IT-Planungsrat

Strategy for strengthening the digital sovereignty of public administration IT

Strategic objectives, approaches and implementation measures

– Version 1.0 January 2021 –

Publication data

Published by

FITKO (Federale IT Cooperation)
Zum Gottschalkhof 3
60594 Frankfurt am Main
Email: poststelle@fitko.de
Institution under public law | Dr Annette Schmidt, president

Contact

Division DG II 2 - Digital Sovereignty for Public Administration IT
Federal Ministry of the Interior, Building and Community
Postal address: Alt-Moabit 140, 10557 Berlin, Germany
Street address: Salzufer 1 (enter from Englische Straße), 10587 Berlin, Germany
Email: DGII2@bmi.bund.de
www.cio.bund.de

Version of

January 2021

Table of contents

Summary

The information technology (IT) of Germany's public administration is highly – in some cases critically – dependent on individual technology vendors. As a result, the public administration is at risk of losing control of its own IT, in which case, among other things, it would no longer be able to ensure information and data protection in compliance with national and EU legislation. Digital sovereignty is defined here as the capabilities and possibilities of individuals and institutions to perform their roles in the digital world autonomously, confidently and safely.[1] In updating the policy paper on strengthening the digital sovereignty of Germany's public administration, the federal, state and local governments agreed on three strategic objectives: I. ability to choose/switch, II. design capability, and III. influence on vendors. Eight approaches are associated with these objectives and intended to help achieve them. The joint working group on cloud computing and digital sovereignty is defining specific measures for each approach and is working on them or supporting their implementation (see Figure 1). The measures are continually being further developed at federal, state and local level.

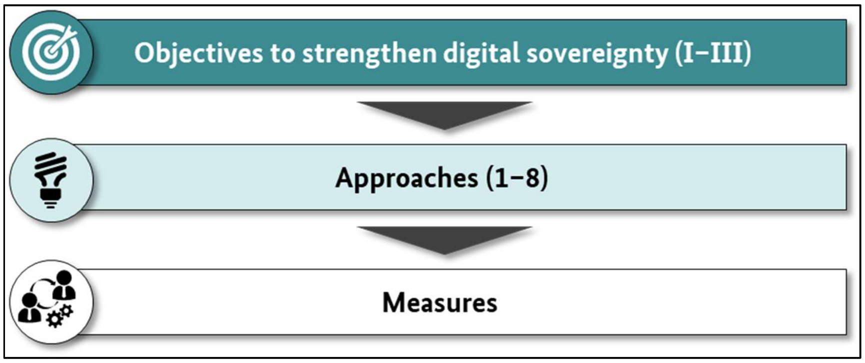


Figure 1: How the strategic objectives, approaches and measures are connected

[1] As defined in the study "Digitale Souveränität" (Digital sovereignty) conducted by the Competence Centre for Public IT (ÖFIT).

1 Introduction

The federal, state and local governments have set themselves the goal of maintaining and continually strengthening the digital sovereignty of the public administration. The IT Planning Council established the working group on cloud computing and digital sovereignty on 27 June 2019 at its 29th meeting (Decision 2019/38) as a joint federal and state working group led by North Rhine-Westphalia and the Federal Government (represented by the Federal Ministry of the Interior, Building and Community) with members from the national associations of local authorities and of data protection. In doing so, the IT Planning Council created a framework for coordinating the project of strengthening the digital sovereignty of the public administration in Germany. With its decision to adopt the policy paper on strengthening the digital sovereignty of public administration[2] (on 25 March 2020 at its 31st meeting; Decision 2020/07), the IT Planning Council also stressed *"the enormous strategic significance [of strengthening digital sovereignty] for the public administration in Germany"*.[3]

The COVID-19 pandemic has highlighted the role of IT as critical infrastructure. With this in mind, the European Union has made millions of euros available for investment in digital infrastructure,[4] among other things; discussed digital sovereignty as a priority during Germany's Presidency of the Council of the EU;[5] and continues to emphasise the special relevance of this undertaking: *"To ensure Europe's economic success and thus its capacity to act going forward, Europe must acquire both technological and digital sovereignty."*[6] Last-minute digital solutions applied in response to crises or their aftermath must be compatible with the norms and values of Germany and the EU, for example with regard to information security and data protection. Digital sovereignty must be a criterion when deciding on the use of – initially inexpensive – cloud solutions.

In their joint policy paper, the federal, state and local governments agreed on the goal of strengthening the digital sovereignty of public administration IT, along with five action areas to achieve this goal:

1. strategic analysis of dependencies and comparable projects
2. design of strategic solutions
3. decision-making and support for implementation
4. coordination and agreement among the federal, state and local levels
5. dialogue with experts

[2] "Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung; Eckpunkte – Ziel und Handlungsfelder (Strengthening the digital sovereignty of public administration – objective and action areas).

[3] See Decision 2020/07 of the 31st meeting of the IT Planning Council: Cloud computing and digital sovereignty.

