IT-Planungsrat

Germany's government cloud strategy: target architecture framework

- Version 2.5.5 of 9 October 2023 -

10/2023

Publication data

Published by
The Working Group on Cloud Computing and Digital Sovereignty
of the IT Planning Council

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

Version of
October 2023

Table of contents

1 Introduction

The concept paper on *Germany's Government Cloud Strategy: The Federal Approach* was agreed on by the IT Planning Council (*IT-Planungsrat*, IT-PLR) at its 33rd Meeting (Decision 2020/54).[1] It forms part of the adopted strategy for strengthening the digital sovereignty of public administration IT;[2] more specifically, it falls under the heading of the following approach, which is defined in this strategy: "*Vendor-independent modularity, (open) standards and interfaces in IT*". In this context, digital sovereignty is defined as "*the abilities and opportunities of individuals and institutions to perform their role(s) in the digital world in an independent, self-determined and secure fashion*".[3]

Germany's government cloud strategy, which was adopted by the IT Planning Council in October 2020, is intended to introduce common standards and open interfaces for public administration cloud solutions as a means of establishing an interoperable and modular federal cloud infrastructure across the board.

The market continues to evolve towards an increased use of cloud solutions; at the same time, a large number of cloud solutions already exist within the federal administrative levels of the Federal Government, federal states and municipalities. Yet a lack of standardisation within the individual cloud architecture layers means that the existing federal cloud solutions are only interoperable and compatible to a limited extent, if at all. The primary goal of Germany's government cloud is to provide the option of using cloud services and software solutions on a multi-cloud or multi-location and reciprocal basis; a further goal is to reduce critical dependencies on individual vendors through its standardised, modular IT architectures.

In its Decision 2020/54, the IT Planning Council tasked the Working Group on Cloud Computing and Digital Sovereignty with developing the target architecture of Germany's government cloud. Based on the IT Planning Council's Decision, the Working Group on Cloud Computing and Digital Sovereignty entrusted the Sub-Working Group on Technology and Operations with the tasks of

---

[1] See IT Planning Council, Decision 2020/54 – Working Group on Cloud Computing and Digital Sovereignty https://www.it-planungsrat.de/beschluss/beschluss-2020-54

[2] See IT Planning Council, Decision 2021/09 – Working Group on Cloud Computing and Digital Sovereignty https://www.it-planungsrat.de/beschluss/beschluss-2021-09

[3] Definition taken from a study on "Digital sovereignty" carried out by the Competence Centre for Public IT (*Kompetenzstelle Öffentliche IT*, ÖFIT).

technical design and operationalisation. Service providers of public administration IT account for a large portion of the membership of this Sub-Working Group, and the proximity to practice achieved in this way provides an ongoing guarantee of technical feasibility in parallel to conceptual design.

In line with the standardisation areas and requirements set out in the concept paper on Germany's government cloud strategy,[4] the Sub-Working Group is split into areas of action[5] (see Chapter 1.3).

Operative objectives were formulated for each area of action and use cases were then highlighted as a means of defining the requirements to be met by the architecture. Based on these, the required system or basic structure of Germany's government cloud was identified[6] and the target architecture described in this document was specified.

1.1 Notes on the first update

Version 1.0 of the target architecture framework was adopted by the IT Planning Council at its 36th Meeting.[7] The IT Planning Council also tasked the Working Group on Cloud Computing and Digital Sovereignty with producing a detailed conceptual design of the cloud service portal and the coordination body for Germany's government cloud, evaluating the reuse of existing public administration structures for the coordination body, performing additional PoCs, further developing the standards for Germany's government cloud, and updating the target architecture framework on a regular basis.

The first update of the framework (Version 2.0) fulfils the latter of these tasks. The framework has been supplemented and updated to include a wide range of extra information reflecting the

[4] In the remainder of this document, the term "concept paper" is used to refer to Decision 2020/54 by the IT Planning Council, see https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-54_Deutsche_Verwaltungscloud_Strategie.pdf

[5] Areas of action 1 and 4 as well as 5 and 7 were combined due to the significant overlaps that have emerged over time between the topics covered.

[6] In the remainder of this document, the term "Germany's government cloud" is used to refer to the standardised, federal cloud infrastructure of the Federal Government, federal states and municipalities in the context of the government cloud strategy adopted by Germany.

[7] IT Planning Council, Decision 2021/46 of 29 October 2021, see https://www.it-planungsrat.de/beschluss/beschluss-2021-46

progress made with the conceptual design to date. In particular, substantive alterations have been made in the following areas:

- **Key standards:** existing standards have been supplemented (see Chapter 5.4.4 Container environment and container clusters, Chapter 5.4.5 Development area) and new standards added (see Chapter 5.4.3 Network connection, Chapter 5.4.6 Communication between the cloud location, software operator and cloud service portal).
- **Methodology underlying Germany's government cloud:** the roles specified for Germany's government cloud have been explained in further detail on the basis of possible usage scenarios (see Chapter 4).
- **Next steps and operationalisation of Germany's government cloud:** this section has been comprehensively updated to reflect the latest developments in relation to the coordination body and the piloting of Germany's government cloud at the time of the update.

A key module has furthermore been integrated into the methodology of Germany's government cloud following the start of productive operation of the public administration's OS platform, Open CoDE.[8] References to Open CoDE have been added at the appropriate points.

1.2 Notes on the second update

Version 2.0 of the target architecture framework was adopted by the IT Planning Council at its 39th Meeting.[9]

The update of the framework in Version 2.5 outlined in this document corresponds to the commissioning of the Working Group on Cloud Computing and Digital Sovereignty agreed by the IT Planning Council in its 36th meeting to further develop the standard for Germany's government cloud and to update the target architecture framework on a regular basis.

The framework has been supplemented and updated to include a wide range of extra information reflecting the progress made with the conceptual design to date. In particular, substantive alterations have been made in the following areas:

[8] See https://www.opencode.de

[9] IT Planning Council, Decision 2022/47 of 10 November 2022, see https://www.it-planungsrat.de/beschluss/beschluss-2022-47

- **Summary of results of the minimum viable product (MVP):** as part of the MVP, the ongoing work, designs and reflections of the Working Group on Cloud Computing and Digital Sovereignty in regard to the coordination body as a central module of the government cloud project as a whole were tested in practice and further developed (see Chapter 1.4).
- **Concept of the implementation project for Germany's government cloud:** it was noted in the minutes of the 41st meeting of the IT Planning Council that the implementation of Germany's government cloud strategy was to begin. Chapter 6.3 provides an overview of the project.
- **Motivation for and presentation of the maturity model:** it was ascertained during implementation of the MVP project that the standards for Germany's government cloud defined in Version 2.0 of the framework are not sufficient on a standalone basis to use as guidelines for creating and operating services for Germany's government cloud. The cloud service maturity model was therefore developed (see Chapter 5.1).
- **More precise definition of the role of the cloud integrator:** the current applicable definition of the role of the cloud integrator was provided in Chapter 4.3.

The decision to publish Version 2.5 rather than Version 3.0 of the document is based on the fact that the introduction of the maturity model and the associated replacement of the current standards for Germany's government cloud are to be tested and optimised in the implementation project.

1.3 Areas of action for the Sub-Working Group

The five areas of action listed in the concept paper on Germany's government cloud strategy[10] were expanded to seven in the first update, and have been further expanded to eight in the current second update of the framework.

The names of the areas of action have been expanded and refined in this document in view of the implementation project for Germany's government cloud that is to be adopted in July (see Chapter 6.3).

[10] See https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-54_Deutsche_Verwaltungscloud_Strategie.pdf

- Area of action 1 “Platform operators and cloud locations”
- Area of action 2 “Information security and data protection”
- Area of action 3 “Cloud service portal ecosystem”
- Area of action 5 “Software operators and software vendors”
- Area of action 6 “Operating model, governance and control”
- Area of action 8 “Proof of concept”
- Area of action 9 “Cloud integrator – integration of external cloud providers”
- Area of action 10 “Identity and access management”

1.4 Germany’s government cloud: minimum viable product

In October 2022, with the participation of the Working Group on Cloud Computing and Digital Sovereignty, the Federal Ministry of the Interior and Community commissioned govdigital to carry out a minimum viable product project. The goal of this project was to test in practice and further develop the ongoing work, designs and reflections of the Working Group on Cloud Computing and Digital Sovereignty in regard to the coordination body as a central building block of the government cloud project as a whole, to evaluate the level of maturity of the concepts for Germany’s government cloud, and to prepare and speed up the subsequent full implementation of the government cloud. The MVP project was successfully completed in February 2023. As part of the project, initial functional versions of the cloud service portal and of a distributed identity and access management infrastructure (IAM infrastructure) were established. Both components (cloud service portal and IAM) were successfully tested in January 2023. Since then, registered cloud service customers[11] have been able to book selected services from cloud service providers[12] using the cloud service portal. The cloud service portal for Germany’s government cloud has been available online since that time at **https://deutsche-verwaltungscloud.de/**.

[11] “The cloud service customer procures services from Germany’s government cloud via a cloud service broker or directly from a cloud service provider. It may be an authority, an entity within the public administration or an IT service provider within the public administration.” [Germany’s government cloud strategy: target architecture framework; Version 2.0.1, of 10 October 2022].

[12] “The cloud service provider offers a service within Germany’s government cloud and is responsible for providing the service. Within Germany’s government cloud, this role is an umbrella term for platform operator, software operator or cloud integrator.” [Germany’s government cloud strategy: target architecture framework; Version 2.0.1, of 10 October 2022].

The results of the testing of the cloud service portal provide an important foundation for planning and carrying out the implementation project. Based on the cloud service portal, which has already been developed, sample contracts and general terms and conditions for the use of the services available on the cloud service portal are also available for further use.

In regard to user requirements and expectations of stakeholders, the findings from the MVP are to be reused in the implementation project.

2 Objectives and framework conditions

This chapter describes the basic objectives and framework conditions for the target architecture outlined in this document. Points covered in particular detail include the target group and the difference between this area of work and related projects and other relevant specifications within the public administration.

2.1 Objective and structure of the concept

This document outlines the target architecture of Germany's government cloud and corresponds to the following task assigned by the IT Planning Council:

> "*The IT Planning Council entrusts the Working Group on Cloud Computing and Digital Sovereignty with the task of developing a target architecture on the basis of the defined standardisation areas and the requirements, and of reporting to the IT Planning Council at its 34th Meeting on progress made*." (Decision 2020/54 by the IT Planning Council)

The objective of the document is to define common standards for the public administration's federal cloud infrastructure and its locations. The specification of Germany's government cloud, building on the concept paper that has already been adopted, will serve as a basis for the ongoing implementation of Germany's government cloud (see Chapter 5.5). The standards defined in Chapter 5 and the detailed standards to be published (see Chapter 2.4) further the goal set in the policy paper[13] and strategy paper[14] of achieving an open, modular and interoperable IT architecture for the public administration. Similarly, the creation of federal cloud structures for the Federal Government, federal states and municipalities forms a core element of the Nine-Point Plan adopted by the Federal Government Commissioner for Information Technology.[15]

The focus of this target architecture framework and the pilot projects based on it (see Chapter 6.2), of the MVP (see Chapter 1.4) and of the implementation project for Germany's government cloud (see Chapter 6.3) is the laying of a foundation for the standardised operation of existing and future

---

[13] See https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-19_Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf

[14] See https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf

[15] See https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/DE/9-punkte-plan.pdf?__blob=publicationFile&v=4

cloud services and software solutions in order to establish or simplify the option to switch software solutions and vendors or operating environments. The further development of Germany's government cloud, e.g. the conceptual design of the coordination body and the development of the cloud service portal (see Chapters 6.1 and 5.5), will take place in stages.

The requirements and specifications that apply to cloud services and software solutions in the context of the procurement process fall outside the scope of this document, and will be addressed separately by the Sub-Working Group on Procurement acting under the auspices of the Working Group on Cloud Computing and Digital Sovereignty (see the Requirements that apply to technology vendors and solutions with a view to strengthening digital sovereignty in Chapter 2.3.2). The provision of software as a service (SaaS) is analogous to the operation and provision of individual software solutions by software operators (see Chapter 4.4).

The content of this document (other than the introductory Chapter 1) is structured as follows:

- **Chapter 2** "Objectives and framework conditions" describes the objectives of Germany's government cloud architecture, the scope and target group, the difference between this area of work and other specifications and projects, and the ongoing future development of this document.
- **Chapter 3** "Added value for the public administration and its IT infrastructure" highlights the multi-faceted added value that might be leveraged by Germany's government cloud.
- **Chapter 4** "Methodology underlying Germany's government cloud" explains the basic elements of Germany's government cloud and the relevant roles, as well as usage scenarios.
- **Chapter 5** "Key standards" defines obligatory and optional standards for Germany's government cloud and specifies selected standards with further explanations.
- **Chapter 6** "Next steps and operationalisation of Germany's government cloud" describes the recommended future actions to be taken in relation to the set-up of Germany's government cloud, outlines additional lines of action for the ongoing specification of Germany's government cloud, and provides an explanation of the coordination body for Germany's government cloud.

2.2 Scope and target group

The adoption of Decision 2021/46 by the IT Planning Council ensured the across-the-board application of the architecture of Germany's government cloud and the corresponding standards to the Federal Government, federal states and municipalities and their IT service providers.

In the context of Germany's government cloud, standardisation is targeted especially at the public administration's existing and future federal cloud infrastructure, in particular the IT service providers involved. For the public administration and its IT service providers, participation in Germany's government cloud entails mandatory implementation of standards.

Deviations from the specified standards will be permitted only in justified exceptional cases and will require documented justification and a time restriction. Approval is to be granted by the architecture board (which is yet to be established) and the coordination body (see Chapter 6.1).[16]

2.3 Clarification

The standards specified in connection with Germany's government cloud are embedded in existing specifications and guidelines for IT solutions at various federal levels. At the same time, the government cloud implementation project must be clearly differentiated from other initiatives in the area of cloud computing, and potential overlaps must be identified. Explanations of related projects and relevant public administration specifications are therefore provided below, in each case with an indication of the extent to which Germany's government cloud differs from or builds on and uses the project or specification.

In summary, Germany's government cloud implements specifications that apply to the public administration (with particular regard to existing standards, e.g. requirements in the fields of information security, data protection and confidentiality), and takes the latest developments in the area of cloud computing as a basis for modernisation of the public administration's IT infrastructure.

[16] The reuse of existing federal structures will be examined at the detailed design stage. For example, it would be possible, in principle, to work towards integration into the federal IT Architecture Board already set up by the IT Planning Council (see https://www.fitko.de/foederale-koordination/gremienarbeit/foederales-it-architekturboard).

