Each reference framework, decision, and control must be associated with explicit responsibilities, with a clearly defined intent.

MS4ICT governance does not rely on implicit responsibilities.

8.1.10 Principle of Decision Traceability

Decisions taken as part of the MS4ICT implementation must be documented and traceable.

This traceability makes it possible to:

- explain the choices made;
- justify trade-offs;
- facilitate audits;
- maintain coherence over time.

8.1.11 Principle of Controlled Improvement

MS4ICT is not a static method, but its evolutions are rare and controlled.

Continuous improvement focuses on:

- enriching reference frameworks;
- evolving the context;
- adapting to new obligations.

It does not call into question the founding principles or the structure of the method.

8.1.12 Position of the Implementation Principles within MS4ICT

The implementation principles:

- frame the application of the method;
- protect MS4ICT against drift;
- guarantee coherent, explainable, and sustainable governance.

They constitute the methodological foundation of any serious adoption of MS4ICT.

8.2 VIGILANCE IN THE IMPLEMENTATION OF MS4ICT

8.2.1 Purpose of the Vigilance Points

The vigilance points identify methodological risks that may compromise the coherence, explainability, or sustainability of ICT governance during the implementation of MS4ICT.

They do not constitute additional rules, but rather structuring alerts intended to preserve the integrity of the method.

8.2.2 Vigilance 1 – Confusing the Method with a Tool

One of the major risks consists in confusing the MS4ICT method with a tool or a technical solution.

MS4ICT:

- describes a governance logic;
- defines reference frameworks;
- imposes coherence rules.

It does not prescribe:

- any software;
- any technical data model;
- any automation.

Any attempt to adapt the method to the constraints of an existing tool constitutes a methodological drift.

8.2.3 Vigilance 2 – Seeking Immediate Exhaustiveness

Attempting to immediately cover the entire ICT scope is a frequent mistake.

An implementation that is too broad, too fast, or insufficiently controlled generally leads to:

- breaks in coherence;
- incomplete reference frameworks;
- loss of readability.

MS4ICT prioritises progressiveness and coherence over exhaustiveness.

8.2.4 Vigilance 3 – Producing Documentation Without Coherence

Producing documents, tables, or registers does not in itself guarantee coherent governance.

Without compliance with the coherence engine:

- reference frameworks become silos;
- links remain implicit or absent;
- decisions are no longer explainable.

The value of MS4ICT lies in the relationships between elements, not in the volume of documentation.

8.2.5 Vigilance 4 – Treating Compliance Independently of Risk

Isolating compliance from risk management reproduces the very drifts that MS4ICT is designed to correct.

Within MS4ICT:

- every obligation must be justified by a risk;
- every control must respond to an obligation or an explicit intent.

Compliance handled without linkage to risk weakens governance and complicates prioritisation.

8.2.6 Vigilance 5 – Multiplying Controls Without Justification

Adding controls without a clear link to risks or applicable obligations leads to heavy, unreadable, and poorly defensible governance.

Each control must be able to answer simple questions:

- which risk does it cover?
- which obligation does it address?
- which responsibility is associated with it?

A control that cannot be justified represents a methodological weakness.

8.2.7 Vigilance 6 – Allowing Implicit Responsibilities

Implicit or assumed responsibilities are incompatible with MS4ICT.

Any governance responsibility must be:

- explicitly defined;
- linked to controls;
- associated with a clear intent.

The absence of explicit responsibility creates grey areas, conflicts, and a loss of accountability.

8.2.8 Vigilance 7 – Adapting the Method to the Existing Organization

MS4ICT is not designed to faithfully reflect the existing state, but to **structure governance**.

Attempting to align the method with disorganised practices, unclear responsibilities, or incoherent reference frameworks neutralises its value.

The organization may evolve.

The method must remain stable.

8.2.9 Vigilance 8 – Reducing MS4ICT to a Documentary Exercise

MS4ICT is neither a documentation model nor a purely declarative framework.

An implementation that does not lead to:

- explainable decisions;
- clear responsibilities;
- assumed trade-offs;

constitutes an **incomplete or distorted implementation**.

8.2.10 Vigilance 9 – Ignoring the Explainability Dimension

Governance that cannot be explained to executive management, auditors, or stakeholders is fragile governance.

Every choice made within MS4ICT must remain explainable without resorting to excessive jargon or deep technical expertise.

Explainability is a success criterion, not a bonus.

8.2.11 Vigilance 10 – Modifying the Method to Solve a Local Problem

A problem encountered during implementation must never lead to a direct modification of the method.

Within MS4ICT:

- local problems belong to implementation;
- adaptations occur at the tooling or organizational level.