[4] See the European recovery plan Next Generation EU, European Commission, July 2020.

[5] See the programme for Germany's Presidency of the Council of the European Union, published by the Federal Foreign Office, July 2020.

[6] Government declaration by Federal Chancellor Angela Merkel, 18 June 2020.

The present strategy paper builds on the policy paper by describing strategic objectives more precisely and developing approaches and measures based on the action areas given in the policy paper.

2 Delimitation and categorisation

Today, digital technologies and solutions are an integral part of daily life and decision-making for many individuals and institutions, including public administration (at federal, state and local level) and society (individuals) as well as business and industry. Digital solutions are relevant for all areas of the executive branch, in particular IT for public administration, internal security, defence,[7] foreign policy,[8] mobility and transport,[9] climate policy, and public health. Digital solutions can be divided into individual technical components (for example, software, hardware, infrastructure, platforms and specialised applications) which together make up the technology landscape. Depending on the actor, policy area and technical components, different capabilities, information and options are needed to strengthen digital sovereignty.

The present strategy focuses on **public administration IT**. This area encompasses all digital solutions needed for operations and individual workstations. In the medium and long term, it is essential to examine the entire technology landscape[10] iteratively for critical dependencies,[11] to identify appropriate options for action and to initiate measures. Technology trends which are highly relevant for public administration IT, such as big data, artificial intelligence and blockchain, must continue to be taken into account.[12]

As the policy paper describes, the public administration plays different roles: *"The federal, state and local governments have set themselves the goal of working together to continually strengthen digital sovereignty in the public administration in its roles as user, provider and contracting authority."* To address all three roles, digital solutions must be viewed in the context of their value-added chains and services (sovereignty dimensions [13]).

These dimensions describe digital sovereignty in its entirety and offer orientation for the subsequent development of the public administration's strategic objectives.

[7] See for example https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710 (in German); with regard to digital sovereignty, see also the policy paper "Ausbau der digitalen Souveränität im Geschäftsbereich BMVg" (Increasing digital sovereignty within the remit of the Federal Ministry of Defence), Federal Ministry of Defence, Directorate-General Cyber/Information Technology.

[8] See for example https://www.auswaertiges-amt.de/de/newsroom/maas-zeit/2284728

[9] See for example https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html

[10] In the context of the present paper, technologies include both software and hardware.

[11] Taking note of existing projects, such as the Federal Government's framework programme for research and innovation, 2021–2024 on microelectronics, Federal Ministry of Education and Research, 2020.

[12] Taking note of the various public administration strategy papers, such as the "Datenstrategie des Bundes" (Federal data strategy), "Strategie Künstliche Intelligenz der Bundesregierung" (Federal Government strategy on artificial intelligence) and "Blockchain-Strategie der Bundesregierung" (Federal Government strategy on blockchain), as well as similar strategies of state and local governments.

[13] See "Digitale Souveränität als strategische Autonomie – Umgang mit Abhängigkeiten im digitalen Staat" (Digital sovereignty as strategic autonomy: Dealing with dependencies in the digital state), Competence Centre for Public IT and Fraunhofer Institute for Open Communication Systems FOKUS, 2020.

Overview of the sovereignty dimensions

User sovereignty (user[14]): This dimension describes access to capabilities and resources to be able to use digital technologies successfully, efficiently and with (legal) certainty in line with own institutional requirements. To do so, the user must be able to choose IT solutions freely from a selection of effective alternatives. The selection makes it possible to switch to alternative solutions in order to meet new user requirements or if new negative consequences of dependence on technology vendors further limit use. The institution utilising an IT solution ("user") is the controller as defined in data protection law. Users must therefore be able to adjust the necessary settings of centrally procured or operated components in particular, such as hardware, software and services, to ensure that processes operate in compliance with the law. The targeted development of user skills is equally necessary to be able to operate alternative digital solutions successfully.

Research, development, product and operational sovereignty (provider[15]): These dimensions describe the freedom to make decisions and the necessary resources and knowledge to address and promote research topics, the design and realisation of a product, the development or revision of software, and the creation and operation of safe, trustworthy and resilient digital systems. The provider must be able to develop, launch and operate own IT solutions independently. The provider must be capable of communicating with manufacturers in the market to participate appropriately in designing solutions (including to ensure data protection and information security). Privacy by design and by default must be an integral part of services and products involved in processing personal data.

Knowledge and transparency sovereignty (contracting authority[16]): These dimensions describe free access to information and knowledge about technologies as well as the ability and possibility to evaluate resources, systems, components and facts. When ordering digital solutions, contracting authorities must be able to choose from multiple competitive vendors and to influence the design of market offerings. Contracting authorities must also be able to hold technology vendors to a binding framework for digital sovereignty (including information security and data protection) when ordering, developing, launching or operating IT solutions.

[14] "User" refers to the institution utilising the IT solution, not the end user; the user is responsible for the operation of IT solutions to support the work of the government agency; users are for example IT departments of government agencies.

