Technical Specification

ISO/IEC TS 38508

First edition
2024-02

Information technology — Governance of IT — Governance implications of the use of a shared digital service platform among ecosystem organizations

Technologies de l'information — Gouvernance des technologies de l'information — Implications de gouvernance de l'utilisation d'une plateforme mutualisée de services numériques dans les organisations d'un écosystème

Reference number
ISO/IEC TS 38508:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Overview of shared digital service platform among ecosystem organizations ... **2**
4.1 The purpose of a shared digital service platform among ecosystem organizations ... 2
4.2 Governance arrangement of shared digital service platform among ecosystem organizations ... 3
4.2.1 General ... 3
4.2.2 Centralized model ... 3
4.2.3 Consortium model ... 3
4.2.4 Open platform model ... 3
4.3 Consortium model — exemplar of an alliance ... 4

5 Benefits of good governance of a shared digital service platform ... **5**

6 Governance framework for a shared digital service platform ... **5**

7 Governance model for organizations participating in shared digital service platform ... **6**

8 Guidance for the governance of a shared digital service platform ... **8**
8.1 General ... 8
8.2 Strategy ... 8
8.3 Acquisition ... 8
8.4 Compliance ... 9
8.5 Performance ... 9
8.6 Human behaviour and culture ... 9
8.7 Data quality ... 10
8.8 Risk governance ... 10
8.9 Organizational governance oversight ... 11

9 Guidance for the management of shared digital service platform ... **12**
9.1 Roles of management ... 12
9.2 Considerations for management systems ... 12

Annex A (informative) **Plug and play architecture of a platform and its ecosystem** ... **14**

Annex B (informative) **Use case of shared digital service platform** ... **15**

Bibliography ... **16**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT service management and IT governance.*

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Organizations are increasingly using plug and play architecture on shared digital service platforms to develop new digital services that can be adapted to meet future needs. This architecture allows organizations to add new applications and features to the platform without disrupting the overall system. Using a shared digital service platform also enables organizations to enhance the value they offer to customers by bundling existing capabilities with new digital capabilities and forming flexible value networks with business partners and suppliers.

The plug and play architecture of a shared digital service platform can easily add the applications of suppliers or other ecosystem organizations. For example, a product manufacturer could monitor product performance data for preventive maintenance by adding applications from their part suppliers and other ecosystem organizations.

The plug and play architecture of a shared digital service platform also enables independently developed applications to be combined and integrated into the platform through a standardized interface, thereby reducing overall adjustment costs incurred in the platform ecosystem. The plug and play architecture of the platform enables ecosystem organizations to focus on their work relatively autonomously, which ultimately helps to lower both application innovation costs and system integration costs borne by the ecosystem organizations.

The plug and play architecture of a shared digital service platform lays the foundation for platform participants to innovate the platform through application development instead of the platform owner being fully responsible for application development and thus platform innovation. The plug and play architecture of the platform and its underlying scalable technologies, with the option of adding additional elements [technology for Internet of Things (IoT), data storage, application development, analytics and security], makes it possible for organizations to dramatically enhance value offered to customers by easily expanding the organizations' existing capabilities with new digital capabilities in cooperation with the ecosystem organizations.

The use of a shared digital service platform creates governance and control issues that the governing body and management have to ensure are addressed. These include ensuring that there is a clear basis for governance and a governance framework that provides policies and accountabilities that meet the organization's requirements.

This document aims to provide guidance to the governing body of organizations that are accountable for their organization's adoption of a digital service platform among an ecosystem organization. Thus, this document focuses on governance and not on the technologies themselves. The technological and managerial aspects of a "digital service platform" are only covered to the extent that is necessary to understand the governance implications of their use.

For information on the technological aspects of digital service platforms and cloud computing, please see ISO/IEC TS 5928 and ISO/IEC 22123-2.

This document is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. This document is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their dependence on data or information technologies.