The method remains stable.

This is an essential condition for its durability and credibility.

8.2.12 Role of the Vigilance Points within MS4ICT

The vigilance points:

- protect the method against drift;
- strengthen the quality of governance;
- facilitate audit and justification;
- ensure controlled adoption.

They should be reviewed at every key stage of the MS4ICT implementation.

9 COMMON PITFALLS IN THE IMPLEMENTATION OF MS4ICT

9.1 PURPOSE OF THE COMMON PITFALLS

This document identifies the most frequently observed pitfalls during the implementation of the MS4ICT method.

These pitfalls do not call the method itself into question, but generally result from:

- misinterpretation of the method;
- operational or regulatory pressure;
- confusion between the method and its implementation.

Identifying them makes it possible to preserve the coherence, explainability, and value of MS4ICT.

9.2 PITFALL 1 – STARTING WITH CONTROLS

A common mistake consists in starting the implementation by selecting or describing controls.

This approach reverses the MS4ICT logic:

- it produces unjustified controls;
- it reinforces a checklist-driven approach;
- it weakens risk-based governance.

Within MS4ICT, controls are a consequence of risks and obligations, never a starting point.

9.3 PITFALL 2 – BUILDING RISKS WITHOUT EVENTS

Formulating risks directly, without relying on the risk events reference framework, introduces a high level of subjectivity.

This pitfall leads to:

- vague or redundant risks;
- divergent interpretations;
- a loss of stability in the risk reference framework.

The event → risk separation is a non-negotiable foundation of MS4ICT.

9.4 PITFALL 3 – MIXING CONTEXT AND RISK

Typical examples include:

- describing an asset as a risk;
- describing an obligation as a risk;
- describing a vulnerability as a risk.

Within MS4ICT:

- ***the context explains why a risk exists;***
- ***a risk results from the structured combination of:***

  event + context + impacts + obligations.

9.5 PITFALL 4 – TREATING COMPLIANCE AS A SILO

Applying MS4ICT solely as a compliance framework is a common drift.

This pitfall manifests itself through:

- obligations listed without any linkage to risks;
- controls applied "by default" or "as a matter of principle";
- difficulty in prioritising or justifying decisions.

Within MS4ICT,

Compliance is integrated into risk-based governance; it is not a separate domain

9.6 PITFALL 5 – CREATING GENERIC RESPONSIBILITIES

Defining responsibilities that are too broad or vague, without an explicit link to controls, weakens governance.

Typical examples include:

- "the CISO is responsible for security";
- "IT is responsible for risks".

Within MS4ICT, a responsibility must always specify:

- the what,
- the how,
- and above all, the intent.

9.7 Pitfall 6 – Attempting to reflect the existing organization

Seeking to make MS4ICT perfectly match the existing organization is a strategic mistake.

This approach:

- freezes existing dysfunctions;
- prevents the clarification of responsibilities;
- neutralises the structuring value of the method.

MS4ICT is not a mirror of the existing state, but a framework for structuring governance.

9.8 Pitfall 7 – Adapting the Method to go faster

Modifying the method to save time or to simplify an implementation is a critical mistake.

- It generally leads to:
- breaks in coherence;
- loss of explainability;
- audit difficulties.

Time or tooling constraints must be addressed at the implementation level, never at the method level.

9.9 Pitfall8 – Multiplying views without coherence

Creating multiple views without strictly relying on the coherence engine leads to contradictions.

Consequences include:

- divergent messages depending on roles;
- misunderstandings between teams;
- loss of trust in governance.

Within MS4ICT, views are coherent projections, not independent representations.

9.10 Pitfall 9 – Reducing MS4ICT to a Documentary delivrable

Producing MS4ICT documents without any impact on decision-making is a frequent drift.

Effective MS4ICT governance must enable:

- explicit trade-offs;
- clear prioritisation;
- assumed and accountable responsibilities.

Without decision-making, the method is used in an incomplete manner.

9.11 Pitfall 10 – Neglecting explanation to stakeholders

Implementing MS4ICT without explaining the underlying logic to the relevant stakeholders weakens its adoption.

The method relies on:

- a shared language;
- a common understanding;
- the ability to explain choices.

Stakeholder appropriation is a key success factor, on a par with methodological rigor.

9.12 Role of common pitfalls in implementation

Common pitfalls:

- serve as benchmarks for self-assessment;
- facilitate the detection of deviations;
- strengthen implementation maturity.

They should be reviewed regularly, in particular:

- during governance reviews;
- prior to an audit;
- when the scope changes.

9.13 Key message

Errors are not failures, but warning signals.

A successful MS4ICT implementation is not one that avoids all errors, but one that is able to identify them, correct them, and preserve the coherence of the method.