2.3.1 Related projects

The following projects cover issues of relevance to the public administration and focus on cloud computing; as such, they were taken into consideration when designing the target architecture:

- **Cloud solutions operated by the Federal Government, federal states and municipalities (e.g. the federal cloud (*Bundescloud*)):** as noted in Chapter 1, various cloud solutions already exist (provision of the service models "infrastructure as a service" (IaaS); "platform as a service" (PaaS) including "container as a service" (CaaS); "software as a service" (SaaS)[17]) at the different administrative levels of the Federal Government, federal states and municipalities.
- **Gaia-X:**[18] the Gaia-X project is aimed at creating a usable federated European data infrastructure by establishing an interconnected system of existing cloud and service providers on the basis of uniform interfaces and standards (the "federation services"). The focus is primarily on shared values, i.e. data sovereignty, openness and interoperability. The introduction of this ecosystem in Europe will follow a stringently open source (OS) approach.
- **Sovereign cloud stack**[19] (SCS): the SCS project is aimed at developing a federatable and completely open software stack for cloud service providers as a way of allowing them to provide and operate a vendor-independent cloud infrastructure. Development work involves the use of tried-and-tested modular standard software components (e.g. Kubernetes) and the implementation of tools and processes for the automated operation of such environments. In this way, SCS supplies an infrastructure component for Gaia-X that can be used as a fully sovereign technical foundation.

---

[17] For basic explanations relating to the topic of cloud computing, see https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html

[18] See https://www.gaia-x.eu

[19] See https://scs.community/de

- **Implementation of the Online Access Act (*Onlinezugangsgesetz*, OZG):**[20] the Act to Improve Online Access to Administrative Services (Online Access Act) obliges the Federal Government and the federal states (and therefore also the municipalities) to offer their administrative services digitally by the end of 2022. "One for all" is a core principle guiding efforts to implement the Online Access Act and implies that solutions developed once by a federal state should be reusable by other states in order to share the responsibility for digitalisation efforts and save time.[21]

When participating in Germany's government cloud, existing public administration cloud solutions and the associated IT service providers must implement the standards defined for Germany's government cloud. Through the consistent implementation of the standards for Germany's government cloud, multi-faceted added value will be leveraged, which will also support implementation of the Online Access Act and the "one-for-all" principle in future (see Chapter 3). It is envisaged that the Online Access Act and Germany's government cloud will be coordinated in future. Implementation of the Online Access Act does not depend on the establishment of Germany's government cloud, however, and is regarded as a parallel line of action. Whereas the aim of the Online Access Act is the digitalisation of administrative services, Germany's government cloud is intended to make the public administration's IT infrastructure fit for the future. Germany's government cloud may, however, have a significant bolstering effect on implementation of the Online Access Act, for example if "one-for-all" services are developed and offered as (cloud) services that are compliant with Germany's government cloud, since it would, in this way, be possible for them to be implemented – for the most part without the need for individual configurations – at all data centres that comply with the standards of Germany's government cloud.

[20] See https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-ozg-node.html

[21] For further explanations, see also https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/nachnutzung/efa/efa-node.html

The IaaS and SaaS solutions provided through the SCS software stack are in line with the European General Data Protection Regulation.[22] The SCS project plan therefore includes measures aimed at helping public administration platform operators to gain baseline protection (*IT-Grundschutz*) certification from the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) by means of appropriate development processes and architecture and by providing relevant knowledge.[23] Compatibility between Germany's government cloud and Gaia-X can be achieved through the involvement of SCS in the Gaia-X consortium, meaning that the public administration will be able to participate in the Gaia-X ecosystem in future using the existing IT infrastructure. Germany's government cloud supports the establishment and expansion of Gaia-X by guaranteeing interoperability with a view to ensuring that Gaia-X cloud and service solutions can be used within the public administration in future, provided that the information security and confidentiality requirements have demonstrably been met. Representatives of the SCS project are therefore in regular contact with the Sub-Working Group on Technology and Operations.

Whereas the primary focus of Gaia-X is the establishment of a networked data infrastructure corresponding to the goals of digital sovereignty, Germany's government cloud is intended in particular to ensure the multi-cloud reusability of cloud services and software solutions. It might be possible in future to carry over solutions from the SCS project or Gaia-X standards and reuse them for Germany's government cloud. The standards established for Germany's government cloud will remain valid, however, and will merely be expanded as required.

2.3.2 Relevant public administration specifications

The following public administration specifications and guidelines were taken into account when designing the target architecture:

- **IT baseline protection (*IT-Grundschutz*)**: the BSI's IT baseline protection lists methods, instructions and recommendations with the aim of raising and maintaining the level of information security within an institution. A holistic approach is followed, with matters relating to infrastructure, organisation and personnel examined alongside technical issues.

[22] See https://scs.community/de – "Was ist Sovereign Cloud Stack?" (What is Sovereign Cloud Stack?).

[23] Based on the current state of planning, a deadline of early 2023 appears realistic for provision of the necessary components and parallel preparation for certification.

IT baseline protection is described in more detail by the BSI's *IT-Grundschutz* Compendium and the BSI standards. The *IT-Grundschutz* Compendium provides the user with instructions for protecting a particular area. A new version of the Compendium is published every year. The BSI standards provide tried-and-tested approaches by means of which the necessary security measures can be systematically identified and implemented.[24]

- **BSI Cloud Computing Compliance Criteria Catalogue (C5)**:[25] the catalogue specifies the minimum information security criteria to be met by cloud services, with the aim of transparently representing the extent to which a cloud service complies with information security criteria on the basis of a standardised audit. The audit report can be used by customers as a basis for their own risk assessments, and the Criteria Catalogue is used by cloud service providers, auditors and cloud customers. C5 also explicitly examines the obligation incumbent upon cloud service providers and cloud customers to cooperate on information security ("shared responsibility").
- **Federal Government's IT Architecture Guideline**:[26] the Federal Government's IT Architecture Guideline follows an active approach to IT architecture management within the Federal Government administration. The areas affected by the federal IT consolidation project[27] are to be provided with proactive decision-making support in the form of specific strategic architecture specifications, and are to use the specifications for the further

---

[24] See the BSI's IT baseline protection, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

[25] C5 – Cloud Computing Compliance Criteria Catalogue, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

[26] See https://www.cio.bund.de/SharedDocs/kurzmeldungen/Webs/CIO/DE/startseite/2022/09_architekturrichtlinie.html

[27] See https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-konsolidierung/it-konsolidierung-node.html

development of the Federal Government's IT. The specifications also promote the alignment of ongoing IT projects with strategic requirements and policy goals. Examples of architecture specifications include ensuring vendor independence and guaranteeing loose coupling/modularity.

- **Additional Federal Government-specific, state-specific and municipal architecture guidelines/specifications and minimum requirements for IT**: as well as the Federal Government's architecture guidelines, additional Federal Government-specific and state-specific architecture specifications and minimum requirements for IT also exist. These include the GDPR, Networks of the Federal Government service provider obligations, and additional BSI request units in cloud projects, including for example the BSI's minimum standards,[28] the instructions on classified information, detection, and approval.
- **Federal IT architecture guidelines**[29]: federal architecture guidelines were defined with a view to guaranteeing and actively steering a uniform architecture across all federal levels, and are based on the specifications of the Federal Government and the federal states described above.
- **Requirements that apply to technology vendors and solutions with a view to strengthening digital sovereignty**:[30] as part of the strategy for strengthening the digital sovereignty of public administration IT,[31] the Working Group on Cloud Computing and Digital Sovereignty and its Sub-Working Group on Procurement define cross-cutting requirements for the procurement of information and communication technology by or for the public administration. The aim of these requirements is to reduce dependency on

[28] See https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html

[29] See https://www.fitko.de/foederale-koordination/gremienarbeit/foederales-it-architekturboard

[30] In development by the Working Group on Cloud Computing and Digital Sovereignty and its Sub-Working Group on Procurement.

[31] See IT Planning Council, Decision No. 2021/09 – Working Group on Cloud Computing and Digital Sovereignty https://www.it-planungsrat.de/beschluss/beschluss-2021-09

individual vendors by specifying a framework for public administration IT services and their vendors as a basis for the development and provision of solutions. It is envisaged that the requirements will include a minimum level of interoperability, modularity and transparency.

Existing specifications, for example those imposed by the BSI (C5 or IT baseline protection), as well as any instructions on classified information issued by the Federal Government and the federal states, were considered and substantiated during development of the target architecture. Any discrepancies between individual specifications will be resolved during the standardisation process.[32] As a supplement to the catalogue of requirements for technology vendors and solutions – which is designed for external use during the future procurement of IT solutions, with the aim of strengthening digital sovereignty – the standards defined here are designed for internal use and are intended to standardise the existing cloud infrastructure of the public administration and make it fit for the future.

2.4 Further development of the document

The standards listed in Chapter 5 will be further developed iteratively and on an ad-hoc basis, but at least once each year, and adopted as a joint decision with the coordination body (yet to be established) and the associated architecture board of Germany's government cloud (see Chapter 6.1). The IT Planning Council will then be informed, but the latter will adopt a decision only in the event of significant alterations to this framework. Responsibility for updating the document will initially remain with the Working Group on Cloud and Digital Sovereignty and its Sub-Working Group on Technology and Operations. The detailed standards of Germany's government cloud, which are regularly published on the IT Planning Council's website, apply in their most recent version alongside the target architecture framework. The detailed standards of Germany's government cloud are currently being developed by the Sub-Working Group on Technology and Operations and examine in greater depth individual points of the specifications laid down in the framework. In a similar way to the framework, responsibility for the detailed standards (right through to establishment of the architecture board for Germany's government cloud) lies with the

[32] If the standards specified for Germany's government cloud are inconsistent with information security or confidentiality standards or requirements or could be interpreted in a contradictory manner, the requirements prescribed by the BSI always prevail and must be implemented.

Working Group on Cloud Computing and Digital Sovereignty and the Sub-Working Group on Technology and Operations. Since the detailed standards are detailed versions of the requirements defined in the framework (see Chapter 5), the IT Planning Council will be informed about the changes without any need for a decision. The detailed standards will be published individually as separate documents.

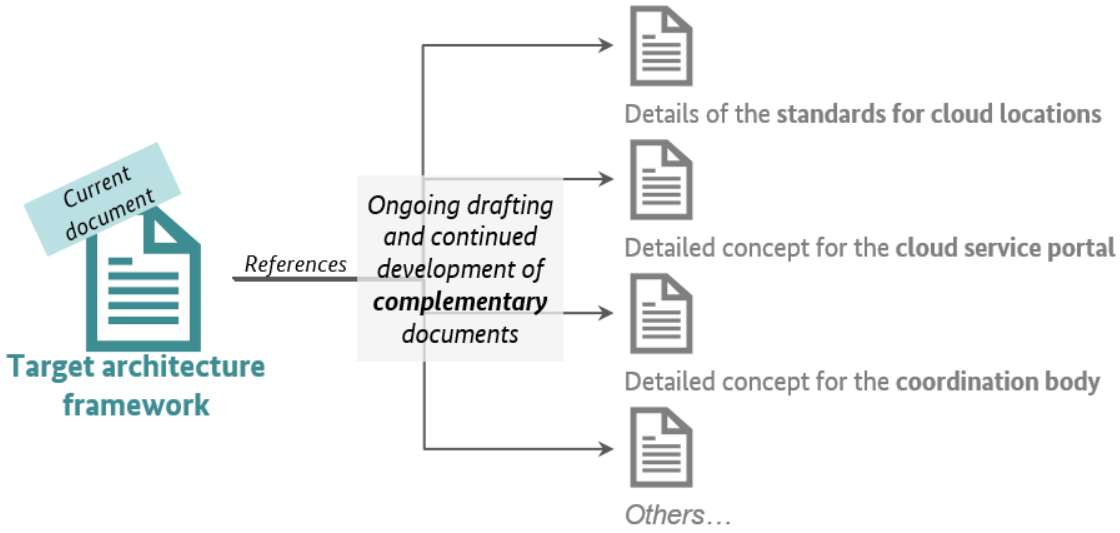

Figure 1: Document structure of the target architecture of Germany's government cloud

Continuous further development of Germany's government cloud and its standards will ensure that Germany's government cloud is always up to date and that it can be flexibly adapted to changing requirements and framework conditions such as technological developments. Certain standards require more detailed explanations prior to implementation; these are described in more depth in Chapter 5.4. Further documents will also be developed on the basis of the methodology and the standards; these are intended, on the one hand, to clarify the technical implementation and, on the other, to specify additional elements of Germany's government cloud (see Chapter 5.5). Figure 1 illustrates the planned document structure and integrates the framework outlined in this document.

3 Added value for the public administration and its IT infrastructure

The aim of Germany's government cloud strategy is to standardise operating concepts and the provision of infrastructure and platforms, and to establish uniform interfaces for federal cloud solutions; this will deliver substantial added value for the public administration (see Figure 2). This added value is based on the strategic objectives for strengthening digital sovereignty[33] (possibility to switch vendors, design capability, and influence on IT vendors) and on the defined objectives of the concept paper on Germany's government cloud strategy.

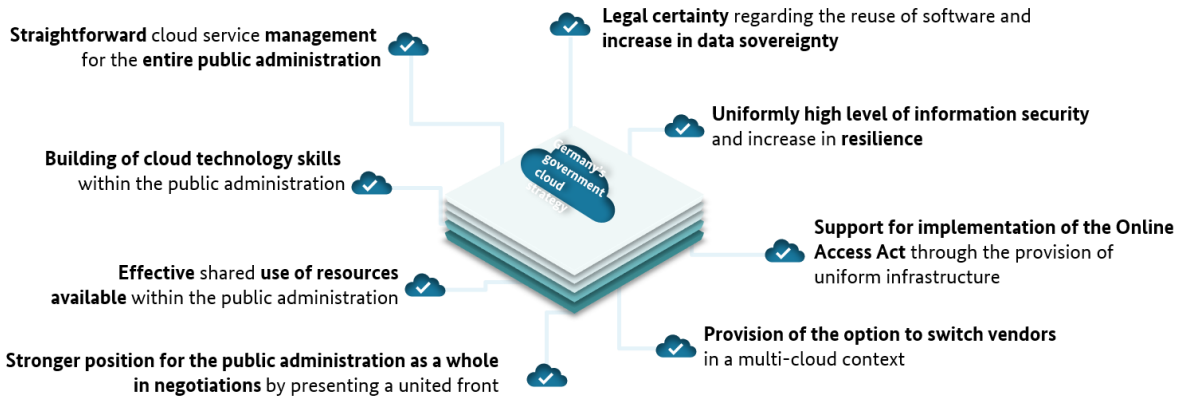

Figure 2: Added value for the public administration and its IT infrastructure (selection)

Germany's government cloud strengthens the digital sovereignty of the public administration by creating possibilities to **switch** vendors, ensuring **design capability** and enabling **influence on IT vendors**. The following features of Germany's government cloud strategy play a particularly important role in this regard:

- The standardisation of operational requirements at various cloud locations will create an attractive market for software vendors, thus expanding the supply.
- The public administration's position will be strengthened in negotiations with software vendors, since the entities at the various administration levels will be able to present a united front on the basis of common standards.