Information technology — Governance of IT — Governance implications of the use of a shared digital service platform among ecosystem organizations

1 Scope

This document provides guidance for members of governing bodies of organizations on the effective, efficient and acceptable use of a shared digital service platform among ecosystem organizations by:

— establishing a vocabulary for the governance of a shared digital service platform among ecosystem organizations;

— providing a framework for understanding the implications of the use of a shared digital service platform among ecosystem organizations;

— guiding governing bodies to evaluate, direct and monitor the introduction and use of a digital service platform, applying the governance principles of ISO/IEC 38500;

— assuring stakeholders that, if the guidance proposed by this document is followed, they can have confidence in the organization's use of shared digital service platform among ecosystem organizations.

This document also provides guidance to those advising, informing or assisting governing bodies, including:

— executive managers;

— members of groups monitoring the resources within the organization;

— external businesses or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies;

— public authorities and policy makers;

— internal and external service providers (including consultants);

— auditors.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 38500, *Information technology — Governance of IT for the organization*

ISO/IEC 38505-1, *Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data*

ISO 37000, *Governance of organizations — Guidance*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 38500, ISO/IEC 38505-1, ISO 37000 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
alliance
collaborative relationship formed between two or more organizations to pursue common interests or objectives

Note 1 to entry: Alliance can be formally contracted agreements or be entirely informal.

3.2
consortium
cooperative arrangement where several organizations or entities join together to achieve a common goal

Note 1 to entry: A consortium typically involves multiple independent entities, such as companies, pooling their resources, expertise, and interests to work on a specific project or pursue shared objectives.

Note 2 to entry: Consortium members typically retain their individual identities and operate independently outside of the consortium.

Note 3 to entry: Consortium members contribute resources, contribute to decision-making, and share the risks and benefits associated with the project or initiative.

Note 4 to entry: Consortia are often governed by a set of agreements or contracts that outline the terms of collaboration, resource allocation, intellectual property rights, and other relevant aspects.

3.3
core partner
organization that has a significant role in shaping a shared digital service platform's direction and core functionality

3.4
ecosystem organization
community of business partners, suppliers and customers that share a digital service platform for mutual benefits

3.5
plug and play architecture
architecture of a digital service platform which ensures that the dependencies between the platform core and applications are kept to a minimum and that changes in a platform core or an application do not require corresponding adjustments to ensure continued interoperability

Note 1 to entry: Through the plug and play architecture, resilience and capacity to accommodate changes in the future that were not originally planned can be ensured.

3.6
shared digital service platform
platform that enables partners, suppliers and customers to share resources, processes and capabilities to deliver unique digital services for the ecosystem organizations

4 Overview of shared digital service platform among ecosystem organizations

4.1 The purpose of a shared digital service platform among ecosystem organizations

The purpose of a shared digital service platform is to enable organizations to collaborate with partners and suppliers to create unique digital services for their organizations. Such a platform provides a software tool that allows businesses to rapidly deliver these services by combining products with sensors, data and advanced analytics, thereby creating new value models with significantly improved or unique value

propositions for their organizations.[6] Through effective ecosystem strategies, third-party software and data integration, the shared digital service platform can provide a powerful tool for businesses to create differentiated and more effective digital services that meet the evolving needs of their organizations. Ultimately, the purpose of a shared digital service platform is to facilitate collaboration and innovation among organizations and their partners, leading to the creation of more valuable digital services for organizations.

The shared digital service platform involves an extensible codebase of a software-based system that provides core functionality shared by applications that interoperate with it and the interfaces through which they interoperate.[7] In the shared digital service platform, an application is defined as an add-on software subsystem that is connected to the platform core to add functionality. This allows applications to add functionality to the shared digital service platform and deliver rapid and continuous innovation to organizations that adopt the shared digital service platform.

For more information on the difference between the technical, economic and general uses of the word "platform" in the context of digital services, see ISO/IEC TS 5928.

4.2 Governance arrangement of shared digital service platform among ecosystem organizations

4.2.1 General

Shared digital service platforms among ecosystem organizations involve an alliance between different organizations using the platform to generate value for their organizations. The shared digital service platform among ecosystem organizations can have different governance arrangements based on the specific industry, organization size and goals.

4.2.2 Centralized model

Under this model, one entity is responsible for providing shared services. This central entity has the authority to set policies, define service standards and ensure compliance across different departments or business units involved.