10 . MS4ICT USE CASES

10.1 MS4ICT USE CASES – GENERAL PRINCIPLES

10.1.1 Objective of the Use Cases

The purpose of the use cases is to illustrate the concrete application of the MS4ICT method in real ICT governance situations.

They do not constitute procedures, nor implementation guides.

They aim to make the method:

- understandable,
- explainable,
- and conceptually applicable.

Use cases make it possible to visualise how the reference frameworks and the coherence engine work together across a variety of contexts.

10.1.2 Nature of MS4ICT Use Cases

An MS4ICT use case is:

- narrative;
- illustrative;
- non-technical.

It describes:

- a governance situation;
- the associated challenges;
- the way in which MS4ICT structures understanding;
- decision-making and coherence.

It never describes:

- a tool;
- a configuration;
- a detailed operational process;
- an automation

10.1.3 Standard Structure of an MS4ICT Use Case

Each MS4ICT use case follows a common logical structure:

1. Context

- description of the organizational situation;
- scope concerned.

2. Events

- facts or situations likely to affect the organization.

3. Risks

- risks identified based on events and context.

4. Obligations

- applicable normative, regulatory, or contractual requirements.

5. Governance Decisions

- selected controls;
- associated responsibilities.

6. Outcome

- MS4ICT's contribution in terms of coherence, readability, and decision-making capability.

This structure reflects the MS4ICT coherence chain, without ever translating it into an implementation.

10.1.4 Use Cases as an Explainability Tool

Use cases play a central role in the explainability of the method.

They enable:

- executive management to understand the decisions that have been made;
- teams to position their role within governance;
- auditors to follow the justification logic;
- stakeholders to share a common language.

A well-formulated use case must be understandable without prior knowledge of MS4ICT.

10.1.5 Use Cases and Non-Exhaustiveness

Use cases do not seek to cover all possible situations.

They are deliberately:

- targeted;
- representative;
- pedagogical.

They serve as conceptual references, not as exhaustive models to be replicated.

10.1.6 Use Cases and Tool Independence

MS4ICT use cases are fully independent of tooling.

They remain valid:

- regardless of the tool used;
- regardless of the level of maturity;
- regardless of the organizational context.

This independence ensures the long-term sustainability of the use cases.

10.1.7 Value of Use Cases within the Method

Use cases make it possible to:

- demonstrate the internal coherence of MS4ICT;
- illustrate risk-based governance;
- facilitate adoption of the method;
- support internal and external communication.

They constitute an essential bridge between methodological rigor and operational understanding.

10.1.8 Position of Use Cases within MS4ICT

Use cases:

- build upon all reference frameworks;
- illustrate the coherence engine;
- precede any tool-based implementation.

They do not modify the method.
They make it readable.

They constitute the final pedagogical layer before moving to implementation, which falls within a different scope.

10.2 MS4ICT USE CASE – ICT INCIDENT WITH GDPR IMPACT

10.2.1 Objective of the Use Case

This use case illustrates how the MS4ICT method structures governance when an ICT incident has a potential impact on personal data.

It demonstrates how MS4ICT makes it possible to:

- link the incident to risk events;
- structure the associated GDPR-related risks;
- clarify the applicable obligations;
- justify governance decisions;
- assign explicit responsibilities.

10.2.2 Context

An organization operates an ICT system supporting critical business processes, including the processing of personal data relating to customers and employees.

The system is essential to business continuity and is subject to multiple regulatory frameworks, particularly those related to data protection.

10.2.3 Event

An incident occurs, resulting in a temporary unavailability of the system, with uncertainty regarding the integrity and confidentiality of the processed data.

The event is classified as an ICT risk event likely to affect:

- service availability;
- the protection of personal data.

10.2.4 Risks

Based on this event, several risks are identified and contextualised:

- risk of impact on the availability of a critical service;
- risk of a personal data breach (unauthorised access, alteration, or loss);
- risk of GDPR non-compliance in the event of failure to meet security or notification obligations.

These risks are analysed taking into account:

- the assets concerned;
- the potential impacts on individuals;
- the legal and reputational consequences.

10.2.5 Obligations

The identified risks reveal several applicable obligations, including in particular:

- the obligation to implement appropriate security measures;
- the obligation to assess the impact of the incident on personal data;
- the obligation to notify, where applicable, in the event of a confirmed personal data breach.

These obligations are never addressed in isolation, but are always linked to the corresponding risks

10.2.6 Governance Decisions

Based on the analysis of risks and obligations, governance decisions are taken:

- activation of controls aimed at restoring service availability;
- structured assessment of the impact on personal data;
- preparation of a reasoned decision regarding whether notification is required;
- coordination between ICT, cybersecurity, DPO, and legal functions.