[33] See IT Planning Council, Decision No. 2021/09 – Working Group on Cloud Computing and Digital Sovereignty https://www.it-planungsrat.de/beschluss/beschluss-2021-09

- The mechanisms of Germany's government cloud will systematically promote OS solutions. One of the advantages of this operating approach is that it lays a foundation for the joint support of OS projects, and thus the promotion of alternative solutions, by various administrative entities.
- The integration of approaches from other initiatives such as Gaia-X/SCS will ensure that the latest developments can be introduced into the administrative structures.
- Germany's government cloud will also increase efficiency and effectiveness in the development, implementation and operation of cloud services and software solutions for the public administration, and strengthen information security across the board. A further goal is to optimise data exchange, storage and use: the provision of cloud services by public IT service providers to the entire public administration via the cloud service portal will contribute to the efficient and effective use of the data centre resources available to the public administration and its service providers. The cloud service portal will support this process through the centralised provision of cloud services.
- The potential exchange and reuse of modular solution components on the basis of standardised underlying infrastructure will ensure compliance with the principle of "one-for-all" solutions based on the centralised or decentralised operation of software solutions in connection with implementation of the Online Access Act.
- A stepping up of cooperation between cloud service providers will create synergistic effects throughout the entire software lifecycle.
- The use and implementation of Germany's government cloud will help to build the skills of public IT service providers and the public administration.
- Platform standardisation and a high level of automation will make it easier to achieve an efficient and effective IT infrastructure for the public administration. The option of distributed operation of cloud services and software solutions will also increase the resilience and scalability of the solutions.

- Germany's government cloud is configured to adhere to the principle of "privacy by design"[34]/"security by design",[35] which will mean that the security requirements are met across all federal levels.
- Strict adherence to existing information security guidelines/specifications when defining the standards will further strengthen information security within the infrastructure.

[34] See https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_de

[35] See https://www.oeffentliche-it.de/-/security-by-design

4 Methodology underlying Germany's government cloud

This chapter outlines the envisaged basic structure of Germany's government cloud. First, the basic principles are set out and the individual elements of the structure are defined. Then the relevant roles within Germany's government cloud are described.

4.1 Basic principles

The Federal Government, federal states and municipalities specified general requirements for Germany's government cloud and its standards in Germany's government cloud strategy. The basic principles outlined below, which apply to the target architecture and its subsequent implementation, are specified on the basis of these requirements, which will also be taken into account when defining the individual standards (see Chapter 5).

- **Distributed IT operation:** The distributed operation of Germany's government cloud will be possible at the data centres operated by the Federal Government, federal states and municipalities. It is to be ensured in this connection that services or applications operated within Germany's government cloud by various platform vendors of the Federal Government, federal states and municipalities are able to switch operations between the various platform vendors without significant effort, in keeping with the principle of multi-cloud capability. Although it is envisaged that this decentralised, federal cloud infrastructure will be provided and operated by the public administration and its IT service providers, cloud service providers outside the public administration will also be involved: the integration of external cloud services is supported in principle, provided that they meet the standards for Germany's government cloud.[36] Specifications are yet to be adopted regarding application of the government cloud standards to cloud service providers outside the administration (e.g. hyperscalers) and their services (see Chapter 4.2). It is envisaged that cloud environments that already exist at Federal Government, federal state and municipality level are primarily to be integrated into the structure of Germany's government cloud. The Federal Government, federal state or municipality, or alternatively the service providers of public administration IT responsible for operation, already have

[36] Integration will only be possible following careful checks on the basis of various criteria (relating to data and information security considerations, for example).

the necessary know-how; the establishment of compatibility between the existing cloud environments will enable the optimum use of existing capabilities and the leveraging of synergies.

- **General availability of cloud services:** It is envisaged that the cloud services (e.g. on the basis of the service models IaaS, PaaS and SaaS) offered within Germany's government cloud will be available for use by all public administration entities at Federal Government, federal state and municipality level. Any extensions or adaptations to a service carried out by one government cloud participant should be reusable at other cloud locations.
- **Use of OS software (OSS):** OSS will be given priority when building Germany's government cloud;[37] commercial distributions of OSS will be allowed.[38] Although it will not be necessary for cloud services and software solutions operated within Germany's government cloud to be OSS-based, efforts are to be made to avoid lock-in effects,[39] enable reuse (e.g. through OSS) and allow for and implement risk mitigation measures.[40]
- **Central management of services:** It is envisaged that users of Germany's government cloud will be able to search for, commission, adapt and cancel services via one central cloud service portal, which is accessible from different networks (e.g. the internet, the administration networks); the target group for this option will mainly be software operators. A standardised service catalogue will be available for management of the services offered. The users of the cloud service or software solution being operated will

[37] The prioritisation of OSS does not mean that proprietary solutions are categorically excluded, and the use of a proprietary software stack within Germany's government cloud is possible. Interfaces must be created in line with common standards, however.

[38] OS solutions (including in the cloud environment) are often (further) developed by companies pursuing commercial business models (e.g. support services, enterprise functionalities). It may be advantageous to make use of these with a view to safeguarding and accelerating the introduction and operation of OS solutions.

[39] The term "lock-in effect" describes a negatively perceived constraint that makes it more difficult for the customer to switch products/services or vendors owing to the costs that will arise and other barriers to switching.

[40] These measures are intended to reduce the likelihood and negative impacts of a "lock-in".

actually access the services provided directly at the cloud location, without recourse to the cloud service portal. Additional information on the cloud service portal can be found in Chapter 5.5. It should be possible for cloud services that are available within Germany's government cloud to be ordered from the cloud service providers and used before the cloud service portal is fully operational.

- **Joint further development:** For the purpose of cooperating on public development projects and fostering the further development of key software components (e.g. standard images or policies[41] for the operation of containers), a proprietary platform will be set up for the administration; it will then be possible to create and update on this platform the repositories for (OS) software projects such as standard (application) images or policies for the operation of containers. It is planned that this repository will be connected via the continuous integration/continuous deployment process. The platform in question is the OS platform for the public administration (Open CoDE), which already provides some of these functionalities. Additional information on Open CoDE can be found on the relevant website.[42]

4.2 Overall structure of Germany's government cloud

Broadly speaking, Germany's government cloud consists of the following central elements:

1) **cloud locations, platform operators, software operators and cloud integrators**
2) **cloud service portal**
3) **coordination body**
4) **OS platform for the public administration (Open CoDE)**

The following chapters contain specifications of the individual elements.

[41] See, among other things, the outcome document of the first PoC for Germany's government cloud: https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/220420_PoC-Ergebnisdokument_Langfassung_AG_Cloud_vf.pdf

[42] https://www.opencode.de

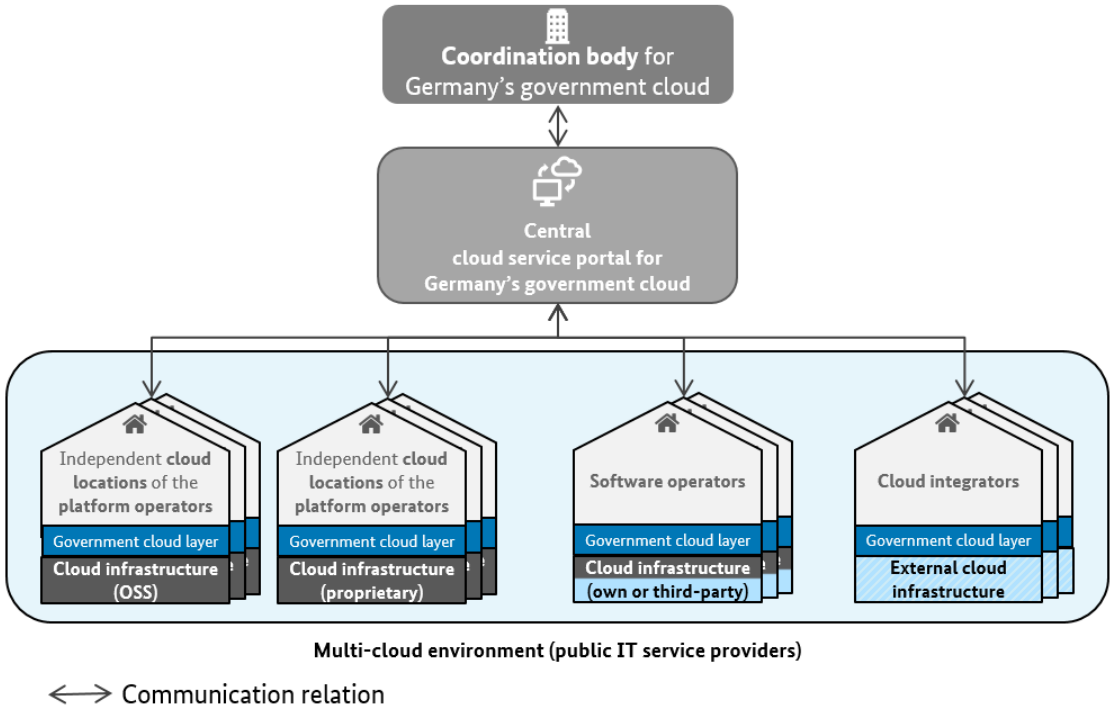

Figure 3: Elements of Germany's government cloud (for illustrative purposes)

The term "**cloud locations**" is used to refer to the data centres operated at Federal Government, federal state and municipality level or by their IT service providers that provide IT infrastructure, for example computing capacities, within Germany's government cloud, offering, in particular, services on the basis of IaaS and PaaS service models. Cloud locations may be accessible exclusively from the internet, exclusively from administration networks, or from both access networks. It is envisaged that automated control of the services of the cloud locations will be possible in future, using programming interfaces (e.g. application programming interfaces, APIs). Cloud locations will be provided by the platform operators. Details of the standards for platform operators and other cloud service providers can be found in Chapter 5.

In addition to platform operators, which make cloud services available at their cloud locations, **software operators** also offer cloud services, albeit exclusively on the basis of the service model SaaS. Software operators use their own or external cloud infrastructure that is compliant with Germany's government cloud in order to operate their SaaS products. A detailed description of the corresponding usage scenarios can be found in Chapter 4.3.

Cloud integrators are service providers of public administration IT that configure the services offered by external cloud providers (i.e. cloud providers outside the administration, such as hyperscalers) in accordance with the standards of Germany's government cloud, and therefore make them available for Germany's government cloud on a legally compliant basis.

The **cloud service portal** is the central entry point for consumers from the public administration for the management of cloud services in a multi-cloud context.[43] It will be accessible from the internet and the administration networks. As a result of the separation requirements[44] that apply to network structures, two separate portal versions will be available. Cloud services will be searched for using a uniform cloud service catalogue. Different services will be displayed as available on the cloud service portal depending on the access network used. When access takes place from the administration networks, it will be possible to see all the cloud services with a connection to the administration networks, and it will be possible to use them accordingly. This also includes internet services. When access takes place from the internet, only the services that are available via the internet will be shown for management.

The implementation project (see Chapter 6.3) will examine how it can be possible to operate a single, central entity of the cloud service portal on the internet taking into account the specifications of the Networks of the Federal Government, and how this entity can also be made available from within the Networks of the Federal Government.

Communication options for the provision and calling off of service products as well as the further exchange of information are to be implemented between the cloud service portal, cloud service providers and other users of the cloud service portal, with due regard for the BSI's requirements such as IT baseline protection (see Chapter 5.4.6.).

Details of the cloud service portal can be found in Chapter 5.5. Links to other service portals operated by service providers of public administration IT at different federal levels are being examined.

---

[43] In this case, multi-cloud means that the cloud services of many different cloud providers (in particular the service providers of public administration IT) can be accessed via the cloud service portal. This also includes the integration of cloud services outside the administration; see also "cloud integrators" in Chapter 4.2.

[44] See connection conditions for the Networks of the Federal Government – Interconnecting Network.

Plans exist to set up a **coordination body** to coordinate the future further development of Germany's government cloud, with due regard for existing federal structures and reuse of these structures wherever possible. In particular, it is envisaged that this entity will be responsible for the cloud service portal, its development and its integration with the cloud locations, and for coordinating updates of the service catalogue – as a list of all the services offered within Germany's government cloud – by the cloud service providers. The coordination body obliges the cloud service providers to enforce the standards of Germany's government cloud. In addition, it is envisaged that the coordination body will develop suitable processes to ensure compliance with the defined standards. Details of the coordination body for Germany's government cloud can be found in Chapter 6.1, in the task document for the coordination body[45] and in the document "Governance of the Coordination Body for Germany's Government Cloud".[46]

In the context of Germany's government cloud, the possibility of switching vendor and multi-cloud capability is guaranteed through standardisation of the requirements imposed on service providers. The technical and organisational standards set by Germany's government cloud are used for this purpose (the government cloud layer, see Figure 3), allowing standardised integration for as many service providers as possible, guaranteeing independence from vendors and OSS projects in keeping with the principle of digital sovereignty. External cloud providers will be integrated via cloud integrators. This means that, in future, software operators will be able to select the cloud location or external vendor for their solutions[47] in a straightforward manner; if data from end customers or authorities are affected, then these stakeholders are to be suitably involved in the decision-making process. The ultimate goal is to ensure that, when operating a cloud service, there is no difference (technically speaking) from the user's perspective between operation by a service provider of public administration IT and operation by an external cloud provider.

The central **OS platform of the public administration (Open CoDE)** is the shared platform of the public administration for exchanging open source software. The target vision of Open CoDE is a

[45] The document "Germany's government cloud strategy: detailed design of the coordination body, tasks of the coordination body" describes the coordination body's core tasks. See https://www.it-planungsrat.de/fileadmin/beschluesse/2022/Beschluss2022-35_Aufgaben.pdf

[46] See https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-rat/beschluesse/beschluss_2023_03_DVS_Anlage_Rahmenkonzept.pdf?__blob=publicationFile&v=3

[47] Note: SaaS solutions are created through provision by a software operator and do not necessarily need to be offered by a cloud location.

central directory of administration-related and available OS software projects/solutions, a web application for version management and the storage of open source code, and participation in projects (code repository), as well as a discussion forum. The code repository has already been used as part of the PoCs for Germany's government cloud for joint project work, the storage of source code and as an external repository for accessing images and software artifacts.