A centralized governing body, consisting of representatives from various departments or business units, makes decisions regarding service offerings, resource allocation and overall strategy for shared services.

The centralized governing body establishes service level agreements (SLAs) with internal stakeholders (e.g. production departments) and external stakeholders (e.g. partners, suppliers and customers), specifying service levels, performance metrics and expectations for shared services.

4.2.3 Consortium model

Under this model, multiple entities, for example manufacturing organizations in the car industry, come together to form a consortium and jointly govern a shared digital service platform (see Annex A for details about roles and responsibilities of the consortium model and Annex B for related use cases). The consortium establishes a governance structure with representatives from participating organizations.

The governing body, consisting of representatives from participating entities, collectively makes decisions regarding service offerings, investment priorities, resource allocation and governance policies for the shared digital service platform.

The consortium establishes SLAs with participating organizations, outlining service levels, responsibilities and financial arrangements for utilizing the shared digital service platform.

4.2.4 Open platform model

Striving to be open, the open platform model encourages collaboration and participation from external stakeholders, such as partners, suppliers or customers. The platform provides a common infrastructure and set of services that can be extended and customized by external parties, fostering innovation and ecosystem

growth. For example, in the financial sector, the platform connects financial institutions and other service providers, enabling seamless integration and interoperability between different financial systems.

In the open platform model, the governance structure includes representatives from the organization operating the platform and external stakeholders, such as partners or developers. The governing body sets rules, standards and policies for platform usage.

The governing body makes decisions related to platform features, integration protocols, data sharing policies, and participation guidelines. It ensures that the platform remains open, secure and aligned with the interests of all stakeholders.

Depending on the nature of the platform, SLAs can be established with external stakeholders, defining service levels, data usage rights and responsibilities.

4.3 Consortium model — exemplar of an alliance

This subclause presents a consortium model as an exemplar of an alliance. Under this model, a shared digital service platform typically involves a consortium of organizations that play different roles (see Annex A for a more detailed description).

The owner of the shared digital service platform is the entity that controls the platform's intellectual property and decides who can participate and in what capacity.[1]

The core partners are the organizations involved in developing the shared digital service platform's core functionality.

Peripheral partners are third-party developers who want to offer their resources, such as applications, sensors, and devices on the shared digital service platform to gain market access.

Organizations can participate in the shared digital service platform ecosystem as either core partners or peripheral partners. Core partners typically have a more significant role in shaping the platform's direction and functionality, while peripheral partners contribute to the platform by adding new applications or devices that can interoperate with the platform's core functionality.

The owner of the shared digital service platform is typically a well-established organization with a large installed base. The owner of the shared digital service platform develops the platform with core partners. The organizations entering the platform ecosystem are attracted to the platform to gain access to the platform owner's installed base, that is, a large customer base. The organizations joining in the ecosystem expect to increase their returns through successful exploitation of the installed base of the platform owner.

Expanding the size of the platform ecosystem is key to the success of the shared digital service platform. In order to do that, the platform owner should incentivize the ecosystem organizations with data, the application programming interface (API) and developer tools to create and monetize services in the platform. To get started, the platform owner needs to actively look for the organizations for collaboration and incentivize them for value cocreation. The platform owner can make a selective decision on integration of the organizations into the ecosystem.

While there are advantages that customers receive through data-based digital services, various problems can occur. Since a large amount of personal data is created, it can be possible to infer the identity of an individual. This in turn can lead to privacy infringement.

Therefore, the governing body of the shared digital service platform needs to establish policies for privacy, security, risk governance and other areas of its digital services.

The governing body ensures that personal data and the fundamental rights of individuals are protected in the case of personal data transfer to third-party processors, especially in third countries. If the platform owner needs to share the sensor data with third-party service providers or make a profit by selling the sensor data, the requirements for the relevant regulations need to be addressed. Guidance should be given on conformance to regulatory requirements for personal data processing.

The governing body should also ensure that its organization implements and maintains appropriate technologies and measures to protect customer and personal data against destruction, loss and unauthorized access or modification. Guidance should be given on conformance with the security and privacy requirements defined in ISO/IEC 27001 and ISO/IEC 27701.