Each decision is justified through the MS4ICT coherence chain, rather than through an improvised reaction.

10.2.7 Responsibilities

Responsibilities are clarified explicitly:

- ICT teams are responsible for the technical analysis of the incident;
- the cybersecurity function contributes to the assessment of security impacts;
- the DPO is responsible for analysing GDPR obligations and for providing a recommendation regarding notification;
- executive management retains responsibility for the final decision, based on explainable and traceable elements.

This allocation avoids grey areas and strengthens accountability

10.2.8 Outcome and Contribution of MS4ICT

Thanks to MS4ICT:

- the incident is analysed in a structured and coherent manner;
- decisions are explainable to executive management and supervisory authorities;
- GDPR compliance is integrated into overall ICT governance;
- responsibilities are clear and assumed.

The organization does not merely “manage an incident”: it demonstrates controlled and defensible governance.

10.2.9 Lessons Learned from the use case

This use case highlights that MS4ICT:

- naturally links incidents, risk, and compliance;
- avoids isolated or contradictory decisions;
- facilitates coordination between functions;
- strengthens explainability and traceability.

It illustrates the value of MS4ICT in critical situations, where operational pressure must not compromise governance.

10.3 MS4ICT USE CASE – COMPLIANCE AUDIT

10.3.1 Objective of the Use Case

This use case illustrates how the MS4ICT method enables the preparation, structuring, and defence of a compliance audit, whether internal or external.

It shows how MS4ICT transforms an audit from a documentary reconstruction exercise into a coherence verification exercise.

10.3.2 Context

An organization is subject to multiple normative and regulatory requirements, particularly in the areas of information security and ICT governance.

A compliance audit is scheduled in order to verify:

- the existence of the required controls;
- their justification;
- their coherence with the applicable risks and obligations.

10.3.3 Event.

The triggering event is the preparation of a compliance audit, whether internal or external, covering a defined ICT scope.

This event highlights the need to demonstrate the coherence of governance decisions, rather than merely the existence of documentation.

10.3.4 Risks

Several risks are identified in the context of the audit:

- risk of non-compliance in the event of missing or poorly justified controls;
- risk of difficulty in explaining the choices that have been made;
- risk of manual reconstruction of links between risks, obligations, and controls;
- risk of loss of credibility with auditors.

These risks are analysed in relation to the applicable obligations and the audited scope.

10.3.5 Obligations

The identified risks reveal the applicable obligations, including in particular:

- obligations arising from information security standards;
- sector-specific or cross-cutting regulatory requirements;
- contractual obligations, where applicable.

Within MS4ICT, these obligations are already linked to risks and integrated into the existing governance framework.

10.3.6 Governance Decisions

Thanks to MS4ICT, governance decisions are not taken in reaction to the audit.

Controls have been:

- selected on the basis of risks;
- justified by explicit obligations;
- assigned to clearly defined responsibilities.

The audit thus becomes an exercise in verifying already structured decisions, rather than a race for compliance.

10.3.7 Responsibilities

Responsibilities are clearly identified:

- the compliance function leads the preparation of the audit;
- ICT and cybersecurity teams provide the factual elements;
- executive management is able to explain and arbitrate the decisions taken.

This clarity avoids last-minute improvisation and strengthens accountability.

10.3.8 Outcome and Contribution of MS4ICT

Thanks to MS4ICT:

- the links between risks, obligations, and controls are immediately visible;
- each control can be justified;
- each exclusion is explained;
- the Statement of Applicability becomes a tool for explanation, rather than a defensive document.

The audit focuses on the coherence of governance, rather than on the volume of documentation produced.

10.3.9 Lessons Learned from the Use Case

This use case highlights that MS4ICT:

- reduces the effort required to prepare audits;
- strengthens the credibility of ICT governance;
- facilitates dialogue with auditors;
- transforms audits into a lever for continuous improvement.

It illustrates the value of MS4ICT in demanding contexts, where the ability to explain and justify is as important as compliance itself.

10.4 MS4ICT Use Case – Artificial Intelligence Project

10.4.1 Objective of the Use Case

This use case illustrates how the MS4ICT method structures the governance of an artificial intelligence (AI) project, from its initiation through to decision-making, while integrating risk, compliance, and accountability considerations.

It demonstrates how MS4ICT helps prevent AI projects from becoming isolated, poorly governed, or difficult to explain.

10.4.2 Context

An organization intends to deploy an artificial intelligence (AI) system in order to automate or support a business decision.

The project involves:

- business teams;
- technical teams;
- compliance and legal functions;
- potentially the DPO and executive management.