4.3 Definition of roles

The following roles are defined with a view to specifying clear competencies/responsibilities in the context of Germany's government cloud. These roles are used in the following chapters in line with the definitions. Entities or individuals may perform multiple roles:

a) **Cloud service customer** – the cloud service customer procures services from Germany's government cloud via a cloud service broker or directly from a cloud service provider. It may be an authority, an entity within the public administration or a service provider of public administration IT.

b) **Cloud service broker** – the cloud service broker procures a cloud service from a cloud service provider within Germany's government cloud and is responsible for operating and providing this cloud service to its cloud service customers in accordance with contractual obligations. It may act as a link between the cloud service provider and the cloud service customer.

c) **Cloud service provider** – the cloud service provider offers a service within Germany's government cloud and is responsible for providing the service. Within Germany's government cloud, this role is an umbrella term for platform operator, software operator or cloud integrator.

   i. **Platform operator** – the platform operator operates the IT infrastructure at the cloud location and provides the software operator with tools for manual and/or automated orchestration.

   ii. **Software operator** – the software operator is responsible for operating and (where applicable) enhancing a cloud service or software solution on the basis of contractual obligations, and manages service orchestration. In addition, the software operator coordinates the requirements for software operation with the software vendor. It acts as the connecting link between the platform operator and the software vendor.

iii. **Cloud integrator** – the cloud integrator is a role within a service provider of public administration IT. It integrates/combines the services of private-sector cloud providers with potential supporting services into an overall service that is compliant with Germany's government cloud and that, following its approval by the coordination body, can be offered to cloud service customers.

Cloud integration is a process in which:

- applications operated in the cloud are linked to other cloud services and/or on-premise solutions within an entity (including companies with distributed locations)
- applications operated in the cloud are connected with other cloud services and/or on-premise solutions among different companies
- (for SaaS vendors) a range of solutions operated in the cloud are integrated

For this integration, services are used that can be ordered via the cloud service portal and operated in the external cloud of a private-sector company.

This means that the cloud integrator either provides integrated infrastructure or platform services, expanding the role of the platform operator, or provides integrated software services, expanding the role of the software operator.

d) **Cloud service portal user** – the cloud service portal is the central entry point for the cloud service customer's employees, who can search for, request, configure and administer various government cloud services there.

e) **Coordination body:** the coordination body coordinates the further development of Germany's government cloud. It is responsible for the cloud service portal and for its development and integration with the cloud locations, as well as for the service catalogue (a list of all the services offered within Germany's government cloud). The coordination body obliges the IT service providers participating in Germany's government cloud to enforce the standards of Germany's government cloud.

f) **Software vendor** – the software vendor is an entity (in the sense of a legal person) or a loosely connected community (group of developers) that provides the software operator with software (releases) in line with the standards of Germany's government cloud.

4.4 Roles and usage scenarios for Germany's government cloud

With a view to clarifying the interactions between the roles defined above (Chapter 4.3), typical scenarios within Germany's government cloud are outlined below for illustrative purposes. These scenarios are to be used as a basis for describing the wide variety of roles that the service providers of public administration IT perform within Germany's government cloud.

Scenario 1: Procurement via a cloud service broker

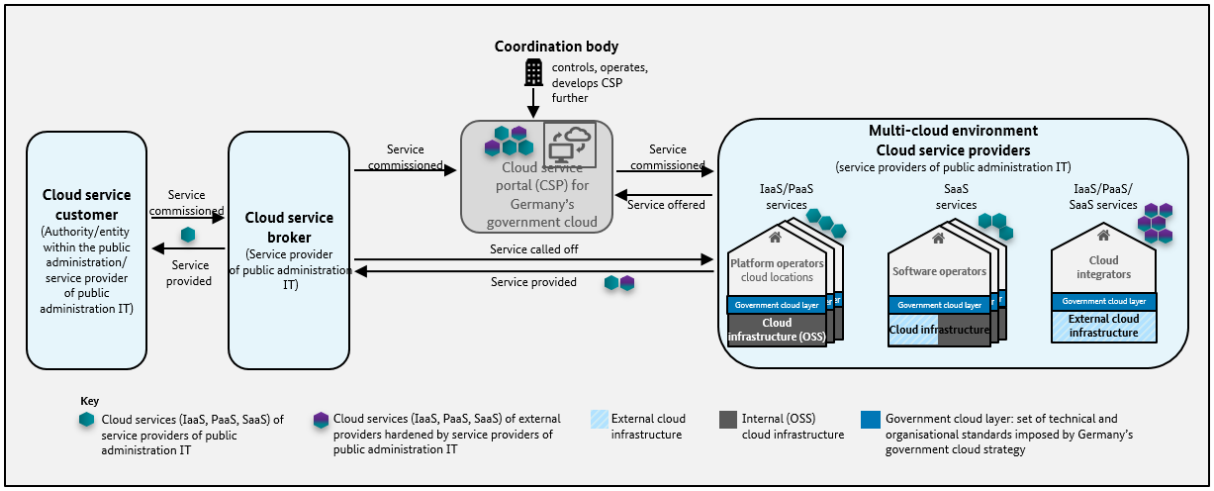

Figure 4: Scenario 1 – Procurement via a cloud service broker

Figure 4 illustrates the interactions in Germany's government cloud for Scenario 1, in which a cloud service customer procures services from Germany's government cloud via its cloud service broker:

1) A **cloud service customer** (authority/entity within the public administration) commissions its **cloud service broker** (service provider of public administration IT) to provide software or a cloud service. The **cloud service broker** orders the requested cloud service from a **cloud service provider** in the cloud service portal. The **cloud service broker** provides the service to its **cloud service customer**.

Scenario 1 thus covers the commissioning of services on the basis of the service models IaaS, PaaS and also SaaS. These can also be procured from an external cloud provider via a cloud integrator. Scenario 1 depicts the case in which the cloud service customer is a public administration entity that is either not a member of Germany's government cloud itself, or that has a central service provider of public administration IT through which it covers all IT procurement operations. This service provider of public administration IT would therefore perform the role of cloud service broker. Although the usual case for this scenario will be commissioning the provision of SaaS, it is also conceivable that a cloud service customer might have its own development departments and might procure infrastructure and platform services for these via its cloud service broker.

Scenario 2: Direct procurement within Germany's government cloud

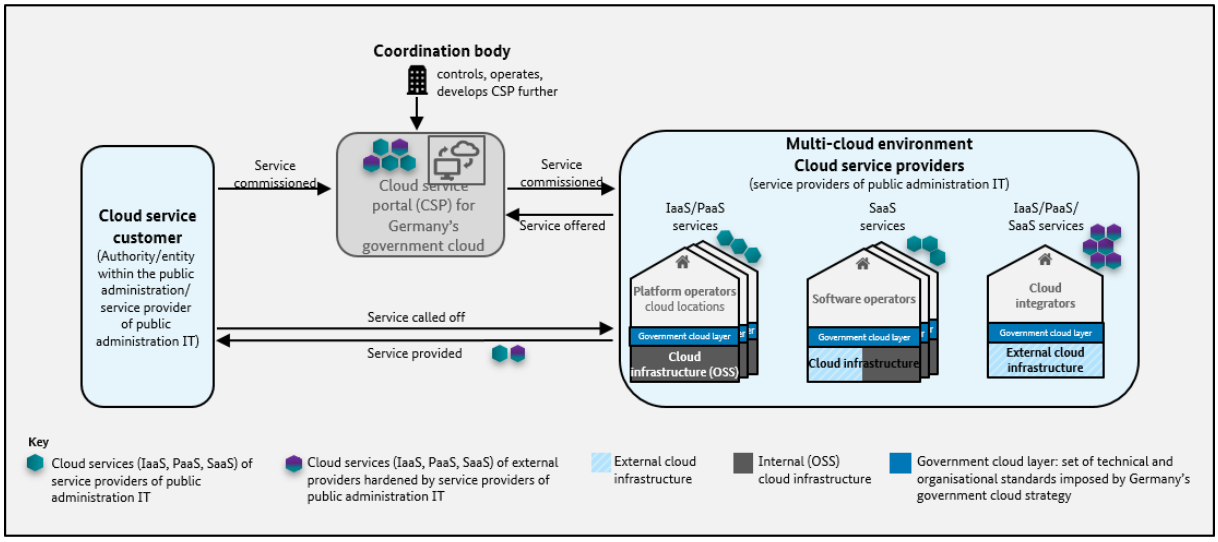

Figure 5: Scenario 2 – Direct procurement within Germany's government cloud

Figure 5 illustrates Scenario 2, in which a cloud service customer accesses the services of Germany's government cloud directly:

2) A **cloud service customer** (authority/entity within the public administration) calls off a cloud service available on the cloud service portal for provision from a **cloud service provider** (depending on the type of service in question, a **software operator**, **platform operator** or **cloud integrator**). The **cloud service provider** provides the cloud service. The **cloud service customer** calls off the services provided from the **cloud service provider**.

Two special cases can be identified on the basis of Scenario 2:

a. A **cloud service customer** calls off one or more cloud services for provision from a **cloud service provider** not for its own use, but instead uses the services to create a new and separate cloud service product.
b. A **cloud service customer** calls off an infrastructure or platform service available on the cloud service portal from a **cloud service provider** (**platform operator** or **cloud integrator**), in order to use it to operate an application (provided by a **software vendor** where applicable) in the role of software operator.

Scenario 2 and its special cases cover not only cases where an authority or entity of the public administration procures cloud services directly from Germany's government cloud as a cloud service user, but also cases where service providers of public administration IT use Germany's

government cloud as cloud service users in order to procure cloud services for their own requirements or to create a separate service-based product.

Scenario 3: Provision of cloud services within Germany's government cloud

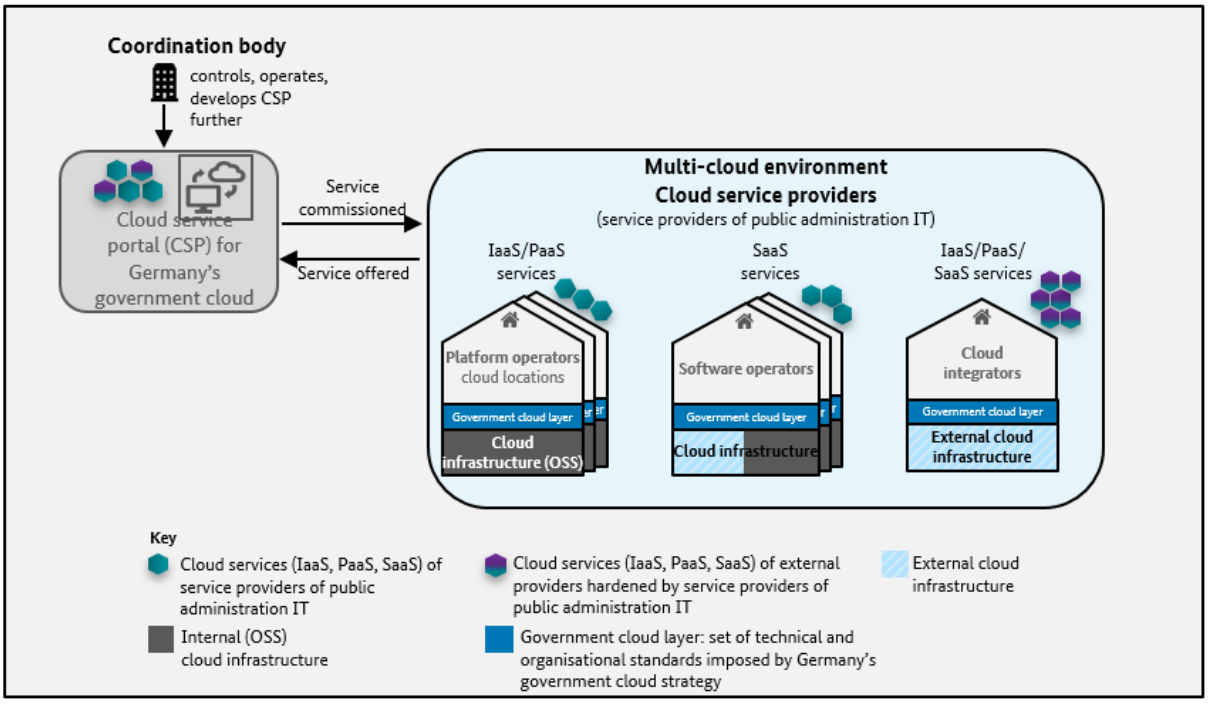

Figure 6: Scenario 3 – Provision of cloud services within Germany's government cloud

Figure 6 illustrates Scenario 3, in which cloud service providers, in other words platform operators, cloud integrators and software operators, offer their cloud services within Germany's government cloud.

3) A **cloud service provider** (this may be a software operator, platform operator or cloud integrator, depending on the type of service) provides its own cloud services via the cloud service portal for ordering and subsequent use, on the basis of the service models IaaS, PaaS or SaaS.

A special case can also be identified on the basis of Scenario 3 in relation to the role of the cloud integrator:

a. A **cloud integrator** purchases a cloud service from an external cloud provider outside Germany's government cloud, configures it according to the standards of

Germany's government cloud, and makes it available via the cloud service portal in a manner compliant with Germany's government cloud.

More detailed user stories can be described for each of the roles, both in the context of the scenario presented above and in a broader sense. The user stories described below are all based on the same pattern: "*As a [role], I want to [requirement/objective/aspiration], in order to [benefit].*"

The user stories that have been selected provide an insight into the capabilities planned for Germany's government cloud in future, and could also be used as a basis for specifying the scope of potential pilot projects (see Chapter 6.2). The list will be updated on a regular basis.

ID	User stories
U1	As a **software operator**, I want to provide standardised platforms for the software vendor in order to ensure that the highest possible level of vendor independence can be achieved when developing solutions at different cloud locations.
U2	As a **software operator**, I want to operate containerised software solutions at different cloud locations in order to achieve reusability.
U3	As a **software operator**, I want to be provided with standardised container clusters in order to facilitate the deployment of software solutions.
U4	As a **software operator**, I want to be provided with tools for managing container environments.
U5	As a **software operator**, I want to be able to inspect the status (including access to monitoring information, for example) of my services in the cloud environments of all platform operators and cloud integrators at all times.
U6	As a **software operator**, I want to be able to check whether the resources I require from the cloud location are compatible with Germany's government cloud standard in order to ensure error-free operation.
U7	As a **platform operator**, I want to use a uniform and common set of rules for the configuration of container clusters in order to be able to provide standardised services.
U8	As a **cloud service portal user**, I want to select services using a filter function in order to find suitable services that meet my criteria.

ID	User stories
U9	As a **cloud service portal user**, I want to commission cloud services (e.g. based on the service models SaaS, PaaS including CaaS, and IaaS) in order to use them at the selected cloud location.