The shared digital service platform may enable organizations to combine devices with sensors, data and advanced analytics to deliver unique digital services to their customers and to shift their existing business model to selling digital services. Since such a shared digital service platform enabled digital transformation requires dramatic changes in strategy, structure, operation and culture, the role of the governing body becomes more important than ever.[5] The following clauses provide governance guidelines on how existing companies can adopt and build the shared digital service platform to spearhead their digital transformations.

5 Benefits of good governance of a shared digital service platform

Good governance of a shared digital service platform assists the governing body in ensuring that the use of a shared digital service platform contributes positively to the performance of the organization by:

— accelerating the flow of innovation into an ecosystem in order to sustain its competitive advantage;

— clarifying role, responsibility and accountability for both the supply of and demand for a shared digital service platform;

— the actual realization of the expected benefits from each IT investment;

— minimizing the risk of negative impact to stakeholders, such as customers, partners and employees, due to security and privacy breaches;

— maximizing the value creation potential of the shared digital service platform by fostering collaboration among ecosystem partners and facilitating the creation of new services and business models;

— building trust among stakeholders through transparent decision-making processes and effective communication.

Overall, good governance of a shared digital service platform can lead to more effective use of digital technologies, improved organizational performance, and enhanced customer experiences.

6 Governance framework for a shared digital service platform

The establishment of a shared digital service ecosystem should involve a governance framework that defines the ecosystem's purpose, guiding principles, decision-making arrangements, participant obligations, and regulatory compliance obligations. This can include memorandums of understanding, SLAs and contracts.

The ecosystem's governing body composition, authority and accountability will depend on the structure of the ecosystem and the basis under which it is organized. Those responsible for the governance of the platform ecosystem should establish a governance framework appropriate for the ecosystem's legal arrangements, complexity and purpose.

Governing bodies of organizations seeking to engage with the shared digital service ecosystem should be aware of the platform alliance's governance arrangements.

The specific issues that need to be dealt with in a governance framework for a shared digital service platform will depend on the purpose and design of the shared digital service platform, but could address the following.

— **Basis:** Whether the ecosystem platform is owned by a single organization or shared by multiple owners.

— **Accountability**: Who is responsible and accountable for budgeting, developing commercial models, marketing, profit sharing, expanding new business lines and criteria for selecting new consortium members?[8]

— **Decision-making structures:** The processes and framework by which decisions are made regarding service offerings, investment priorities, resource allocation and governing policies for the shared digital service platform.

— **Technical strategies:** The mechanism and responsibility for setting information security and other standards for accessing the ecosystem solution, permitting new platform participants when they satisfy applicable criteria and standards, determining the timing of upgrade to a new version of the software, and resolving disputes.[8] Once established, technical architecture is not easy to change, and on a shared digital service platform, such architecture presents a challenge in determining the future evolutionary trajectory of the shared digital service platform. In other words, as technical decisions in the shared digital service platform result in significant strategic consequences, it is necessary for the governing body to strategically review the platform's technical architecture. Thus, the governing body needs to familiar with those technical terms and to recognize that IT architecture is no longer treated a technical component. Rather, the architecture of the shared digital service platform is as a strategic outcome.

— **Policies and practices:** Articulation of policies and practices for managing the platform, which includes:[9]

  — whether the platform is open or closed,

  — who can access the platform,

  — what services are allowed, and

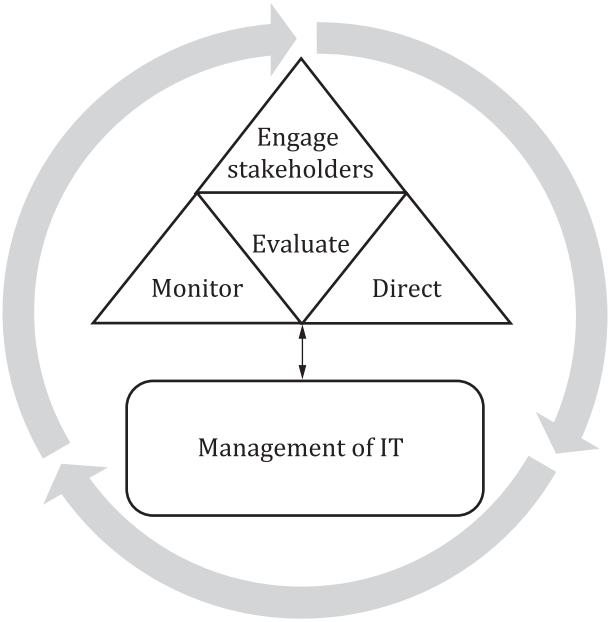
  — the mechanisms to manage the quality of the services.