The AI system is likely to have an impact on individuals, sensitive decisions, or regulatory compliance.

10.4.3 Event

Several risk events are identified within the scope of the AI project, including in particular:

- automated decision errors;
- bias in data or outcomes;
- lack of explainability of decisions;
- use inconsistent with the original intended purpose;
- excessive reliance on an algorithmic system.

These events are identified independently of any technical solution, as facts that may occur.

10.4.4 Risks

Based on these events, AI-related risks are constructed and contextualised, such as:

- risk of infringement of individuals' rights and freedoms;
- risk of regulatory non-compliance;
- reputational risk in the event of a contestable decision;
- risk of loss of control over a critical process.

These risks are analysed taking into account:

- the context in which the AI system is used;
- the potential impacts;
- the applicable obligations.

10.4.5 Obligations

The identified risks reveal several obligations, including in particular:

- obligations related to AI governance;
- requirements regarding explainability and oversight;
- personal data protection obligations, where applicable;
- internal governance and ethical requirements.

These obligations are integrated into the governance of the project, rather than being treated as isolated external constraints.

10.4.6 Governance Decisions

Based on the analysis of risks and obligations, governance decisions are taken, for example:

- strictly framing the authorised use cases;
- defining human oversight mechanisms;
- imposing explainability requirements;
- limiting or conditioning certain automated decisions;
- formalising acceptance and termination criteria for the system.

Each decision is justified through the MS4ICT coherence chain, rather than by a mere technological opportunity.

10.4.7 Responsibilities

Responsibilities are explicitly clarified:

- business teams are responsible for the use of the AI system and the decisions taken;
- technical teams are responsible for ensuring the system's compliance with the defined requirements;
- compliance, legal, and DPO functions contribute to the analysis of risks and obligations;
- executive management retains responsibility for arbitration and risk acceptance.

This allocation avoids diffuse or implicit responsibilities, which are frequent in AI projects.

10.4.8 Outcome and Contribution of MS4ICT

Thanks to MS4ICT:

- the AI project is governed as a risk-driven project, rather than as a mere technical innovation;
- decisions are explainable to executive management, stakeholders, and supervisory authorities;
- obligations are integrated from the outset;
- accountability for decisions is clearly assumed.

Artificial intelligence thus becomes a controlled governance object, rather than an organizational grey area.

10.4.9 Lessons Learned from the Use Case

This use case shows that MS4ICT:

- enables anticipation of AI-related risks before they materialise;
- structures AI project governance in a coherent and sustainable manner;
- facilitates dialogue between business, technical, compliance, legal, and executive functions;
- makes AI-related decisions defensible and explainable.

It illustrates MS4ICT's ability to integrate emerging technologies into risk- and accountability-based ICT governance.

10.5 MS4ICT Use Case - Dependency on a Crtical ICT Supplier

10.5.1 Objective of the Use Case

This use case illustrates how the MS4ICT method enables the structuring of governance for dependencies on critical ICT suppliers or third parties.

It shows how MS4ICT helps the organization to:

- identify risks related to third parties;
- link those risks to the applicable obligations;
- justify governance decisions;
- clarify the associated responsibilities.

10.5.2 Context

An organization relies on an external ICT supplier for the operation of a critical service (hosting, cloud services, application platform, or managed service).

This supplier plays a central role in business continuity and in the processing of sensitive information.

Dependency on this third party introduces specific risks that extend beyond the organization's internal scope

10.5.3 Event

Several risk events are identified in relation to this dependency, including in particular:

- prolonged unavailability of the supplier's service;
- operational or financial failure of the third party;
- a security incident affecting the supplier;
- non-compliance with contractual commitments;
- unilateral changes to the service conditions.

These events are identified as facts that may occur, independently of the organization's internal capabilities.

10.5.4 Risks

Based on these events, risks are constructed and contextualised, such as:

- risk of disruption to service continuity;
- risk of loss of operational control;
- risk of regulatory non-compliance in the event of supplier failure;
- legal and reputational risk related to liability towards customers or supervisory authorities.

These risks are analysed with regard to:

- the criticality of the service concerned;
- internal dependencies;
- the potential impacts on the organization.

10.5.5 Obligations

The risks related to the supplier reveal several applicable obligations, including in particular:

- obligations related to third-party risk management;
- continuity and resilience requirements;
- contractual and regulatory obligations;
- requirements for supplier oversight and supervision.

These obligations are integrated into overall governance, rather than being treated as isolated constraints.