4.5 Potential software solutions for operation at cloud locations

The IT solutions examined when designing the methodology described above and the standards for cloud locations defined on its basis were solutions that could, in principle, be operated at every cloud location, and the various use cases for data centre operation were defined so that Germany's government cloud would meet the requirements of the individual software solutions. The use cases taken into consideration in relation to the software solutions to be operated included the following:

ID	Name of the use case
A1	**Specialist procedure with online application form** The procedure makes it easier for administrators at one or more offices to process applications, take decisions and make services payable. It offers an online application interface and can support electronic record systems.
A2	**TR-RESISCAN and TR-ESOR** TR-RESISCAN involves the operation of a scanning line for the local scanning of documents while maintaining their evidential value at a government site. Once they have been scanned in, they are stored in the repository in accordance with the TR-ESOR standard, in such a way as to maintain their evidential basis.
A3	**AI-based assistance systems for the administration** Personal (voice) assistance systems help citizens by acting as a central access channel to the administration (e.g. chatbots in the digital arena). Similarly, employees of the administration can use "personal assistants" as a decision support tool (to detect anomalies, for example) in order to handle cases more effectively.

ID	Name of the use case
A4	**Email communication** A service is operated for the receipt and sending of emails and the provision of an IMAP mailbox. Emails are sent via an SMTP server. The service can be accessed via a client application or a web frontend.
A5	**Collaboration platforms** Collaboration platforms are used to collaborate on documents, lists and structured data. The platform can be accessed via a client application or a web frontend.
A6	**Video conferencing and messaging systems** A communication platform with messaging, voice over IP, video streaming, chat and file transfer functions is provided. A federated approach is applied to the end-to-end encryption of communications. In a typical case, a group of platforms is established, with the integration of third systems where applicable.
A7	**Online services computer interface (OSCI) and other data transfer mechanisms** A "virtual post office" is provided at the cloud location that can receive data and transfer the data in encrypted form to a different cloud location. OSCI is used as an example.
A8	**Sovereign Workspace for the public administration** Efforts are in progress to develop and provide an alternative workspace for the public administration (with the working title of "Sovereign Workspace"). The Sovereign Workspace will be based on existing OSS solutions and is intended to cover all of the basic functions required by the public administration. This applies, in particular, to the areas of productivity (word processing, spreadsheets, file storage, printing, etc.), collaboration (collaborative work on shared files) and communication (video and audio conferences, emails, text messages, etc.).

5 Key standards

It is envisaged that Germany's government cloud will introduce standards for all participating software operators, platform operators and their cloud locations and cloud integrators at Federal Government, federal state and municipal level. The aim of this chapter is to describe and put into concrete terms a framework for action.

It was ascertained during implementation of the MVP project that the standards for Germany's government cloud defined in Version 2.0 of the framework are not sufficient on a standalone basis to use as guidelines for creating and operating services for Germany's government cloud. On the one hand, they were seen by cloud service providers as an obstacle to creating cloud service solutions that were in line with the market, while on the other, they were seen by cloud service customers as overly limiting; cloud service customers want to be able to request services that are not in line with the maximum demands of current government cloud standards. In response to this, a cloud services maturity model was developed (see Chapter 5.1), which took into account the results of the testing of services during the MVP. The maturity criteria on which the maturity model is based, and the maturity levels assigned to them, were tested and refined during the implementation project. On completion of the implementation project, the current government cloud standards are to be adapted to ensure that they can meet the demands on them in combination with the maturity model. While doing this, it will be necessary to revise the titles of the current government cloud standards, to condense government cloud standards, or to replace them with maturity criteria. Chapter 5.1 is to be seen as an introduction to the topic of maturity levels. The model will be introduced in full as part of Framework Version 3.0.

5.1 Maturity model

It was ascertained during the MVP project that, if all of Germany's government cloud standards were to be strictly implemented, the cloud service portfolio would probably be very limited. Depending on what is required of a service, it is still not essential for every service always to meet every one of the standards for Germany's government cloud in full. This means that it is very much possible to envisage test environments that are set up rapidly via the government cloud. These generally have less stringent requirements than production environments. To achieve this grading of the strict standards for Germany's government cloud, the maturity model described below was developed.

The goal of the model is to develop up to four maturity levels for each maturity criterion. The lowest maturity level must always be reached. One or more maturity criteria can be assigned to each standard for Germany's government cloud.

The maturity level of each of the services offered in the cloud service portal is to be shown transparently.

The grading of the standards for Germany's government cloud into maturity levels has demonstrated a range of benefits:

- The potential of service providers of public administration IT at Federal Government, federal state and municipality levels is wide ranging. The maturity model also allows small and medium-sized service providers to participate in Germany's government cloud.
- The public administration is always under obligation to procure services cost effectively. The maturity model makes it possible to define a cloud service based on the requirements placed on it, allowing public contracting authorities to optimise the costs incurred.
- The requirements imposed on services depend on the intended purpose of these. The maturity model makes it possible to plan services with lower requirements. This will have an effect first and foremost on the speed of provision by the cloud service provider.

Specification pyramid for Germany's government cloud ecosystem

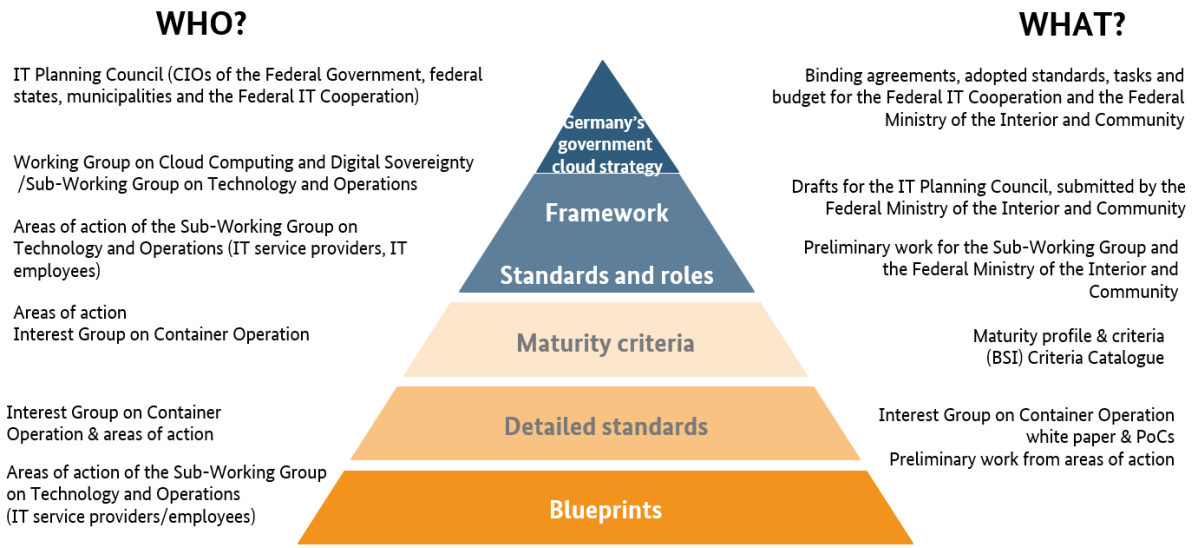

Figure 7: Specification pyramid for Germany's government cloud ecosystem

The government cloud standards are the highest level of the specification pyramid for Germany's government cloud, which has been expanded to include the government cloud maturity model in full. The maturity model makes it possible for cloud service providers to progressively increase compliance with the standards of Germany's government cloud for a set of defined maturity criteria; the lowest level already permits the correct use of the cloud services within the public administration. The set of maturity criteria is termed the maturity profile, and is presented in Chapter 5.1.4. The maturity model creates a bridge to the detailed standards of Germany's government cloud that are to be implemented in full for higher maturity levels. Technical implementation blueprints can be assigned to the detailed standards of Germany's government cloud.

5.1.1 Standards for Germany's government cloud and maturity criteria assigned to them

In the maturity model, the government cloud standards are assigned one or several maturity criteria. The requirement levels currently assigned to Germany's government cloud standards will be reflected by the maturity levels in the maturity model.

The following table provides two examples to clarify the assignment of maturity levels.[48]

[48] The table contains some examples and is to be completed. The IDs provided are not definitive.

Standard for Germany's government cloud	Maturity criteria
DVC-001-R01 – Applicable law	• DVC-RK002-R01 – The service can be utilised in compliance with data protection criteria (GDPR).
DVC-002-R01 – Production specifications	• DVC-RK003-R01 – The point of production for the service is in Germany. • DVC-RK004-R01 – A change of operator requested by the customer is made possible. The service supports the portability of data when changing vendor. • DVC-RK005-R01 – A change of operator requested by the customer is to be made possible. In an ideal situation, therefore, the service is provided at several cloud locations.

Table 1: Table with the assignment of maturity criteria for the standards of Germany's government cloud

5.1.2 Maturity criteria

The general requirements for a maturity criterion are set out in its use case. The implementation of the maturity criterion is defined in four progressive maturity levels. A maturity criterion can be assigned to one or several standards.

5.1.2.1 Template for the specification of maturity criteria

A uniform format was chosen for the description of maturity criteria. A maturity criterion is identified by means of a unique title and an auditable identification number (ID). The following template is based on the template provided in the Federal Government's IT Architecture Guideline.[49]

[49] See https://www.cio.bund.de/SharedDocs/kurzmeldungen/Webs/CIO/DE/startseite/2022/09_architekturrichtlinie.html

Title	**Title of the maturity criterion**
ID	**Auditable identification number**
Use case	Description of the maturity criterion use case.
Note	Brief note of how the maturity criterion is to be graded.
Reference detailed standard	***Optional*:** Reference to detailed standard document and underlying maturity level. • Maturity level ID: Link to detailed standard

Table 2: Template for the specification of a maturity criterion

DVC (prefix indicating that the standard forms part of Germany's government cloud) –

RKXXX (consecutive, unique serial number) –

RXX (suffix identifying the revision status of the standard, with R01 for the initial version)

5.1.2.2 Example of a maturity criterion

The example below does not represent the final definition, and is only provided to help illustrate a maturity criterion.

Title	The software is horizontally **scalable.**
ID	**DVC-RK001-R01**
Use case	Implementation of the (horizontal) scalability of (containerised) software.
Note	The software provides options for horizontal scalability. The structural scaling limits are documented.
Reference detailed standard	

Table 3: Example of a maturity criterion

5.1.3 Maturity levels

In the current document, each standard and its specifications is assigned a requirement level. The requirement level will be replaced by the introduction of maturity levels. Each maturity criterion can be assigned up to four maturity levels. Unless otherwise stated, the specifications of higher maturity levels automatically also include the lower levels. This means that maturity level 4 encompasses the specifications of maturity levels 1–3. It is not always necessary to define all four levels of a maturity criterion.

5.1.3.1 Template for the specification of maturity levels

A uniform format was chosen for the description of maturity criteria and the maturity levels assigned to them. As part of this, maturity levels are identified by means of a unique auditable identification number (ID). The following template is based on the template provided in the Federal Government's IT Architecture Guideline.[50]

[50] See https://www.cio.bund.de/SharedDocs/kurzmeldungen/Webs/CIO/DE/startseite/2022/09_architekturrichtlinie.html

ID	ID of the maturity criterion
Maturity level 1	Definition of maturity level 1
Maturity level 2	Definition of maturity level 2
Maturity level 3	Definition of maturity level 3
Maturity level 4	Definition of maturity level 4

Table 4: Template for the specification of maturity levels

The maturity level ID consists of:

Maturity criterion ID (ID of the maturity criterion) –

X (maturity level)

5.1.3.2 Example of a maturity level

The example below does not represent the final definition, and is only provided to help illustrate the maturity level assigned to a maturity criterion.

ID – Name	DVC-RK001-R01 – Horizontal scalability of the software
Maturity level 1	The **software vendor provides the possibility of horizontal scalability of the software** that can be **put into operation almost without disruption**. The structural scaling limits are documented. The **software vendor has a process in place** to recognise and implement the demand for horizontal scaling. The structural scaling limits are documented.
Maturity level 2	The **software vendor supports autoscaling for the horizontal scalability of the software that can be put into operation without disruption**. The structural scaling limits are documented. The **software operator has a process in place that permits autoscaling within the structural scaling limits (upscaling and downscaling).** The structural scaling limits are documented.
Maturity level 3	The **software vendor** supports autoscaling for the horizontal scalability of the software that can be put into operation without disruption. The structural scaling limits are documented. **These can be configured and adapted at an application level.** The **software operator** has a process in place that permits autoscaling within the structural scaling limits (upscaling and downscaling). The structural scaling limits are documented. **The scaling parameters can be adapted to the run time.**

ID – Name	DVC-RK001-R01 – Horizontal scalability of the software
Maturity level 4	The **software vendor** supports autoscaling for the horizontal scalability of the software that can be put into operation without disruption. The structural scaling limits are documented. These can be configured and adapted at an application level **and changed without disruption.** The **software operator** has a process in place that permits autoscaling within the structural scaling limits (upscaling and downscaling). The structural scaling limits are documented. The scaling parameters can be adapted to the run time **by the customer on a self-service basis.**

Table 5: Example of a maturity level

5.1.4 Maturity profile

Cloud service customers have the option to define the minimum quality level of their cloud service based on the pre-defined maturity level of the maturity criteria. A requirement maturity profile for the respective cloud service is developed for the cloud service customer based on all of the necessary maturity criteria for a cloud service, and the necessary maturity level in each case. This can be aligned with the cloud service maturity profile of the cloud service provider included in the cloud service catalogue of the cloud service portal.

Two example maturity profiles are provided below to help illustrate the concept.

Maturity profile Canteen software

Maturity criterion	Maturity level			
	1	2	3	4
A	X			
B		X		
C		X		
D	X			
...				
Z	X			

Figure 8: Maturity profile of canteen software

In the example of the maturity profile for canteen software, customer requirements for the maturity criteria have classed a maturity level of 1, such as:

- dispensing with the provision of a data export function for a potential switch of operator (A)
- providing the possibility of horizontal scalability of the software (D)

as acceptable.

Maturity profile Critical software

Maturity criterion	Maturity level			
	1	2	3	4
A			X	
B			X	
C				X
D				X
...				
Z				X

Figure 9: Maturity profile of critical software

Customer requirements in the example of the maturity profile for critical software look very different. In this case, the customer regards the following as necessary:

- for a potential operator switch: "The option of data provision in case of a switch (import and export capability) is available and can be used by the cloud service customer" (A).
- for the horizontal scalability of the software: "The software vendor supports autoscaling for the horizontal scalability of the software that can be put into operation without disruption. The structural scaling limits are documented. These can be configured and adapted at an application level and changed without disruption. The software operator has a process in place that permits autoscaling within the structural scaling limits (upscaling and downscaling). The structural scaling limits are documented. The scaling parameters can be adapted to the run time by the customer on a self-service basis." (D)

The customer has specified maturity level 3 for maturity criterion A and maturity level 4 for maturity criterion D.