  The policy statements can also include roles, responsibilities and accountability for setting up such policies.

— **Capabilities for managing external relationships:** The organization's ability to manage the relationships between its IT function and external stakeholders such as partners, suppliers, customers, third-party developers and third-party data service providers. This includes the mechanism and responsibility for managing inter-organizational dependencies and architecture of participation.

7 Governance model for organizations participating in shared digital service platform

The roles of the governing body in the Governance of IT are described in ISO/IEC 38500 as shown in Figure 1.



[SOURCE: ISO/IEC 38500:2024, Figure 1]

Figure 1 — Model for the governance of IT

Members of the governing body are accountable for the effective, efficient and acceptable use of the shared digital service platform. In this regard, the governing body should govern organizational use of a shared digital service platform through the following tasks.

— Engage with relevant stakeholders regarding the use of shared digital service platforms to understand their expectations. This will help the organization to determine the capabilities required and establish agreements regarding the use of IT and data.

— Evaluate recommended proposals and plans for managing the organizational use of a shared digital service platform, ensuring that they will meet the organization's internal and external requirements (or pressure) effectively.

— Direct the organization by adopting strategies and policies for use of a shared digital service platform, ensuring that they are kept up-to-date through periodic review.

— Monitor the organization's performance and conformance with these policies, ensuring that the policies facilitate the organization's achievement of its strategic objectives, and that the management and use of a shared digital service platform conform to internal policies and external requirements (or pressure).

Although the responsibility and authority of a shared digital service platform management are delegated to the management team, the ultimate accountability of a shared digital service platform governance resides in the governing body. The governing body should establish a clear accountability framework for a shared digital service platform. To guide the organization on the use of a shared digital service platform, the governing body needs to ensure that its direction is sufficiently communicated. As specified in ISO/IEC TS 38501, directions from the governing body not only include authorization of strategy, delegations of authority, a range of policies, risk appetite and compliance, but also culture, budgets, required resources and skills, and stakeholder involvement and responsibilities.

8 Guidance for the governance of a shared digital service platform

8.1 General

While a broader guidance for the governance of IT is available in ISO/IEC 38500, this clause elaborates the guidelines on the following areas to fit the purpose of organization's use of a shared digital service platform: (1) strategy, (2) acquisition, (3) compliance, (4) performance, (5) human-behaviour and culture, (6) data quality, (7) risk governance and (8) organizational governance oversight.

8.2 Strategy

The use of a shared digital service platform will potentially have a significant impact on the organization's strategic objectives and value generation model. The governing body of the organization using the platform should, therefore, ensure that the potential impact on the organization's value generation model from the use of such technology is considered. This includes considering how the use of such technology might reshape the organization's business strategies, transforming its business models and processes, and creating new value in the market. For example, a shared digital service platform could be used to connect customers' IoT devices to a broad supply chain of partners, enabling the organization to transform its existing product-based business model into a service-oriented one.

The governing body should assess whether by designing seamless processes with partners and suppliers, the shared digital service platform can help the organization deliver value to its customers. However, the governing body should also consider whether the adoption of a shared digital service platform with the specific partners is appropriate in the organization's competitive environment, taking into account relevant regulatory requirements. They should give consideration to whether the overall purpose and use of the shared digital ecosystem aligns with the purpose, culture and values of the organization.

The governing body should instruct the organization to consider the benefits of utilizing a shared digital service platform as a means of flexible inter-business network redesign. This will enable the organization to collaborate with broad ecosystems, which can provide greater market strength through complementary products and services, rather than competing against them. Flexible inter-enterprise process integration with partner organizations can help the organization develop a broad and new supply and partner network, which can enable it to reshape its business model by leveraging the network's capabilities.