10.5.6 Governance Decisions

Based on the analysis of risks and obligations, governance decisions are taken, for example:

- formally framing the relationship with the supplier;
- defining continuity and security requirements;
- establishing oversight and evaluation mechanisms;
- identifying fallback or mitigation solutions;
- formalising the conditions for acceptance of residual risk.

Each decision is justified through the MS4ICT coherence chain, rather than through an opportunistic approach.

10.5.7 Responsibilities

Responsibilities are explicitly clarified:

- ICT teams are responsible for assessing the technical dependency;
- compliance and legal functions contribute to the analysis of obligations and contractual commitments;
- executive management is responsible for accepting the risk related to the supplier;
- business functions are involved in assessing the business impact.

This allocation avoids diffuse responsibilities and strengthens accountability.

10.5.8 Outcome and Contribution of MS4ICT

Thanks to MS4ICT:

- dependency on the supplier is treated as a governed risk;
- decisions are explainable and traceable;
- obligations are integrated within a coherent governance logic;
- accountability for residual risk is clearly assumed.

The relationship with the supplier is no longer purely contractual or technical, but is fully integrated into ICT governance.

10.5.9 Lessons Learned from the Use Case

This use case highlights that MS4ICT:

- enables the structured management of critical third-party dependencies;
- avoids blind spots related to external dependencies;
- facilitates coordination between ICT, legal, compliance, and executive functions;
- strengthens the resilience and credibility of ICT governance.

It illustrates MS4ICT's ability to integrate external risks into coherent and sustainable risk-based governance.

11 . MS4ICT GLOSSARY

This glossary defines the key terms used in the MS4ICT method (*Management System for ICT*). The definitions are normative: they are authoritative within the scope of the method and prevail over any external interpretation.

Asset

An element that has value for the organization and falls within the scope of ICT governance.

An asset may be:

- informational;
- technical;
- human;
- organizational;
- or related to a third party.

Within MS4ICT, only assets that are relevant to risk and governance are considered.

Coherence

A fundamental principle of MS4ICT ensuring that each governance element is logically, justifiably, and traceably linked to the others.

No element exists in isolation:
a control responds to a risk, a risk is linked to an event, and a responsibility is associated with an intent.

Context

A structured description of the environment in which ICT governance is exercised.

The context includes, in particular:

- the organizational scope;
- critical assets;
- roles and entities;
- applicable obligations;
- internal and external dependencies.

The context is the starting point of any MS4ICT analysis.

- **Control**

A measure decided by the organization to reduce a risk or limit its impacts, and to respond to one or more obligations.

Within MS4ICT:

- a control never exists without a risk;

- it is always justified;
- it is associated with explicit responsibilities.

A control may simultaneously address multiple normative frameworks.

- Risk Event

A fact that may occur and affect the organization, independently of context or impacts.

Examples include:

- service unavailability;
- system compromise;
- human error;
- supplier failure.

Risk events constitute the objective foundation of MS4ICT risk analysis.

- Explainability

The ability to clearly explain ICT governance, the decisions taken, and the relationships between elements, without relying on technical or normative jargon.

Within MS4ICT, every decision must be:

- understandable;
- justifiable;
- defensible.

ICT Governance

The set of decisions, responsibilities, and mechanisms enabling the controlled, coherent, and goal-aligned management of information technologies.

MS4ICT considers ICT governance as:

- transversal;
- risk-oriented;
- explainable;
- sustainable.

Risk-Based Governance

An approach in which risk constitutes:

- the entry point;
- the prioritisation criterion;
- and the exit point of ICT governance.

Within MS4ICT, all governance decisions are founded on risk.

Method

A structuring framework defining principles, rules, and reference frameworks for organizing ICT governance.

MS4ICT is a method, and not:

- a tool;
- a standard;
- a software product;
- or a procedure.

Coherence Engine

The central component of MS4ICT ensuring systematic and traceable links between:

- context;
- events;
- risks;
- obligations;
- controls;
- responsibilities.

The coherence engine transforms independent reference frameworks into an integrated governance system.

Obligation

A requirement arising from:

- a standard;
- a law or regulation;
- a contract;
- or an internal commitment.

Within MS4ICT, an obligation is always analysed through the risk it addresses.

Reference Framework

A structured set of information covering a specific aspect of ICT governance.

MS4ICT relies on several distinct reference frameworks:

- context;
- responsibilities;
- risk events;
- risks;

- controls.

Each reference framework is autonomous in its content, yet dependent in its meaning.

Responsibility

An action or decision assigned to a role, exercised according to a defined mode and with an explicit intent.

Within MS4ICT, a responsibility is described according to the model:

- Who – the responsible role or entity;
- What – the action or decision to be carried out;
- How – the means or methods by which it is exercised;
- Intent – the purpose and justification of the responsibility.