5.2 Template for the specification of standards

The standards in Version 2.5 of the framework have not been amended and remain valid until the introduction of the maturity model.

A uniform format was chosen for the description of the standards. A standard is identified by means of a unique title, a requirement level and an auditable identification number (ID). The following template is based on the template provided in the Federal Government's IT Architecture Guideline.[51]

Title: Title of the standard	**Requirement level: MUST / SHOULD / MAY / MUST NOT**
ID: auditable identification number	
Description	Brief description of the standard that must be complied with.
Reference	*Optional*: Reference to Chapter 5.4 et seqq. for further details of the standard and further (technical) explanations, or reference to existing specifications/documents.

Table 6: Template for the specification of standards

As explained in Chapter 2.4, it is envisaged that the standards will be updated and further developed on a regular basis, and at least once per year. An auditable ID ensures that the traceability of changes is guaranteed at any time. The ID is structured as follows:

DVS (*prefix indicating that the standard forms part of Germany's government cloud strategy)* –

XXX (*consecutive, unique serial number*) –

RXX (*suffix identifying the revision status of the standard, with R01 for the initial version*)

[51] See https://www.cio.bund.de/SharedDocs/kurzmeldungen/Webs/CIO/DE/startseite/2022/09_architekturrichtlinie.html

The requirement level (MUST, SHOULD, MAY, MUST NOT) is also specified in a standardised format to reduce the scope for interpretation and promote a shared understanding. Definitions of the individual requirement levels can be found in Chapter 7.1 (Annex).[52]

5.3 Collection of standards

This subchapter outlines the current status of the key standards for Germany's government cloud. Additional (technical) details concerning individual standards are provided in the following chapters.

Title: Applicable law		**Requirement level: MUST**
ID: DVS-001-R01		
Description	German law MUST be fully applicable to all services provided in the context of Germany's government cloud.	
Reference	Ensuring that the legislative requirements relating to correct administrative action are met.	

[52]Definitions based on RFC 2119 (https://datatracker.ietf.org/doc/html/rfc2119).

Title: Specifications relating to production, service and sub-contractors		Requirement level: MUST
ID: DVS-002-R01		
Description	The following framework conditions MUST be met when operating cloud services and software solutions subject to requirements in the areas of confidentiality, security and legal certainty: - the point of production is in Germany - the point of service is in Germany Each cloud service provider MUST be in a position to maintain a list of subcontractors throughout the entire supply chain and guarantee that only employees with security clearance have access to the systems.	
Reference	• Strategy for strengthening the digital sovereignty of public administration IT. • Ensuring that the legislative requirements relating to correct administrative action are met.	

Title: Sovereign control of hardware and software		Requirement level: MUST
ID: DVS-003-R02		
Description	The hardware and software used MUST be selected and operated in such a way that the capacity of the cloud service customers to take action is not jeopardised by decisions on the part of the software vendor or a cloud service provider. In the case of important procedures, sovereign control[53] over the hardware and software used MUST remain with the public administration. In accordance with the strategy that has been adopted for strengthening the digital sovereignty of public administration IT, design capability MUST be ensured.	
Reference	Strategy for strengthening the digital sovereignty of public administration IT.	

Title: Standards for software components		Requirement level: MUST
ID: DVS-004-R01		
Description	Each cloud service provider MUST use software components based on the standards of Germany's government cloud; this applies, in particular, to container operation. Products built on the components may deviate in certain ways.	
Reference	See Chapter 5.4.1.	

[53] In this context, "sovereign control" is exercised if the public administration has adequate sway over the systems to guarantee the necessary availability, information security and data protection.

Title: IT baseline protection certification from the BSI		Requirement level: MUST
ID: DVS-005-R01		
Description	Each cloud service provider MUST define a suitable information network and arrange for it to be certified in line with ISO 27001 on the basis of the BSI's IT baseline protection standard.	
Reference	*No reference.*	

Title: Compliance with the C5 Criteria Catalogue		Requirement level: SHOULD
ID: DVS-006-R01		
Description	Each cloud service provided in connection with Germany's government cloud SHOULD[54] meet the criteria set out in the BSI's C5 Criteria Catalogue.	
Reference	*No reference.*	

[54] The requirement level for this standard is planned to be MUST from 1 January 2024. The context to this decision is that the BSI's C5 Criteria Catalogue for container technology is not yet in sufficiently widespread use.

Title: Sovereign control over crypto modules and keys		Requirement level: MUST
ID: DVS-007-R01		
Description	The public administration MUST exercise sovereign control over the crypto modules/keys in order to have self-determined control of access to the stored data. The service providers MUST be able to adapt the encryption technologies in order to ensure that the BSI's specifications can be implemented at any time.	
Reference	• Strategy for strengthening the digital sovereignty of public administration IT. • Data encryption requirements based on IT baseline protection.	

Title: Provision of a container environment (CaaS) and container clusters		Requirement level: MUST
ID: DVS-008-R01		
Description	Each platform operator MUST provide a container environment (container as a service, CaaS) for the operation of software solutions. The environment includes the IaaS and PaaS components required for container operation and the container services.	
Reference	See Chapter 5.4.4.	

Title: Delivery of container solutions		Requirement level: MUST
ID: DVS-009-R01		
Description	Each cloud location MUST provide a system for delivering container solutions (container registry) for the software operators. The system MUST support the description of target states for the rollout or update of the software solutions operated. The vulnerability scanning system MUST be supported for the software solutions.	
Reference	See Chapters 5.4.1 and 5.4.4.	

Title: Extensions for the container environment		Requirement level: MAY
ID: DVS-010-R01		
Description	Each platform operator MAY offer extensions to the container environment or extensions with a connection to the container environment. Examples of possible options include specific standard images, frameworks or database management systems (DBMS).	
Reference	See Chapter 5.4.4.	

Title: Accessibility of locations		Requirement level: MUST
ID: DVS-011-R02		
Description	Each cloud location MUST be accessible from the administration networks for which it offers cloud services, e.g. the Networks of the Federal Government, or from the internet. Communication between cloud locations MUST comply with statutory provisions, e.g. the German IT Network Act (*IT-Netzgesetz*, IT-NetzG). The requirements of Germany's government cloud are to be taken into account in the implementation of the public administration information network as part of the 2030 Network Strategy.[55]	
Reference	See Chapter 5.4.2.	

Title: Implementation of the zone model		Requirement level: MUST
ID: DVS-012-R02		
Description	Each cloud location MUST implement the blueprint of the zone model for uniform access routes. Location-specific deviations are possible provided that they comply with the BSI's specifications (IT baseline protection).	
Reference	• See Chapter 5.4.2. • BSI's IT baseline protection.	

See https://www.bdbos.bund.de/DE/NdB/Ziele/ziele_node.html

Title: Establishment of an interface with the cloud service portal		Requirement level: MUST
ID: DVS-013-R01		
Description	Each cloud service provider MUST be able to meet the requirements that apply in relation to the provision, alteration or cancellation of services through the cloud service portal via a standardised (technical) interface. This interface MUST also support incident[56] and change[57] management. It MUST additionally be possible to transfer information concerning the service catalogue and the provision of services and billing data to the cloud service portal via the interface.	
Reference	See Chapters 5.4.6 and 5.5.	

[56] In this context, "incident" means a security incident or malfunction involving an IT solution.

[57] In this context, "change" means a modification or update to an IT solution.

Title: Possibility of switching operator		Requirement level: MUST
ID: DVS-014-R02		
Description	Each cloud service provider MUST offer suitable options for a cloud service customer to switch operators within Germany's government cloud. Stored data MUST be exportable and provided to the cloud service customer in such a way that they can feasibly be imported or restored by another cloud service provider. For all services offered, the software or platform operator MUST provide the necessary functionalities for exporting data in an open and standardised format. Both international technology standards (e.g. file format standards) and the XML in Public Administration (XÖV) standards of the public administration (e.g. XProzess, XDatenfelder, XDomea) must be taken into account in this connection.	
Reference	*No reference.*	

Title: Provision of required documentation		Requirement level: MUST
ID: DVS-015-R01		
Description	Each platform operator MUST make available to the software operator the required documentation for the services provided.	
Reference	*No reference.*	

Title: Provision of development areas		Requirement level: MAY
ID: DVS-016-R01		
Description	Each platform operator MAY provide development areas.	
Reference	See Chapter 5.4.5.	

Title: Connection to the central OS platform for the public administration (Open CoDE)		Requirement level: MUST
ID: DVS-017-R01		
Description	If development areas are provided, each platform operator MUST facilitate a connection to the OS platform for the public administration (Open CoDE).	
Reference	See Chapter 5.4.5 and https://www.opencode.de.	

Title: Support for DevOps approaches		Requirement level: MUST
ID: DVS-018-R01		
Description	The development areas provided by each platform operator MUST support the DevOps approaches of continuous integration and continuous deployment referred to in Chapter 5.4.5.	
Reference	See Chapter 5.4.5.	

Title: Provision of software as a service (SaaS)		Requirement level: MAY
ID: DVS-019-R01		
Description	Each software operator MAY offer services based on the SaaS service model via the cloud service portal.	
Reference	*No reference.*	

Title: Function of a backup data centre		Requirement level: MAY
ID: DVS-020-R01		
Description	Each cloud location MAY offer the function of a backup data centre for the operation of specialised applications with special requirements (e.g. with the aim of georedundancy).	
Reference	*No reference.*	

Title: Cloud service portal		Requirement level: MUST
ID: DVS-020-R01		
Description	A self-service cloud service portal will be set up for the public administration; it will be possible to use this portal to manage cloud services based on different service models (e.g. IaaS, PaaS, SaaS).	
Reference	See Chapter 5.5 and the detailed concept for the cloud service portal.	

5.4 Details of individual standards

A number of the standards previously specified will be clarified in further detail below. These clarifications do not constitute a definitive technical specification, however. In some cases,

particularly important requirements from the *IT-Grundschutz* Compendium are highlighted, but it should be noted in this connection that IT baseline protection is fundamentally to be implemented by the participating cloud service providers. It is envisaged that additional documents (see Chapter 6) will provide users, in particular the cloud service providers, with **technical guidance** on targeted implementation.

Figure 10 provides an overview of how a cloud location is designed on the basis of the standards set out in Chapter 5.3. Further details can be found below.

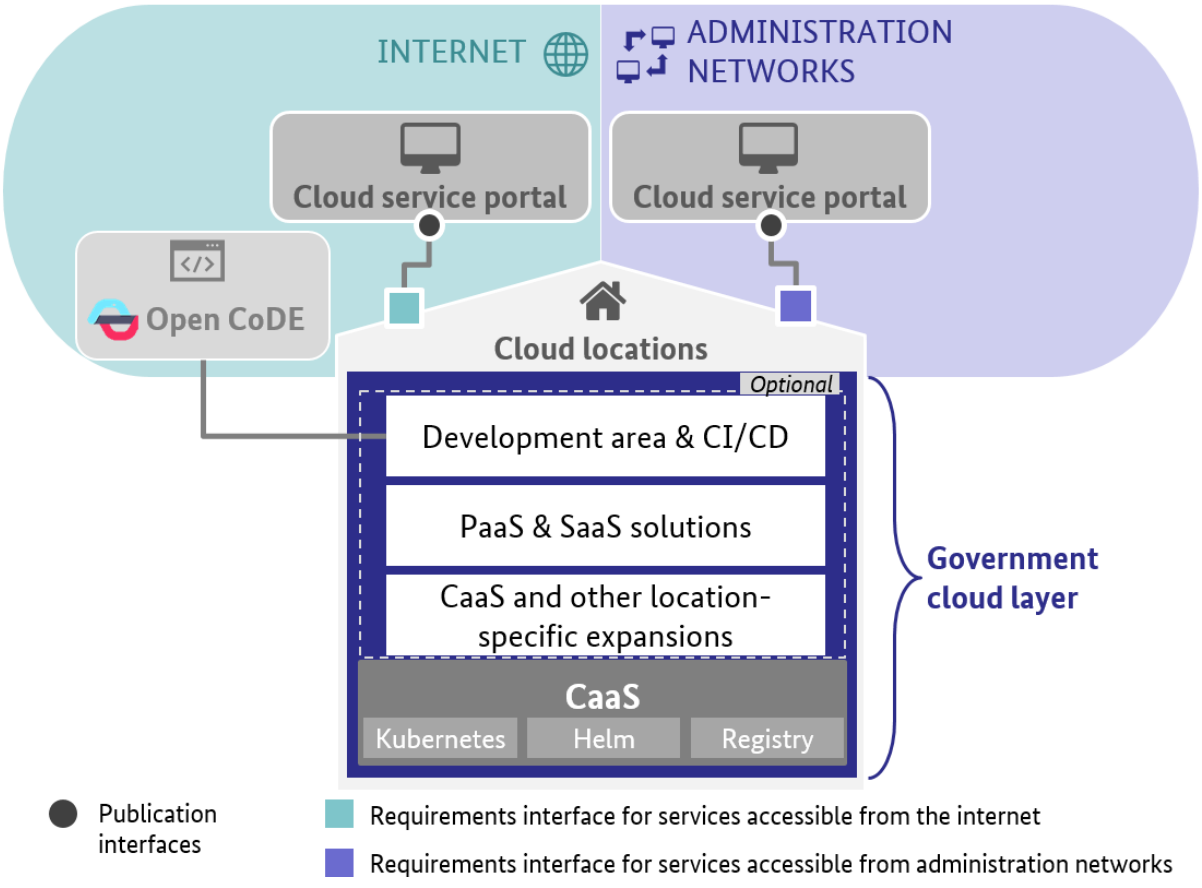

Figure 10: Obligatory and optional standards for cloud locations (for illustrative purposes)

5.4.1 Specified software components

As explained in the section outlining the basic principles of Germany's government cloud (see Chapter 4.1), priority will be given to the use of OS solutions. Uniform, scalable, OS-based software

components must therefore be used for the provision of container environments at the relevant cloud locations. The following list is not exhaustive; in the course of further development, additional components may be added or the specified components replaced with alternatives (e.g. components that are more up-to-date or more suited to the purpose; in these cases, transitional periods for migrations are required):

Kubernetes – software for the automated orchestration and management of container applications (e.g. scaling, operation and maintenance) on distributed hosts.

Helm – software that acts as a package manager for Kubernetes and facilitates the deployment of containerised software solutions as well as version management using "Helm charts".

Container registry (e.g. Harbor) – a software type for managing repositories for software artifacts and images (memory dump of a container) with additional features such as vulnerability scanners. Products built on the software components may deviate in certain ways. For example, commercial distributions (see Chapter 4.1) of OSS or proprietary products based on software components are possible in principle; the use of OSS is preferred.