[15] "Providers" are responsible for developing, launching and operating IT solutions; for example, they are IT service providers in the public administration.

[16] "Contracting authorities" are responsible for ordering and acquiring new IT solutions; for example, they are the IT service providers and procurement offices of the public administration.

3 Strategy

In the present document, **strategic objectives** (Section 3.1) will first be identified based on the roles of the public administration and on the sovereignty dimensions (see Section 2). Next, **approaches** for achieving these objectives will be described (Section 3.2). These strategic objectives and approaches should be compared to the existing IT objectives[17] and objectives of existing IT programmes.[18] The objectives and approaches described here apply the current IT security standards.

3.1 Strategic objectives

For the public administration to be able to play its three roles as user, provider and contracting authority, three strategic objectives are being pursued.

I. **Ability to choose and switch:** the public administration is able to choose freely among IT solutions, components and vendors and switch flexibly between them. This means that effective and tested alternatives are available, allowing the public administration to switch to alternative products at short notice.[19] IT architecture, procurement methods and staff training must be designed in a way that enables such changes to be made at reasonable cost and with an appropriate amount of effort.

II. **Design capability:** the public administration has the capability to design its own IT or to participate in the design process. The public administration has the necessary skills and structures for working (cooperatively) to understand and assess IT solutions and to operate and develop them (further) as needed.[20]

III. **Influence on vendors:** the public administration can articulate its requirements and needs (for example with regard to product features, negotiation and contract terms) and have them met by technology vendors. In addition to legal requirements and conditions, this includes the option of IT operations in public administration data centres, compliance with guidelines on information security and privacy, and influence on licence models and the product roadmap.

[17] Along with the strategic objectives to strengthen digital sovereignty, existing objectives for federal and state IT are taken into account (objectives defined in the IT strategy of the federal administration for 2017–2021 and objectives defined in the IT Planning Council's National E-Government Strategy).

[18] For example the standardisation and consolidation efforts at federal, state and local level.

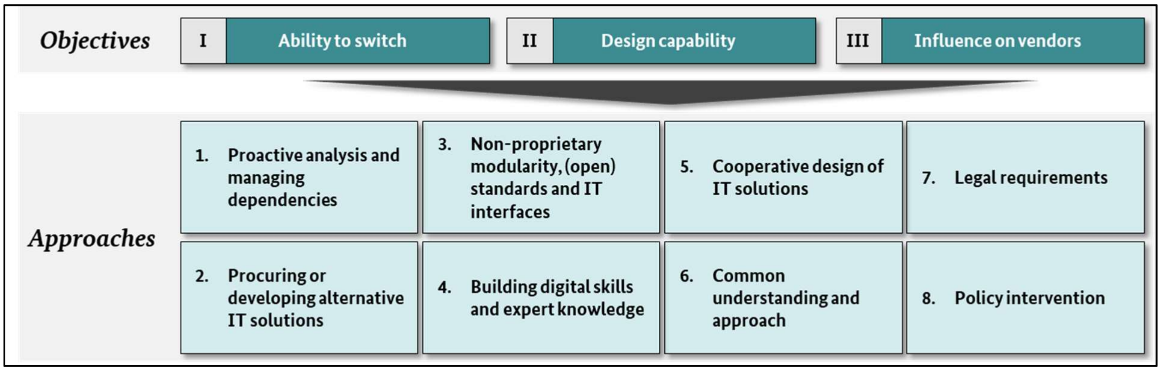
[19] To pursue such a dual-vendor strategy, it is necessary to promote competition and to create a framework in which as many vendors as possible can operate.

[20] The necessary added value for the public administration should be determined for each technical component (for example based on criteria such as relevance, cost-effectiveness and specificity).

These three strategic objectives make up a comprehensive approach to strengthening digital sovereignty (**hybrid strategy**). For example, depending on the situation, switching to a different vendor or product, designing or helping to design alternative products, commissioning a vendor, or some combination thereof may be the most effective way to manage dependencies.[21]

3.2 Approaches

Several approaches for achieving the strategic objectives have been identified (see Figure 2). They are based on the approaches from the policy paper action areas and will be expanded and described in more detail in the following. The annex to Section 6.1 illustrates how the approaches are derived from the action areas. The specific measures associated with the approaches are described in Section 4.



Objectives

I Ability to switch

II Design capability

III Influence on vendors

Approaches

1. Proactive analysis and managing dependencies
2. Procuring or developing alternative IT solutions
3. Non-proprietary modularity, (open) standards and IT interfaces
4. Building digital skills and expert knowledge
5. Cooperative design of IT solutions
6. Common understanding and approach
7. Legal requirements
8. Policy intervention

Figure 2: Approaches for achieving the strategic objectives

How each approach helps to achieve the strategic objectives is described below.