A responsibility without explicit intent is not valid within MS4ICT.

Who – What – How – With What Intent

Risk

A structured combination of:

- an event;
- a context;
- potential impacts;
- and applicable obligations.

Within MS4ICT, risk is an explainable, traceable, and actionable object, not a simple abstract formulation.

SoA (Statement of Applicability)

A structured view of the controls reference framework indicating:

- applicable controls;
- excluded controls;
- and their justification.

Within MS4ICT, the SoA is a result of coherence, not an isolated document.

Traceability

The ability to retrace the origin, justification, and relationships of each governance decision.

Traceability enables:

- auditing;
- justification;
- continuity of governance over time.

MS4ICT View

A coherent and filtered projection of the reference frameworks, tailored to a specific role (executive management, ICT, cybersecurity, compliance, DPO, legal, AI).

A view creates no new information; it makes governance readable for its intended audience.

Tool-Agnostic

Principle according to which the MS4ICT method is independent of any tool, technology, or software solution.

Tools must adapt to the method, never the reverse.

12 TOOLING REQUIREMENTS FOR THE MS4ICT METHOD

12.1 PURPOSE OF THE TOOLING REQUIREMENTS

The tooling requirements define the minimum capabilities that a tool, platform, or documentary support must provide in order to enable a faithful implementation of the MS4ICT method.

These requirements do not describe:

- a specific tool;
- a technical solution;
- a target architecture.

They express what tooling must comply with so as not to alter the coherence, explainability, and sustainability of the method.

12.2 GENERAL PRINCIPLE OF ALIGNMENT WITH THE METHOD

Any tooling used within the scope of MS4ICT must adapt to the method, and must not constrain or modify it.

A tool is considered compatible with MS4ICT if it enables the application of all reference frameworks, the coherence engine, and the views, without introducing any methodological break.

12.3 REQUIREMENT 1 – EXPLICIT SUPPORT FOR MS4ICT REFERENCE FRAMEWORKS

Tooling must allow the representation of all MS4ICT reference frameworks, namely:

- context;
- responsibilities;
- risk events;
- risks;
- controls.

Each reference framework must be managed as a distinct object, without undue merging or simplification.

12.4 REQUIREMENT 2 – ABILITY TO MANAGE COHERENCE RELATIONSHIPS

Tooling must enable the explicit representation of relationships between reference frameworks, in accordance with the rules of the coherence engine.

It must be possible to link:

- an event to one or more risks;
- a risk to an explicit context;
- a risk to obligations;
- an obligation to controls;
- a control to responsibilities.

Any implicit or non-traceable relationship constitutes a methodological non-compliance.

12.5 Requirement 3 – Full Traceability of Decisions

Tooling must allow governance decisions to be traced, in particular:

- why a risk is identified;
- why a control is selected or excluded;
- why a responsibility is assigned;
- why residual risk is accepted.

This traceability is essential for audit, justification, and sustainable governance.

12.6 Requirement 4 – Support for Explainability

Tooling must enable governance to be explained without requiring advanced technical expertise.

It must be possible to:

- understand the links between elements;
- justify decisions;
- produce a readable view for executive management, compliance, or auditors.

A tool that obscures or complicates governance logic is incompatible with MS4ICT.

12.7 Requirement 5 – Generation of Coherent Views

Tooling must allow the production of differentiated views from a single source of truth, without data duplication.

Views must:

- be coherent with one another;
- reflect the coherence engine;
- be adapted to roles (executive management, ICT, cybersecurity, compliance, DPO, legal, AI).

Any view that is contradictory or disconnected from the reference frameworks constitutes a methodological breach.

12.8 Requirement 6 – Management of the Statement of Applicability

Tooling must enable the production of a Statement of Applicability consistent with MS4ICT.

Each control must be:

- justified by a risk;
- linked to an obligation;
- associated with responsibilities.

Exclusions must be explainable and traceable.

12.9 Requirement 7 – Independence from Normative Frameworks

Tooling must not impose a single or rigid view of a specific normative framework.

It must allow:

- multi-framework alignment;
- coexistence of multiple obligations;
- justification of a single control
- against multiple reference frameworks.

Any single-standard logic is contrary to the spirit of MS4ICT.

12.10 Requirement 8 – Evolution Without Loss of Coherence

Tooling must allow reference frameworks to evolve without breaking overall coherence.

It must be possible to integrate:

- new risks;
- new obligations;
- new contexts;
- new use cases (e.g. AI);

without calling into question the existing methodological structure.

12.11 Requirement 9 – Clear Separation Between Method and Implementation

Tooling must not:

- force operational workflows;
- impose technical processes;
- conflate governance with execution.