8.3 Acquisition

When making decisions about whether to make or buy a shared digital service platform, the governing body should instruct that there be appropriate and ongoing analysis. Such analysis should strike a balance between the benefits, opportunities, costs and risks, both in the short term and the long term.

In considering whether to adopt a specific shared digital service platform approach, the governing body should evaluate whether the governance arrangements and framework of the platform alliance or consortium are appropriate. This includes considering the legal basis for governance, accountabilities, governance mechanisms and policies and practices.

The governing body should be aware of the advantages and disadvantages of build versus buy. While building a shared digital service platform allows organizations to maintain skills and infrastructure internally and maintain exclusive control of future technology development, it requires significant R&D expertise and expenses. Traditional companies without well-established software development expertise can experience delays in their development plans by building a shared digital service platform instead of gaining a competitive advantage.

Alternatively, by buying services rather than developing a shared digital service platform in-house or outsourcing, companies can focus on their core competency and adapt and scale the future demands without requiring capital investments. However, buying services can cause the organization to lose learning opportunities by not maintaining skills and resources related to a shared digital service platform. This, in turn, exposes the organization to a possible service provider's opportunistic behaviour.

Therefore, the governing body should carefully consider the organization's strategy and competitive environment when deciding whether to make or buy a shared digital service platform. They should balance the benefits and risks of each approach and determine the most appropriate path forward.

8.4 Compliance

The governing body of the platform alliance should establish mechanisms to oversee and ensure the compliance of shared platform policies with legal obligations, and regulatory and contractual obligations. This involves assessing the consortium organization's policies and ensuring that they align with the requirements set out by external bodies such as regulatory authorities and contractual agreements.

The governing body of an organization using the platform as a core partner ensures that its operations and activities on the platform comply with the policies set out by the governance structure of the consortium. This includes adhering to the guidelines and regulations outlined by the governance structure and ensuring that the organization's policies align with those of the shared platform policies.

In addition to the policies set out by the governance structure of the consortium, core partners sometimes need to establish their own policies to govern their use of the platform. These policies can include the following.

— Data privacy and security policies: As core partners are likely to handle sensitive data on the platform, they can need to establish policies that ensure the privacy and security of this data. This can involve guidelines around data access, storage, sharing and disposal.

— User policies: Core partners can need to establish policies that govern how users interact with their products or services on the platform. This can include guidelines around user behaviour, content moderation and dispute resolution.

— Compliance policies: Core partners can need to establish policies that ensure compliance with relevant regulations and laws related to their business operations. For example, if a core partner operates in a highly regulated industry such as healthcare or finance, they can need to establish policies that ensure compliance with industry-specific regulations.

— Intellectual property policies: Core partners can need to establish policies that govern how intellectual property is protected on the platform. This can include guidelines around copyright infringement, trademark violations and trade secret protection.

Overall, the core partner policies should complement the shared digital service platform policies and ensure that their use of the platform aligns with both internal and external requirements.

NOTE Some legislations require responsible stewardship of the organization in handling customer data, especially in relation with operating the platform. For example, the European Union's Digital Service Act requires that customers online be protected with transparency, that organizations provide explanations about how their recommender systems work, and that users can change the criteria used for the recommendation and even block it.

8.5 Performance

The governing body of an organization is accountable for its performance, even when utilizing a shared digital service platform. Therefore, the governing body should monitor the platform's performance and the value being obtained by setting specific, measurable goals that align with the organization's objectives. Key performance indicators (KPIs) for a shared digital service platform will vary depending on the initiative's goals, which could include enhancing organizational and customer productivity, as well as improving customer experience and satisfaction. The governing body ensures that high-level views of key performance metrics are monitored and met.

8.6 Human behaviour and culture

The governing body plays a critical role in addressing the impact of human behaviour and culture on the implementation of a shared digital service platform. By identifying cultural and behavioural factors, developing policies and guidelines, educating and training partners, and monitoring and evaluating

implementation, the governing body can ensure that the platform aligns with the partners' cultural values, norms, and expectations. Key aspects include collaboration between partners, user adoption and change management in the adoption of new processes and practices.