1. **Proactive analysis and managing dependencies**

Contribution:

- Early identification and analysis of critical dependencies and lock-in effects[22] in the technology landscape.
- Creating transparency concerning measures taken to reduce dependencies.

Approach: To start with, a survey is conducted of the existing technology landscape and IT trends (e.g. cloud computing, big data, internet of things, artificial intelligence). The subjects of analysis are next ranked by priority (e.g. selected vendors, parts of the technology stack or specific technologies), followed by a thorough analysis of the negative consequences of dependencies. This analysis

[21] In the process, the public administration or the relevant federal, state or local administration should seek as much conformity with standardisation and consolidation efforts as possible.

[22] "Lock-in effect" refers to a situation in which the resulting expense and other barriers make it difficult for customers to switch to other products, services or vendors.

	includes a description of the public administration’s desired objectives and possible options for action. Progress towards achieving these objectives is transparently monitored in order to ensure that measures to reduce dependencies are effective.
2. Procuring or developing alternative IT solutions	**Contribution:** • Creating efficient (in particular open source) IT solutions to meet actual needs and increase diversification. • Supporting the ability to choose and switch flexibly among IT solutions. **Approach:** Alternative IT solutions are identified, procured and used in the public administration. Necessary alternatives are developed as needed, with attention to the desired architectural principles such as modularity, open standards and interfaces (see Approach 3). Attention must also be paid to factors for success (e.g. alternatives are user-centred to ensure user acceptance, performance and availability of data). There is a focus on greater use of open source software (OSS), i.e. software that is open and, depending on the licence chosen, free from technical or legal restrictions on usability. OSS encourages freedom of choice, reusability of code and solutions, flexible modification of solutions, and transparency of modifications to source code. [23], [24],[25] The source code must be available in an understandable form[26] so that the public administration can issue new invitations to tender for support and the further development of the code.
3. Non-proprietary modularity, (open) standards	**Contribution:** • Reducing barriers to switching between IT solutions, components and vendors • Promoting reusability of solutions and components

[23] See the decision of the IT Planning Council (special meeting of 18 September 2020) on investing in the implementation of the Online Access Act (*Onlinezugangsgesetz*) according to the principle of open standards and open source, among other things.

[24] See “Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen” (Creating digital sovereignty for the public administration – improving the protection of personal data), resolution of the Conference of the Independent Data Protection Authorities of the Federation and the Federal States, 22 September 2020.

[25] See Open Source Software Strategy 2020–2023, European Commission, October 2020.

[26] The source code must be documented and structured in a way that third parties can understand and further develop it and that makes it possible to compile the possible software from the source code provided.

and interfaces in IT	• Reducing barriers to entry for vendors **Approach:** Modular and non-proprietary IT architectures are defined and established for all levels of public administration, along with open and free standards, interfaces and open file formats. These principles must be followed in the medium and long term, in particular when developing IT solutions for IT projects within the public administration (e.g. the implementation of the Online Access Act and consolidation projects).[27] In the medium and long term, it is also necessary to decouple specialised IT applications from the client while ensuring that they can still be integrated within the same administrative processing platform (process platform approach). Further, active participation in national (e.g. XÖV), European and international standardisation efforts is desired.
4. Building digital skills and expert knowledge	**Contribution:** • Independent evaluation of IT solutions • If necessary, (further) development/operation of solutions • Transfer of knowledge and experience from similar projects in public administration, private industry and academia **Approach:** (IT) expert knowledge and skills are built up and shared. A clear division of tasks is maintained, e.g. in software development, procurement and operations as well as in subject areas and requirements management. (Inter-)national exchange with public and private interest groups is fostered at all levels of public administration, also at EU level, e.g. to identify and learn from similar projects.
5. Cooperative design of IT solutions	**Contribution:** • Participating in the design of IT solutions by working with various vendors and (inter-)national actors • Making the technology market aware of the needs and requirements of the public administration **Approach:** Cooperation within public administration IT is intensified at national and European level to produce interoperable solutions across national borders. Cooperation between sectors should be intensified as well in order to

[27] In future standardisation and consolidation projects and programmes for reusing solutions, digital sovereignty must be taken into account as one dimension in the process of making decisions on suitable partners and technology vendors. Appropriate criteria should be drawn up and agreed on.

	increase the diversity of what vendors have to offer. This encompasses in particular greater cooperation with OSS communities, OSS vendors, proprietary vendors and small and medium-sized enterprises (SMEs). Accessible source code and OSS licences suitable for reuse and joint (further) development encourage participation in the design of IT solutions.[28]
6. Common understanding and approach	**Contribution:** • Strengthening the position of the public administration in its negotiations with technology vendors • Avoiding redundancies and additional effort while taking advantage of synergies in the public administration • Agreeing on a common strategy for strengthening the digital sovereignty of the public administration **Approach:** The public administration at federal, state and local level regularly defines and agrees on common objectives and approaches. This includes coordinating procurement and defining negotiating strategies as needed while keeping markets open, also for SMEs. Policy-makers and public administration staff are aware of the need to strengthen digital sovereignty and of the critical nature of unwanted dependencies.
7. Legal requirements	**Contribution:** • Positioning and ensuring that technology vendors meet the public administration's core requirements • Clearly defining a space for action and legal certainty for vendors and the public administration[29] **Approach:** Requirements are specified in the form of clear legal and regulatory provisions, e.g. for the development, procurement, use and operation of IT solutions. The requirements of digital sovereignty are taken into account in procurement, the wording and awarding of contracts, and operations. The protection of the public administration's intellectual property must be ensured at the same time. It is necessary to check that the necessary principles for strengthening digital sovereignty are enshrined in procurement law and whether preference for OSS can be enshrined in the law if the OSS offers the same functions