5.4.2 Zone model

A uniform zone model aligned with IT baseline protection[58] was defined as a blueprint for implementation at all cloud locations (see Figure 11). Location-specific deviations that comply with the BSI's specifications are possible.

The following three zones are separated from each other: 1) external zone, 2) internal zone and 3) zone with increased protection needs or confidentiality requirements (e.g. VS-NfD (restricted)). BSI-compliant separation can be carried out both physically and virtually provided that an equivalent level of security is achievable. The zones will be put into operation on the basis of the possibilities available for cloud locations, and there is no obligation to offer all zones.

[58] See inter alia https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_1_1_Netzarchitektur_und_design_Edition_2021.pdf?__blob=publicationFile&v=23

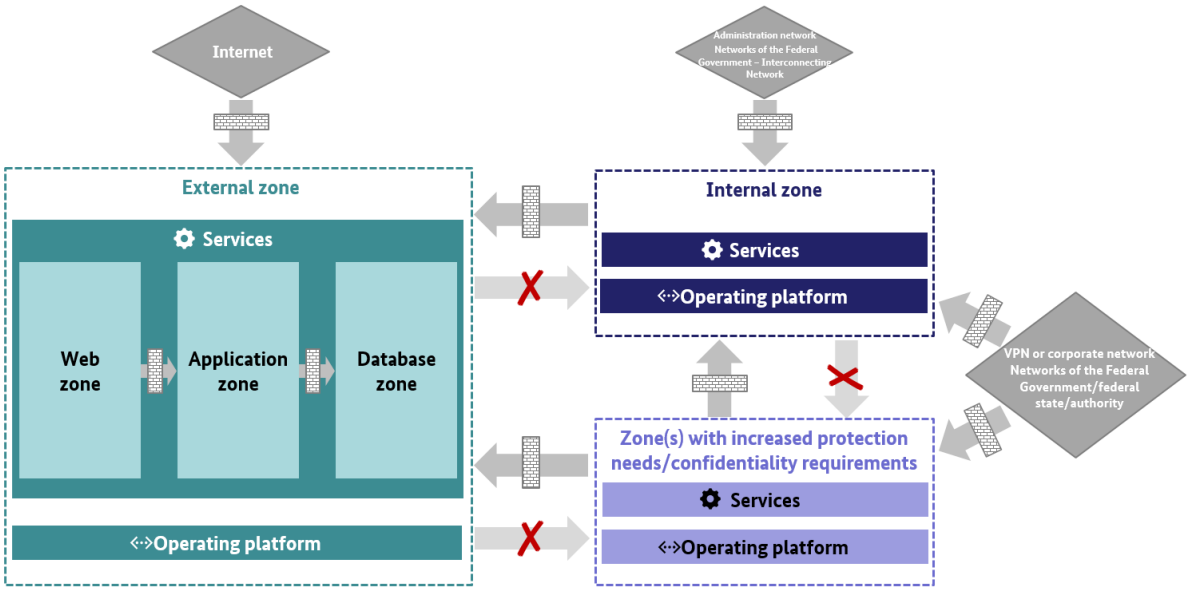

Figure 11: Blueprint of the uniform zone model for the cloud locations

The external zone is designed for use from the internet and is further subdivided into the web, application and database zones. These three zones each fulfil different purposes: the web zone is used to provide the application level gateway or web proxy, the application zone is used to provide application servers, and the database zone is used to provide the DBMS. The boundaries of a demilitarised zone (DMZ) within the external zone are defined in Chapter 5.4.4, since this task is closely related to the provision of container clusters.

Access from the exterior (e.g. from the internet or via the Networks of the Federal Government – Interconnecting Network) is filtered by means of security gateways[59] (packet filter – application level gateway – packet filter – (P-A-P) structure in line with the BSI's recommendation[60] or comparable), see Chapter 5.4.3. The connection requirements of the relevant network operators must be met upon connection to the network. The specific technical equipment must be chosen accordingly and have the necessary authorisations, e.g. for documents classified as VS-NfD (restricted). In future, the public administration information network, which is defined in the 2030

[59] See the glossary for a definition of the term "BSI".

[60] The "packet filter – application level gateway – packet filter" (P-A-P) structure should be used, see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.pdf?__blob=publicationFile&v=2

Network Strategy, may also be supported. Communications between the zones are filtered by means of packet filters. High-performance firewalls at layer 4 of the OSI model (transport layer) or higher must be used for network separation. Specific access routes from one zone to another cannot be granted in this connection, hence access from the internet to the internal zone via the external zone is not permitted. It is envisaged that an independent operating platform on which the services will be orchestrated and controlled will be established for each zone.[61]

More detailed requirements that must be met by the platform operator can be identified on the basis of the zone model described above:

- The platform operator MUST achieve logical or physical separation of the networks for administration of the hosts and container service from the application networks, e.g. on the basis of a virtual local area network (VLAN).
- The platform operator MUST achieve separation of the various management interfaces of the IT systems on the basis of their intended purpose and their network position using a stateful packet filter or comparable solution.
- The platform operator MUST ensure that zone-based segmentation cannot be circumvented through management communication. The possibility of bridging segments MUST be excluded.
- The platform operator MUST ensure BSI-compliant management of the administration accounts and the technical accounts.
- The platform operator MUST ensure the connection of monitoring and logging systems in accordance with a BSI-compliant methodology (see IT baseline protection modules).
- The platform operator MUST establish an audit system[62] for system areas, including the configuration files, registry and software operating process.

[61] Based on the IT baseline protection module NET: Networks and communication – NET.1.1 Network architecture and design, NET.1.2 Network management, NET.3.1 Routers and switches, NET.3.2 Firewall.

[62] See the glossary for a definition of terms.

5.4.3 Network connection

On a supplementary basis to the zone model in Chapter 5.4.2, this standard contains specifications on the network connection or gateways. The analysis focuses on the transition from the internet to the web zone of the external zone and the packet filters (firewalls) originated from there in front of the application zone (see Figure 11).

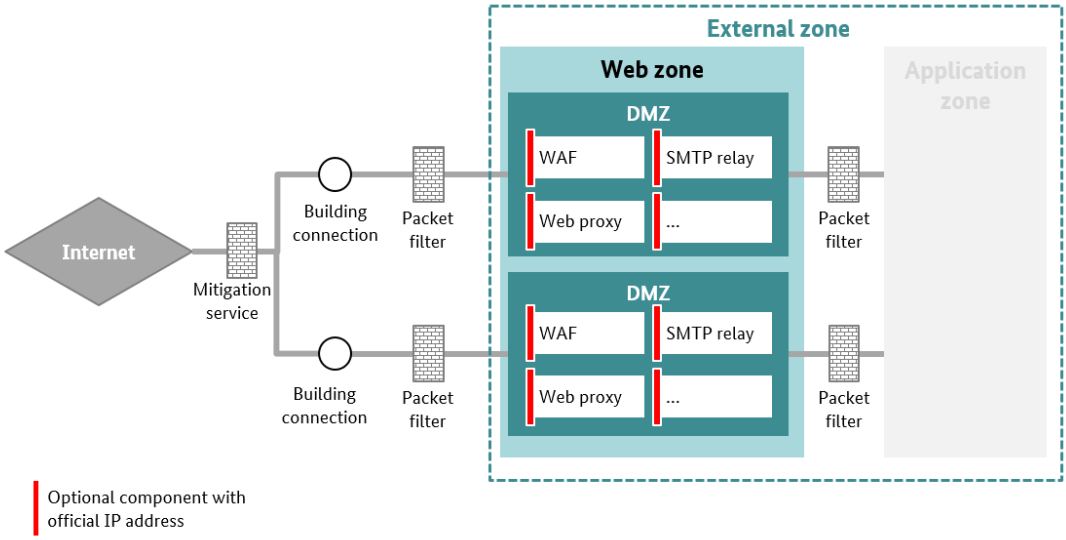

Figure 12: P-A-P structure in line with the BSI's IT baseline protection

According to the BSI's IT baseline protection, a P-A-P structure is to be planned (see Figure 12). Upstream of the P-A-P structure, the internet provider should provide a service for the detection and prevention of attacks, for example a DDoS mitigation service. The cloud location itself is connected with at least two physical lines to the internet by means of a redundant network connection. The two packet filters also perform the role of firewalls. The application level gateway (web zone in Figure 12) contains components such as a web application firewall (WAF), a web proxy, an SMTP relay, or similar. Public IP addresses terminate in this zone and at these components, i.e. only internal IP addresses are assigned in all downstream structures. In addition, application logic is not permitted in the web zone, i.e. no application servers or similar can be operated there.

Accordingly, the following requirements apply to the network connection:

- The cloud location MUST guarantee a redundant network with separate routing.
- The cloud location MUST guarantee a network connection that is node-disjoint and edge-disjoint.
- The cloud location SHOULD use an upstream service for the detection and prevention of attacks when accessing the internet.
- All network accesses MUST be part of an information network for which IT baseline protection has been implemented.
- IPv4 MUST be supported.
- IPv6 SHOULD be supported.
- The aim MUST be conversion to IPv6.

The following requirements apply in particular, and result from the IT baseline protection module NET.1.1:

- A P-A-P structure MUST be used when connecting to the internet.
- All data flows MUST be restricted by the firewall structure to the required protocols and communication relations, and documented.
- Auditable logging MUST be possible at the firewall.
- Security information and event management (SIEM) MUST be used.

Furthermore, the following classifications apply in respect of the IT baseline protection requirement NET.1.1.A9:[63]

- The internet is regarded as an insecure network.
- The Networks of the Federal Government – Interconnecting Network (NdB-VN)[64] is classified as trusted. It does not achieve the same level of trust as the networks of the cloud location, however.

The P-A-P structure described here is prescribed for connection to the internet. Access from administration networks is possible on an analogous basis, but a streamlined structure of the

[63] Extract from the BSI baseline protection module NET.1.1.A9 *Basic Protection of Communication with Untrusted Networks*: "Every network's level of trustworthiness MUST be defined. Networks that are not trusted MUST be treated like the Internet and secured accordingly."

[64] Netze des Bundes – Verbindungsnetz.

protection for incoming and outgoing communications is possible, subject to the fundamental assumption that it involves a communication partner from a secure network.

5.4.4 Container environment and container clusters

A fundamental aspect of providing a container environment is the establishment of clusters for executing containerised software solutions. Kubernetes offers a namespace creation feature for the further subdivision of individual clusters. Namespaces can be regarded as virtual clusters within a Kubernetes cluster.

Among other things, the design of the clusters depends on the relevant technology and security requirements, such as those resulting from the zone model defined in Chapter 5.4.2. On the basis of the model, schematics have been developed for the provision of container clusters for web applications within the external zone.

The web zone is regarded as a DMZ. A P-A-P structure is therefore used to separate the application zone and the exterior (for details, see Chapter 5.4.3), and thus provides protection towards the internet. Each communication relation between container clusters and namespaces requires explicit approval. Figure 13 illustrates the container environment.

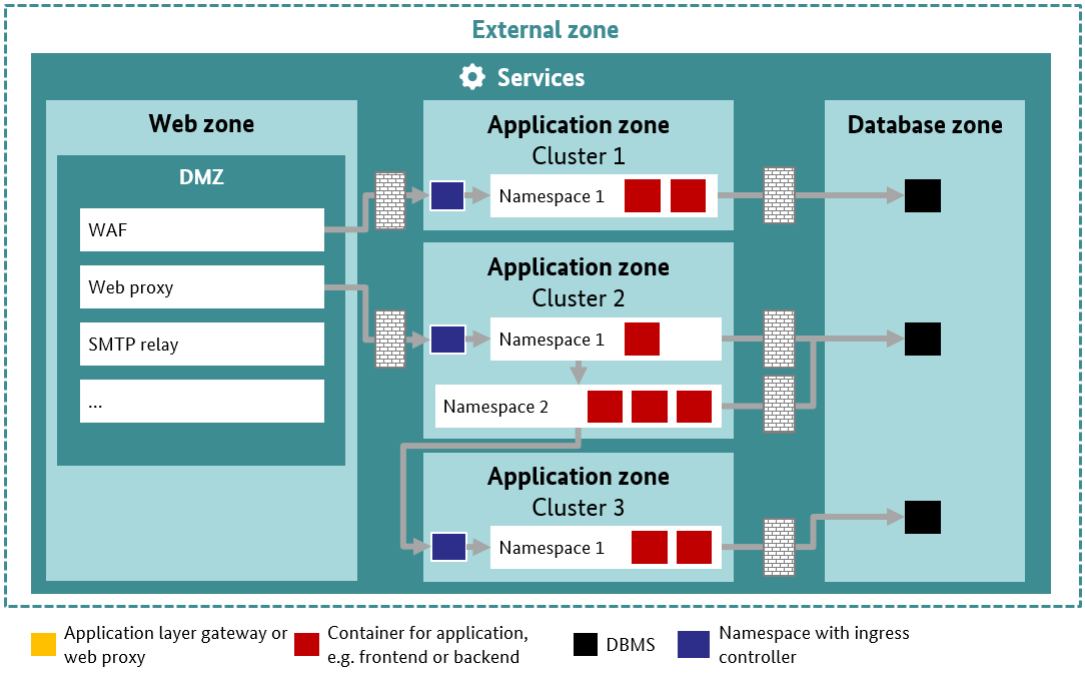

Figure 13: Arrangement of container clusters behind a traditional P-A-P structure (for illustrative purposes)

Applications within a cluster are separated using namespaces. Ingress controllers are operated in separate namespaces in this connection. Within the clusters, all applications must reach the same level of protection respectively. The distribution of application containers in the cluster is not otherwise regulated; this must then be planned according to the security concepts of the relevant applications.

Additional requirements that apply to the platform operator were developed to supplement the aforementioned division of the container clusters. Various IT baseline protection modules (including *SYS.1.6*: Containerisation[65] and *APP.4.4:* Kubernetes[66]) were used for this purpose:

- The platform operator SHOULD provide a separate IP address at the ingress for each externally exposed service. It should be possible to distinguish between different externally exposed services on the basis of IP addressing in order to streamline protective measures outside the Kubernetes environment.
- If multiple applications are published via the ingress, each application SHOULD have a separate IP address.
- It MUST be possible to access the applications via DNS.
- The ingress MUST be separated from other functionalities.
- The platform operator MUST use secure tunnel protocols for communication between the nodes of the Kubernetes cluster.
- The platform operator MUST restrict communication to the required communication paths, including nodes, communication protocols and ports, which are required for implementation and operation of the cluster and its nodes.
- The platform operator MUST ensure that user workloads can never share (system) namespaces with the host.
- The platform operator MUST ensure isolation of the containers through suitable permissions for resources and kernel functions.