The MS4ICT method must remain readable and usable independently of the tooling used.

12.12 Requirement 10 – Support for Governance, Not Substitution

Tooling must support governance decision-making, not replace it.

It must enable:

- human arbitration;
- explicit risk acceptance;
- accountability for decisions.

A tool that automates governance or removes arbitration is incompatible with MS4ICT.

12.13 Position of Tooling Requirements within MS4ICT

The tooling requirements:

- define the compatibility framework for tools;
- protect the method against technical drift;
- guarantee a faithful implementation.

They constitute a methodological contract between the MS4ICT method and any present or future implementation solution.

13 ANTI-DRIFT RULES FOR MS4ICT TOOLING

13.1 PURPOSE OF THE ANTI-DRIFT RULES

The anti-drift rules define the methodological prohibitions applicable to any tooling used with the MS4ICT method.

They aim to prevent tooling from:

- distorting the method;
- introducing incoherences;
- replacing governance with automation.

These rules are non-negotiable.

Any tooling that violates them is incompatible with MS4ICT.

13.2 RULE 1 – PROHIBITION OF CREATING CONTROLS WITHOUT RISK

Tooling must never allow the creation or activation of controls without an explicit link to an identified risk.

Any control must be:

- justified by a risk;
- linked to an obligation or to an explicit intent.

A tool that facilitates the addition of "default" or "template-based" controls without justification introduces a checklist-driven drift.

13.3 RULE 2 – PROHIBITION OF GENERATING RISKS WITHOUT EVENTS

Tooling must not allow the creation of risks without attachment to a risk event.

The event → risk separation is a foundation of MS4ICT.

A risk generated directly, without an event-based foundation, introduces subjectivity and instability.

13.4 RULE 3 – PROHIBITION OF MASKING THE COHERENCE CHAIN

Tooling must never mask, simplify, or make invisible the MS4ICT coherence chain.

Context → Event → Risk → Obligation → Control → Responsibility

Any information presented must be traceable back to the complete coherence chain.

A tool that "hides complexity" by removing links directly weakens explainability.

13.5 Rule 4 – Prohibition of Automated Governance Decisions

Tooling must never:

- decide on risk acceptance;
- impose a control;
- validate compliance;
- assign a responsibility.

MS4ICT governance relies **on human, reasoned, and assumed decisions**.

Tooling supports decision-making; it does not decide.

13.6 Rule 5 – Prohibition of Freezing the Method in a Technical Model

Tooling must not lock MS4ICT into a rigid or non-evolutive technical schema.

The method must be able to:

- evolve with context;
- integrate new frameworks;
- adapt to new uses (e.g. AI).

A tool that prevents such evolution creates an unacceptable methodological dependency.

13.7 Rule 6 – Prohibition of Confusing Governance and Operations

Tooling must not:

- impose operational workflows;
- transform governance into procedures;
- confuse controls with execution.

MS4ICT clearly distinguishes between:

- governance (what, why);
- implementation (how).

Any mixing of the two weakens the method.

13.8 Prohibition of Contradictory or Incoherent Views

Tooling must never produce views that contradict one another across roles.

Two views may be different, but never incoherent.

Any unexplained divergence between Executive, ICT, Cybersecurity, or Compliance views constitutes a coherence breach.

13.9 Rule 8 – Prohibition of Critical Dependency on the Tool

Tooling must not render the MS4ICT method unusable outside of itself.

The method must remain:

- documented;
- understandable;
- exportable;
- transferable.

Critical dependency on a tool undermines governance sustainability.

13.10 Rule 9 – Prohibition of Methodological Opacity

Tooling must never:

- conceal justifications;
- make decisions unreadable;
- prevent logical auditing.

Every choice must remain:

- traceable;
- explainable;
- defensible.

Opacity is incompatible with MS4ICT.

13.11 Rule 10 – Prohibition of Adapting the Method to Tool Limitations

Tool limitations never justify adapting the method.

If a tool does not allow MS4ICT to be applied correctly, the tool is unsuitable, not the method.

13.12 Role of the Anti-Drift Rules within MS4ICT

The anti-drift rules:

- protect methodological integrity;
- serve as exclusion criteria for tooling;
- guarantee sustainable governance;
- prevent techno-centric drift.

They constitute the last line of defence between the MS4ICT method and any implementation that could weaken it.

Management System for ICT.

The Method
Version 1.0
Edition 2026

MS4ICT is a methodological framework for ICT governance, founded on risk, coherence, traceability and explainability of decisions.

The method is independent of any tool and is intended for executive management, as well as ICT, cybersecurity, compliance and governance professionals

ISBN 978-99987-651-1-5