[28] See Open Source Software Strategy 2020–2023, European Commission, October 2020.

[29] Note: if technology vendors currently do not meet the public administration's core requirements but agree to do so by a certain date, then it is possible in principle to award a contract.

	and is as cost-effective as proprietary solutions. With regard to operations, a key feature of digital sovereignty is the option of on-premises operation in public administration data centres.
8. Policy intervention	**Contribution:** • Positioning the objectives concerning digital sovereignty within national and European digital policy • Establishing a policy framework to strengthen digital sovereignty at national and European level **Approach:** The objective of strengthening digital sovereignty has priority on the public administration's policy agendas and in the Federal Government's coalition agreements. The necessary funds and resources are made available (e.g. by means of specific funding programmes). The EU is an active strategic partner that has the same values and shared governance mechanisms.

4 Implementation

The approaches are implemented using various measures (see Section 4.1). The list of measures presented here is **not exhaustive**. Cooperation between the federal, state and local levels is described in Section 8.

4.1 Measures to implement the approaches

The initial overview of measures offers a frame of reference for the *working group on cloud computing and digital sovereignty* and its subgroups. This overview is regularly updated jointly. The findings of the strategic market analyses in future can help in further developing the measures. As a matter of great urgency, the Federal Ministry of the Interior, Building and Community commissioned an initial market analysis of software vendors[30] in 2019. Measures, such as proof of concept, OSS alternatives and negotiations in line with defined requirements for vendors, were initiated based on the findings of that analysis. Further analyses will be carried out in future on the basis of the comprehensive overview of the technology landscape and the priority of the subjects of analysis.

Public administration at federal, state and local level can take part in drafting the measures and suggest additional measures via the subgroups. Figure 3 provides an overview of the measures derived from the approaches. The working group and subgroups regularly update the details of the measures (e.g. actors, milestones) in separate brief descriptions.

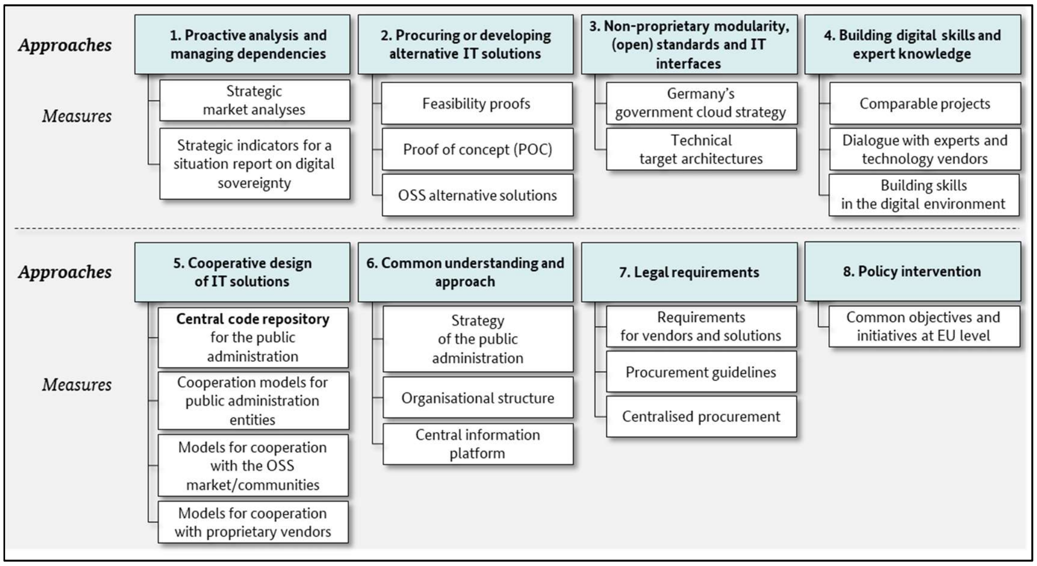

Approaches
Measures
1. Proactive analysis and managing dependencies
Strategic market analyses
Strategic indicators for a situation report on digital sovereignty
2. Procuring or developing alternative IT solutions
Feasibility proofs
Proof of concept (POC)
OSS alternative solutions
3. Non-proprietary modularity, (open) standards and IT interfaces
Germany's government cloud strategy
Technical target architectures
4. Building digital skills and expert knowledge
Comparable projects
Dialogue with experts and technology vendors
Building skills in the digital environment
Approaches
Measures
5. Cooperative design of IT solutions
Central code repository for the public administration
Cooperation models for public administration entities
Models for cooperation with the OSS market/communities
Models for cooperation with proprietary vendors
6. Common understanding and approach
Strategy of the public administration
Organisational structure
Central information platform
7. Legal requirements
Requirements for vendors and solutions
Procurement guidelines
Centralised procurement
8. Policy intervention
Common objectives and initiatives at EU level

Figure 3: Measures to implement the approaches

The latest measures for each approach are described in the following.