The governing body should ensure that the organization has the right human resources. This includes data scientists and application developers who are needed to analyse platform data and develop applications. New talent pools should be recruited, and existing employees should be retrained to build the organization's data and digital capabilities. It is important to recognize the fear of existing employees being replaced by new talent, and the governing body should make efforts to relate the strengths of employees to the tasks of the digital transformation process. Additionally, the governing body should recognize the development efforts of existing employees and the resulting new credentials they acquire.

The governing body needs to ensure that a new culture is fostered to accept new thoughts, new ways of doing things, and to balance these new talents with existing old culture. Fast and agile decision-making over bureaucracy are considered to be effective in digital transformation. Existing reward systems may need to be redesigned. Developing incentives for creative concepts and projects are considered to be effective for new talents.

8.7 Data quality

The resources associated with a digital service platform are diverse, including physical infrastructure for data collection, IT infrastructure for data storage and processing, and end-applications for users and machine learning algorithms. Some of these resources are under the control of the organization, while others are managed by third parties. For instance, data can be collected from different sources, including vendors, customers, employees, and other stakeholders, creating complex governance challenges.

To address these challenges, the governing body should direct and oversee the implementation of data quality governance to mitigate data quality-related risks and to enhance trust in data for analytical and AI applications. While ISO/IEC 38505-1 describes a broader overview of governance of data, data quality has further practical importance for the shared digital service platform.

NOTE This topic is to be covered in the future ISO/IEC 5259-5:—.[1)]

The general terms of governance implications of the data use in artificial intelligence can be found in ISO/IEC 38507.

One of the governance challenges in a multi-party environment is determining the responsible party if machine learning produces an incorrect output due to anomalies in data collected from multiple sensors, or if the ownership of sensor data lies with external vendors or partners. The governing body needs to establish clear guidelines on data ownership, quality and privacy to ensure accountability and mitigate legal risks and reputational risks.

Furthermore, the governing body should foster collaboration among different stakeholders to promote a culture of trust and transparency. This involves developing communication channels to ensure that all parties have access to relevant information, engaging in open dialogue to address concerns and build consensus, and developing incentives to encourage collaboration and cooperation.

In summary, the governing body of a digital service platform needs to establish clear guidelines and policies for data governance, promote collaboration among stakeholders, and foster a culture of trust and transparency to ensure accountability and mitigate risks associated with data use in artificial intelligence.

8.8 Risk governance

The governing body should ensure that the risks faced by organizations during the development and operation of a shared digital service platform are identified, analyzed, evaluated and monitored as a part of the organization's overall risk management framework.

1) Under preparation. Stage at the time of publication: ISO/IEC CD 5259-5:2023.

Some of these issues are as follows.

— Multiple stakeholders: Shared digital service platforms involve multiple stakeholders who can have different risk tolerances and priorities. Risk management strategies need to take into account the diverse perspectives and priorities of these stakeholders.

— Data privacy and security: Shared digital service platforms often involve the sharing and processing of sensitive data. Risk management strategies need to ensure that appropriate measures are in place to protect the privacy and security of these data.

— Legal compliance and regulatory compliance: Shared digital service platforms need to comply with different natures of legal requirements and regulatory requirements. Risk management strategies need to ensure that the platform meets these requirements, and that appropriate measures are in place to manage legal risks and compliance risks.

— Dependence on third-party services: Shared digital service platforms can rely on third-party services such as cloud computing providers or software vendors. Risk management strategies need to take into account the risks associated with these third-party services and ensure appropriate measures are in place to manage these risks.

— Technical complexity: Shared digital service platforms may involve complex technical systems and architectures. Risk management strategies need to take into account the risks associated with these technical complexities and ensure that appropriate measures are in place to manage these risks.

Overall, the specific issues that need to be considered when establishing risk management for a shared digital service platform will depend on the nature of the platform and its stakeholders. However, the issues outlined above are common considerations that need to be addressed in any effective risk management strategy for a shared digital service platform.

The governing body should also ensure that a framework for the risk management is set and managers reflect risk management policies into their management practices. Such policies include the policies for agreed SLAs of cloud providers as well as policies for the protection of data and members of the workforce. The governing body should also ensure that the necessary resources (such as risk experts with adequate knowledge) are allocated for effective risk management.