1. Proactive analysis and managing dependencies

[30] See "Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern" (Strategic market analysis to reduce dependency on individual software vendors), PwC Strategy& GmbH, 2019.

- **Conducting strategic market analyses to reduce dependencies:** the initial *strategic market analysis to reduce dependency on individual software vendors* examines the negative consequences of dependencies in the area of software and identifies possible options for action. A market analysis in the area of databases is currently being conducted.
- **Formulating strategic indicators for a situation report on digital sovereignty:** strategic indicators are defined to measure progress and the effectiveness of the project to strengthen digital sovereignty. Data are used to prepare a comprehensive overview of the public administration's technology landscape, including information on dependencies, vulnerabilities and current measures to remedy them. This overview of the technology landscape is the foundation for determining the priority of further subjects of more detailed analysis. The organisation affected can formulate operational (SMARTe) objectives on this basis and keep track of how they are being achieved.

2. Procuring or developing alternative IT solutions

- **Updating the overview of feasibility proofs[31] in the public administration:** existing alternatives (preferably OSS-based) are identified and the overview is kept up to date in the form of a "map" of feasibility proofs.[32] This map contains critical success factors from projects with alternative IT solutions and an overview of areas in which the public administration has gained experience. The map is intended to make it easier to put alternative solutions to work at federal, state and local level.
- **Conducting proof of concept (POC):** the feasibility of alternative IT solutions is tested in POC projects to meet existing needs. This will test in particular those solutions which do not yet have proof of feasibility in the public administration. The first POC projects have already been launched, e.g. in the area of collaboration platforms.
- **Promoting OSS alternative solutions:** the availability of efficient and scalable open source alternatives is secured and the use of OSS in the public administration is increased. Institutional support for OSS solutions enables, among other things, better distribution of resources, more possibilities to switch and greater influence on the development of OSS in line with needs.

3. Non-proprietary modularity, (open) standards and interfaces in IT

- **Designing Germany's government cloud strategy – the federal approach:**[33] the modularity, compatibility and interoperability of cloud solutions is ensured in order to enable substitutions

[31] A feasibility proof is defined as proof of the technical and organisational feasibility of an alternative IT solution.

[32] The latest version, of August 2020, was published on 3 September 2020: https://www.cio.bund.de/SharedDocs/Kurzmeldungen/DE/2020/20200330_Machbarkeitsnachweise_download.pdf?__blob=publicationFile (in German)

[33] Adoption of Version 1.4.1 of 17 November 2020 on 23 October 2020 at the 33rd meeting of the IT Planning Council.

and reuse. To create such a federal cloud network, Germany's government cloud strategy defines non-proprietary, modular architectures as well as open standards and interfaces extending across all levels of public administration (e.g. in the area of containerisation) for developing, launching and running cloud applications while paying close attention to existing developments and activities.[34]

- **Defining additional technical target architectures:** additional target architectures are defined to reduce identified dependencies and avoid foreseeable ones, taking into account the requirements of the public administration (consulting the Coordination Office for IT Standards and paying attention to existing developments and activities as needed). A target architecture should be defined for each area of application. In the area of software, this architecture should ideally consist of OSS components and should be of interest to private industry as well, in order to take advantage of network effects.

4. Building digital skills and expert knowledge

- **Identifying and sharing information and experience gained from comparable (inter-)national projects:** knowledge transfer and experience-sharing with comparable projects, particularly in the EU, is ongoing and serves to identify success factors and best practices.
- **Dialogue with experts and technology vendors:** establishing suitable dialogue formats (such as a council of experts) enables ongoing identification of existing or foreseeable dependencies, possible solutions and potential challenges. Examples include dialogue with experts in academia, with non-governmental organisations in the field of open source, and with selected vendors.
- **Building skills in the digital environment:** the skills needed to understand, evaluate, investigate, develop, run or use technologies are improved and increased. Initial, advanced and continuing training in the public administration (e.g. training for skilled workers; courses of study) must be modified and/or expanded accordingly. For example, occupational profiles in the area of data and (agile) project management should be expanded, including possible improvements to pay and incentives in the public sector.

5. Cooperative design of IT solutions

- **Building a central code repository for the public administration:** standards from Germany's government cloud strategy are used to create a code repository. This includes planning and preparing the technical, organisational and legal measures which such a project entails (including the selection of a suitable sponsor).

[34] Such as the public sector domain in GAIA-X.

- **Designing models for cooperation among public administration entities:** organisational fundamentals for efficient and effective cooperation within the public administration when developing solutions are identified and assessed (e.g. along the lines of FITKO's FIT-Connect).
- **Designing models for cooperation with the OSS market/communities:** ways to involve the OSS market/communities to ensure effective solutions for the present and future (e.g. through funding programmes) are identified and assessed.
- **Designing models for cooperation with proprietary vendors:** ways to involve proprietary vendors to ensure effective solutions for the present and future while satisfying the requirements of the public administration (e.g. through ongoing dialogue with industry) are identified and assessed.

6. Common understanding and approach

- **Developing a strategy of the public administration:** the public administration at federal, state and local level continuously defines and agrees on common objectives and approaches. The present strategy sets out the strategic elements of the policy paper in greater detail.
- **Establishing the structure for the work of the cloud computing and digital sovereignty working group:** to formalise and promote cooperation between the federal, state and local levels, a structure was set up to organise the work of the working group on cloud computing and digital sovereignty by means of subject-focused subgroups. The subgroups present their results to the working group, which prepares proposals for decisions by the IT Planning Council as needed.
- **Setting up a central information platform:** a communications strategy is designed and content made available using an information platform to promote communication among actors, provide information and increase awareness of digital sovereignty.

7. Legal requirements

- **Formulating requirements for technology vendors and solutions:** overarching requirements for procuring information and communications technology by and/or for the public administration are defined. These requirements are intended to reduce dependencies on particular vendors by setting a framework for IT services and their providers for the public administration when developing and providing solutions.
- **Producing procurement guidelines:** further requirements, for example additions to the established templates for EVB-IT[35] contracts and an update of the UfAB,[36] are added to the specific requirements for digital sovereignty (such as those concerning support, service times and data protection) in the procurement process.
- **Examining possibilities for central procurement:** ways to procure alternative solutions centrally in the public administration are identified and secured. Methodology should also be developed for surveying and compiling the needs of the public administration at federal, state and local level.

8. Policy intervention

- **Coordinating common objectives and initiatives at EU level:** common objectives for strengthening digital sovereignty are adopted. Joint initiatives for cooperation at European level, with Germany serving as a model, are initiated. Proposals for joint initiatives include for example promoting open digital ecosystems, coordinating the implementation of EU legislation for public procurement, creating public-private partnerships in the fields of artificial intelligence, data and robotics,[37] and setting up an open source programme office.[38]

4.2 Governance

To implement the measures to strengthen digital sovereignty, the involvement of numerous actors at federal, state and local level is sought. The process began when the IT Planning Council set up its *working group on cloud computing and digital sovereignty*. The working group's subgroups[39] are responsible for elaborating the specific details. In doing so, they explicitly seek to share information with industry, private-sector experts and other key partners. The subgroups present their results to the working group, which then prepares

[35] EVB-IT: supplementary contract conditions for procuring IT services (*ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen*).

[36] UfAB: guidelines issued to public authorities for the procurement of IT products and services (*Unterlage für Ausschreibung und Bewertung von IT-Leistungen*).

[37] See "Digital sovereignty for Europe", European Parliament Research Service, July 2020.

[38] See Open Source Software Strategy 2020–2023, European Commission, October 2020.

[39] These are 1) the subgroup on technology and operations; 2) the subgroup on procurement; and 3) the subgroup on communication.

further recommendations for decisions by the IT Planning Council. The organisational details were defined in a paper on the *structure for the work of the cloud computing and digital sovereignty working group*. In its Decision 2020/31, the IT Planning Council asked the federal, state and local governments to actively participate in the subgroups within the defined organisational structure.

Effective cooperation within the public administration in Germany and with European Union member states, with industry and the research community is needed to achieve the desired objectives. In the next steps, the working group must examine the best way to ensure that the subject of digital sovereignty and its governance is firmly established in institutional terms, for example by means of a central sponsoring organisation or in decentral units.

5 Outlook

The strategic objectives and approaches sketched out here lay the groundwork for jointly and continuously strengthening digital sovereignty. On this basis, measures (see Section 4.1) are being drawn up and further developed. The working group and its subgroups provide further details on the measures in separate brief descriptions specifying the relevant actors and schedules for implementation, along with any binding deadlines needed for migration and to introduce the standards. New measures are also being developed, for example based on the results of the market study on databases.