For more information on SLAs in cloud computing, see the ISO/IEC 19086 series.

8.9 Organizational governance oversight

The governing body should have oversight of management's progress in implementing the strategy and any risks to the organization that can arise. This requires that the governing body be informed about progress in implementing the organization's IT strategy, as well as the impact of changes to the organization's external and internal environments, to identify areas in which the strategy needs to be adjusted.

When a shared digital service platform is used, the governing body should ensure that there are policies associated with such things as cooperation with other partners within the platform, security of the platform and sharing of data.

The governing body should ensure that the oversight of managers' performance in achieving the business objectives of a shared digital service platform is through the established committee and has mechanisms in place to measure against the desired outcomes. The committee is also responsible for tracking progress on the change activities in relation with shared digital service platforms and gathering and coordinating all relevant information required for direction of the governing body as specified in ISO/IEC TS 38501.

As the needs of the organization evolve, the governing body should monitor the effectiveness of the mechanisms for the governance and management of a shared digital service platform by requiring independent assessments.

9 Guidance for the management of shared digital service platform

9.1 Roles of management

Managers are responsible for attaining the strategic objectives of a shared digital service platform within strategies and policies set by the governing body. In order to achieve the strategic objectives of a shared digital service platform, managers are responsible for implementing management systems.

The management of a shared digital service platform requires a collaborative and structured approach that focuses on governance, user management, and ongoing maintenance to ensure the platform remains secure and effective for all stakeholders.

— A shared digital service platform requires a formal governance structure to oversee its management and ensure that it meets the needs of all stakeholders. This can include a steering committee or advisory board composed of representatives from different organizations using the platform.

— A shared digital service platform can require a more sophisticated user management structure, including identity and access management (IAM) systems, to ensure that only authorized users are granted access to the platform.

— A shared digital service platform can require a dedicated technical support structure to provide support to users and ensure that the platform remains operational and secure.

— A shared digital service platform can require a structured approach to data management, including policies and procedures for data storage, sharing and protection, to ensure compliance with applicable regulations.

— A shared digital service platform can require a formal change management structure to manage updates and upgrades to the platform, including testing and implementation procedures.

Overall, the structures required to manage a shared digital service platform would need to be more complex and tailored to the unique needs of the platform and its users. Effective management of a shared digital service platform requires a coordinated effort among different stakeholders, and the right structures can help to ensure that everyone is aligned and working towards common goals.

To ensure shared digital service platform strategy meets its purpose, managers should establish and enforce shared digital service platform policies. Such policies become rules and guidelines in both the operations and management of a shared digital service platform. The policies should be based on principles and directives set by the governing body as specified in ISO/IEC TR 38502. Policies should also reflect national and international stakeholder requirements and risk appetite.

Managers are responsible for monitoring and assessing the performance and conformance and reporting to the governing body. Roles, responsibilities and reporting procedures should be defined to ensure that management obligations for a shared digital service platform performance and conformance are met. As specified in ISO/IEC TR 38502, managers should also establish internal risk control as part of the management system.

9.2 Considerations for management systems

Managers are responsible for implementing management systems for shared digital service platforms, which include systems dealing with the demand for and the supply of digital services by internal units or external partners as well as the conformance and performance of the shared digital service platform and reporting to the governing body.

Organizations should consider the use of Agile and DevOps practices for software development to enable faster adaptation to changing strategic needs. Agile and DevOps are both approaches to software development that prioritize speed, flexibility and collaboration. Agile emphasizes iterative development and close collaboration between cross-functional teams, while DevOps emphasizes the integration and automation of software development and IT operations.

A shared digital service platform can help to facilitate these practices by providing a common set of tools and resources that enable cross-functional teams to work together more effectively. For example, a shared digital service platform can provide access to tools for continuous integration and deployment, which are critical to the DevOps approach. It can also provide collaboration tools for Agile teams, such as agile boards and real-time communication channels.

Furthermore, a shared digital service platform can help organizations to adapt quickly to changing strategic needs by enabling rapid deployment of new features and functionality. This is especially important in today's fast-paced organizational environment, where organizations need to adapt quickly to changing market conditions and needs.