Important next steps concerning concrete measures include the following:

1. drafting standards and target architectures based on Germany's government cloud strategy (decision of 23 October 2020 at the 33rd meeting of the IT Planning Council),
2. deciding in the IT Planning Council on requirements for technology vendors and solutions (tentatively planned for mid-2021),
3. planning a central coordinating office to promote OSS in the public administration. The first step is to determine where OSS is needed in the public administration and where it offers added value (in particular to reduce dependencies found in the market analysis to be critical with regard to work stations),
4. drawing an overall picture for strengthening digital sovereignty (see Section 4.1, Formulating strategic indicators for a situation report on digital sovereignty). In line with the digital policy dashboard,[40] such a situation report must provide a comprehensive overview of the technology landscape of public administration IT. The situation report is intended to aid in determining the priority of further subjects of more detailed analysis and in simplifying the systematic examination of the entire technology landscape. Further, the progress and effectiveness of measures to strengthen digital sovereignty must be transparent. The situation report should later be expanded to include an assessment of new technologies which may be relevant in future for public administration IT (e.g. data, artificial intelligence, blockchain). And further actors (e.g. in the field of education, industrial policy, defence policy, health and mobility) should be considered as well.

[40] See "Digitalisierung gestalten" (Designing the digital transformation), Federal Government, 2020 (https://www.digital-made-in.de/dmide, 2020)

6 Annex, list of figures and list of abbreviations

6.1 Approaches derived from the policy paper action areas

The concept of digital sovereignty is currently being discussed and advanced in various contexts. The different contributions to the discussion naturally focus on individual aspects of this very complex issue and emphasise different perspectives. These contributions should be seen as complementary; they also build on each other over time and develop different approaches further, while the central message remains the same.

The policy paper and the strategy presented here are intended as a general statement of policy and its further specification aimed at implementation. The areas of action referred to in the policy paper describe approaches for strengthening digital sovereignty. The present document expands and further differentiates these approaches and fleshes them out with measures (see Figure 4). The content has also developed further, and the areas of action have been subsumed under newly formulated or more precise strategic objectives.

Action area 1 has been expanded to include not only the analysis of dependencies, but also their management (see Section 4.1, Formulating strategic indicators for a situation report on digital sovereignty). In line with the pursuit of a hybrid strategy, various technical, organisational and legal approaches to reduce critical dependencies and/or strengthen digital sovereignty at every level are specified in the design of strategic solutions (action area 2). The measures are mostly divided between a conceptual part (action area 2) and a part focused on deciding on the deployment of the solutions and strategies that have been developed and of support for implementation (action area 3). Action area 4 has been expanded to include not only ongoing coordination between the federal, state and local levels, but also the political positioning of the issue of digital sovereignty at national and European level. Action area 5 has been expanded to include not only dialogue with experts, but also continuing improvement of skills.

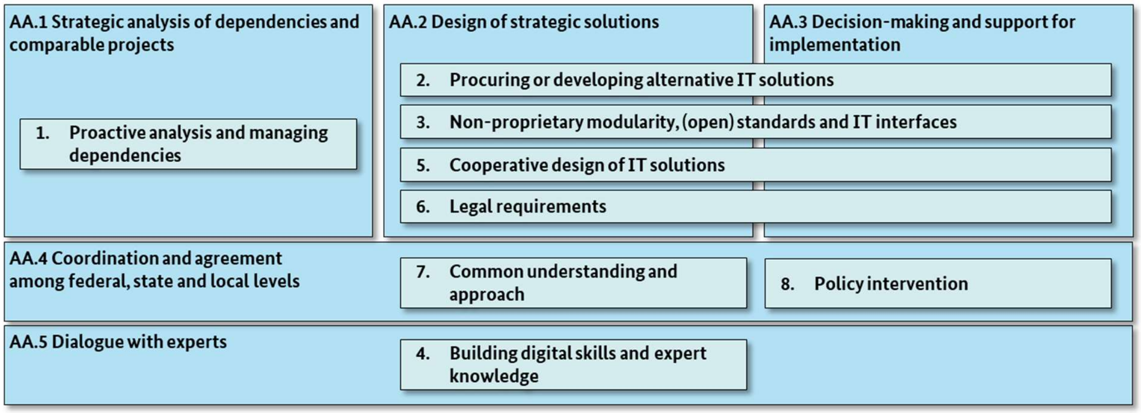

AA.1 Strategic analysis of dependencies and comparable projects
1. Proactive analysis and managing dependencies
AA.2 Design of strategic solutions
AA.3 Decision-making and support for implementation
2. Procuring or developing alternative IT solutions
3. Non-proprietary modularity, (open) standards and IT interfaces
5. Cooperative design of IT solutions
6. Legal requirements
AA.4 Coordination and agreement among federal, state and local levels
7. Common understanding and approach
8. Policy intervention
AA.5 Dialogue with experts
4. Building digital skills and expert knowledge

Figure 4: Approaches derived from the policy paper action areas

6.2 List of figures

6.3 List of abbreviations

German abbreviation	English equivalent
EU	European Union
EVB-IT	supplementary contract conditions for procuring IT services
FITKO	body for federal IT cooperation
IT	information technology
OSS	open source software
POC	proof of concept (feasibility study)
UfAB	guidelines issued to public authorities for the procurement of IT products and services