---

[65] See https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/07_SYS_IT_Systeme/SYS_1_6_Containerisierung_Edition_2022.html

[66] See https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_4_4_Kubernetes_Edition_2022.pdf

- The platform operator MUST ensure that master nodes are not allowed to run user workloads.
- The platform operator MUST operate the development environment and the production environment in different Kubernetes clusters.
- The platform operator MUST separate the control plane from the worker nodes.
- The platform operator MUST operate specialised procedures with different protection needs in separate container clusters.

The delivery of software solutions for the container clusters that are provided is an important interface in the context of interactions between the software operator and the platform operator. It is of fundamental importance for secure operational execution and the implementation of measures that guarantee IT security. The following minimum requirements must therefore be met in this area:

- The platform operator MUST provide a container registry for the provision of software solutions for implementation in the container environment.
- The software operator MUST define a target state that can be rolled out on an automated basis by the platform operator.
- The platform operator MUST ensure that an automated vulnerability scan can be executed and that its results can be viewed by the software operator. As part of this process, the platform operator MUST immediately notify the software operator of critical vulnerabilities.
- The platform operator MUST ensure provision of the guaranteed resources and rollout of the supplied target states, provided that the integrity of the environment is not jeopardised.
- The platform operator MUST roll out containers on an automated basis for troubleshooting, in line with the agreed service level agreements (SLAs), and for scaling. If the container runtime is limited, the platform operator MUST forward the incident to the software operator for troubleshooting.
- The platform operator MUST ensure that deployment planning in the context of a change can be controlled and documented. In addition, the platform operator MUST ensure that

the change can be initiated at least via the cloud service portal using interfaces; the initiation MAY be supported on an automated basis via a pipeline.

- The software operator MAY use its own CI/CD pipeline. In this case, the platform operator provides suitable handover points.

5.4.5 Development area

A cloud location can support decentralised software development by providing various extensions separately from the production environment. No mandatory standards are prescribed in this area because of the large number of tools and the rapid rate of innovation (see Chapter 5.3). In the context of provision, however, it is necessary to guarantee compatibility with Germany's government cloud, to ensure compliance with the information security and data protection specifications[67] and the architecture guidelines that apply in this connection (see Chapter 2.3.2) and to support a satisfactory roles and rights management system. In particular, development areas must facilitate a connection to the central OS platform for the public administration (Open CoDE).

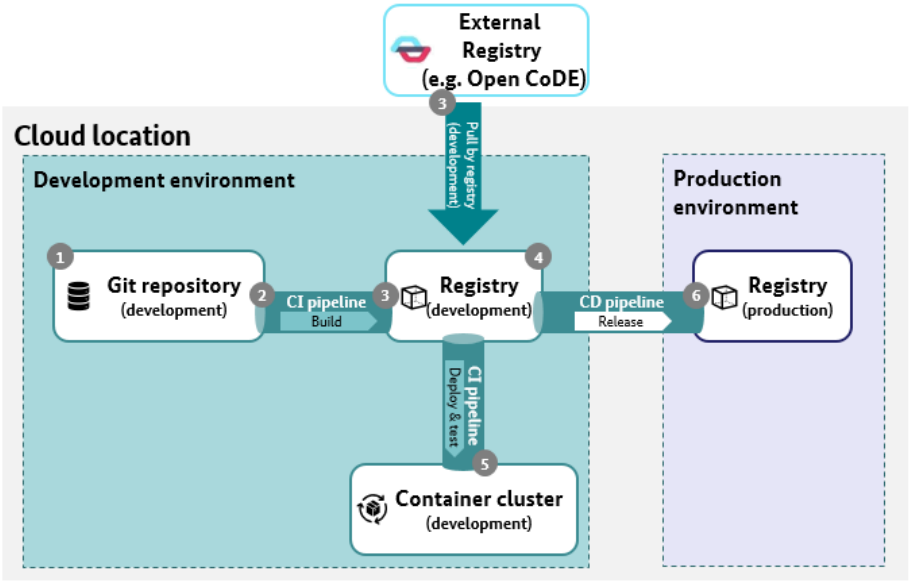

Figure 14: Development area and CI/CD pipeline

[67] Through the strict separation of development and production environments, for example.

A cloud service and software solution development approach that involves a high level of automation is a vital aspect of modern IT infrastructure. A standardised workflow has therefore been developed for the continuous integration or continuous deployment process (CI/CD pipeline), which is outlined in Figure 14 and is structured as follows:

1. Source code check-in in the Git repository in the development environment provided at the cloud location.
2. Automated (time-controlled) or manual triggering of the process for building the new artifact or image.
3. Check-in or push of the new artifact or image in the development environment's registry. In the event that an artifact or image is made available by an external registry (e.g. by the OS platform for the public administration (Open CoDE) or by another vendor), the new version is accessed through a pull by the development environment's registry. If the external registry does not support this process, the new artifact or image can alternatively be pushed from the external registry to the development environment's registry. More in-depth descriptions of this process will be provided in the relevant detailed standard.
4. Vulnerability scan of the new artifact or image in the development environment's registry.
5. Deployment and testing of the new artifact or image from the registry in the cluster of the development environment.
6. Following successful deployment and test: generation of a change by the software operator to the platform operator and subsequent automated or manual triggering of the release rollout for the new artifact or image and handover of the artifact or image to the production environment's registries.

The aforementioned change for triggering the release can be confirmed on a manual or automated basis, and triggers the execution of the CD pipeline as a result. Automatic confirmations are, however, possible only in the case of standard changes (see Glossary). By way of derogation from Figure 14, the registries of the development and production environment can also be operated in one system only. This presupposes that the appropriate arrangements have been made for a logical separation between the development and production environments. More in-depth specifications will be provided in a corresponding detailed standard.

The following requirements are defined for the CI/CD process:

- The platform operator MUST provide a Git repository at the cloud location. This may also be an external repository.
- The platform operator MUST ensure that the pipeline supports at least the use of systems for Git-based source code management and access to systems for build creation.
- A registry MUST be provided at the cloud location for the delivery of artifacts and images in the development area. An additional registry SHOULD be set up for the storage of productive deployments.
- The platform operator MUST ensure that images and description files for target states can be delivered at the registry.
- The platform operator MUST ensure that the software operator is able to track changes to its images and files.
- The registry for the development environment provided by the platform operator MUST be able to mirror external registries on the basis of pull requirements. This requirement will be examined in greater depth in the relevant detailed standard.
- The registry provided by the platform operator for the development environment MAY support push requirements of external registries.
- The registry provided by the platform operator MUST be able to support the storage of images, configuration files, Helm charts and additional deployment files. The storage of a complete deployment MUST be allowed.
- The registry provided by the platform operator MUST allow the signature of artifacts and images to be checked.
- In the event of version updates, it MUST be possible for vulnerability scans to be carried out in the development environment. The vulnerability scan MUST be triggered by the registry. Cyclical and at least daily vulnerability scans MUST be supported. It MUST be possible for the responsible members of staff at the software operator to be informed by email about any vulnerabilities that have been identified. The vulnerability scan will be defined in greater depth in the relevant detailed standard.
- It MUST be possible for versions of artifacts and images to be tagged clearly.

- It MUST be possible for the CI/CD pipeline to be configured in such a way that the provision of the artifacts and images created for a repository is supported for rollout in a test environment.
- The platform operator MAY provide interfaces at its cloud location for webhooks, etc. so that the pipeline can be controlled by external development environments.
- The release of an artifact or image for the production environment MUST be documented with a change.
- The platform operator MUST ensure that artifacts and images are handed over via separate repositories in order to ensure a strict separation between development and productive operation. The platform operator SHOULD use separate registries for development and productive operation.
- The platform operator MUST ensure that the separation of the CI pipeline from the continuous delivery pipeline complies with the requirements laid down in Chapter 5.4.3.
- The platform operator MAY provide tools for code quality checks and security tests.
- The platform operator MAY provide a ticketing system to support software development.

The technically and organisationally secure design of processes must be ensured throughout the entire CI/CD pipeline. Further details will be provided in the relevant detailed standards.

5.4.6 Communication between the cloud location, software operator and cloud service portal

It is necessary for data to be exchanged on a regular and direct basis between the cloud service portal (Chapter 5.5) and the cloud service providers. The relevant APIs required for this purpose must be provided by all parties. The data to be communicated between the parties involved include the following:

- information on the commissioning, alteration and cancellation of cloud services;
- information on the creation of incidents and changes and the relevant status changes;
- billing data; and
- availability reports on the cloud services for monitoring purposes.

The cloud service portal will not provide a full ticketing system; it will, however, offer an interface to the ticketing systems of the cloud service providers, cloud service brokers and cloud service customers in order to facilitate the receipt and management of tickets. The end-to-end nature of the support process must be retained in this connection; in other words, the parties involved in each case should be able to connect their ticketing systems and continue using them. The transparency of the current status between the cloud service portal and the cloud location or software operator must always be maintained during this process and in respect of the aforementioned data, i.e. the same information must always be available to all parties.

Further particulars of the communication relations between the cloud service portal and the platform or software operators, cloud integrators and cloud location, as well as the technical details, will be provided in the relevant detailed standards.

5.5 Standards for the cloud service portal

Germany's government cloud is intended to serve as a central self-service portal for the entire public administration; it will take the form of a web-based solution that makes it possible to advertise, register, search for, commission, adapt and cancel cloud services (e.g. based on the service models IaaS, PaaS including CaaS, and SaaS) in a multi-cloud context. The cloud service providers will be connected to the cloud service portal by means of uniform technical interfaces in order to facilitate a consistently high level of automation, and it will be mandatory for each cloud location to establish these interfaces.

The portal will act as a central entry point for employees of the contracting authority or software operator and must be accessible via the administration network between the Federal Government and the federal states (Networks of the Federal Government – Interconnecting Network), and from the internet. Cloud service providers can determine in each case whether the service is to be visible and accessible from the internet or from the administration networks. Development areas can be accessible from the internet, for example, whereas specialised procedures will only be offered within the administration networks.

A navigable service catalogue listing and describing the services will be created for users of the cloud service portal. It will contain clearly defined attributes for each service that provide more detailed information about that service. Long-term compatibility with Gaia-X and the federated

catalogue[68] is to be guaranteed, and it will be necessary for the descriptions of the services offered to meet a minimum standard. The following key characteristics have been specified as attributes for the purposes of the service catalogue:

- name and brief description of the service;
- information about the provider (e.g. number and location of data centres, references and certifications/attestations);
- version of the service (including period of validity/support period, version history);
- scope of delivery;
- price per unit;
- dependencies with other services;
- protection needs and confidentiality levels[69] supported from the operator's perspective;
- zone for provision (external zone, internal zone, zone with increased protection needs (e.g. classified information zone, for confidentiality requirements));
- list of all sub-service providers and subcontractors involved in providing the service;
- billing arrangements and purchase volumes;
- SLA (including operating hours, response times and recovery times, service classes and service times for the service);
- arrangements for change requests and for the service desk; and
- reporting.

Further additions are possible at the detailed planning stage.

A wide range of functions that simplify the management of various services will be made available to the users of the cloud service portal. For the purpose of managing users of the cloud service

[68] The federated catalogue standardises the description of services in the context of the Gaia-X project by means of uniform attributes. The goal is therefore to achieve the highest possible level of commonality with the service catalogue for Germany's government cloud.

[69] Each service catalogue entry will be assigned a "normal" protection need. If a "high" protection need is supported, the characteristics must be described (encrypted data storage with persistent memory, for example).

portal, it is envisaged that it will be possible to create both entities and sub-entities, as well as users with different permissions, following a registration procedure. It is also planned that billing information and links to service monitoring tools, for example, will be available on the cloud service portal. All functional and non-functional requirements will be examined in the future detailed conceptual design of the cloud service portal. These will also include the procedure to be followed when logging and handling incidents, when responding to change requests and when implementing service changes, as well as when a cloud service provider rolls out a new software version or an altered service.

The software operator will also be responsible for licensing in collaboration with the platform operator, although the platform operator must have a right of veto which it can use in cases where the software operator wishes to use licenses that jeopardise the license conformity of the platform operator's cloud location. The platform operator should therefore ensure that the services it offers are licensed, document the licenses used in the service catalogue accordingly and provide information on the conditions for use. The software operator will then be responsible for licensing the software solution components deployed that use the platform operator's services. Plans exist to publish a separate document outlining the detailed implementation of responsibilities and procedures in connection with license management.

The detailed concept for the cloud service portal was at the drafting stage at the time when this framework was updated. It is planned that the continuous further development of Germany's government cloud will also encompass regular further development of the cloud service portal. The coordination body (yet to be established) will be responsible for the associated task of recording new functional and non-functional requirements (see task document for the coordination body and Chapter 6.1).

6 Next steps and operationalisation of Germany's government cloud

This chapter describes the next steps to be taken in relation to the design of Germany's government cloud. Additional work already done in connection with the conceptual design and implementation of Germany's government cloud is also outlined.

Information on the progress made in regard to the individual lines of action and the associated operationalisation of Germany's government cloud, in particular as regards updates to the standards, will be provided to the IT Planning Council on a regular basis.

6.1 Conceptual design of the coordination body for Germany's government cloud

At some stage in the future, the Sub-Working Group on Technology and Operations will assign substantive responsibility for Germany's government cloud (including the creation and updating of concepts) to a coordination body that is yet to be specified. It is envisaged that this coordination body for Germany's government cloud will be responsible for the cloud service portal and, among other things, will cover the financing needs for its development and operation. The entity will also be responsible for updating the service catalogue, and will coordinate the continuous updating of the catalogue by the platform and software operators. In addition, the coordination body is to be assigned the task of checking and enforcing compliance with the standards.[70]

It is envisaged that the coordination body will essentially act as a broker between the cloud service providers and cloud service brokers or cloud service customers and oversee and coordinate their participation in Germany's government cloud. It is planned that it will also be authorised to exclude individual entities from Germany's government cloud if necessary (if there is a possibility that information security might be compromised, for example). A detailed description of the tasks

[70] See https://www.it-planungsrat.de/fileadmin/beschluesse/2022/Beschluss2022-35_Aufgaben.pdf

of the coordination body is available in the document "Governance of the Coordination Body for Germany's Government Cloud".[71]

In addition to the coordination body, plans exist to set up an architecture board which will take action on a regular basis in future to bring the standards of Germany's government cloud into line with legislative amendments and technological trends/further developments.[72]

6.2 Execution of pilot projects

Based on the standards for Germany's government cloud as defined in Chapter 5, a proof of concept (PoC) was carried out with a view to piloting implementation, during which key standards for Germany's government cloud were trialled in practice. The first PoC for Germany's government cloud was carried out between 1 July 2021 and 14 January 2022. One of its goals was to verify the basic principle of Germany's government cloud, namely the standardised operation of software containers at different cloud locations throughout Germany. This goal was achieved; existing defined standards for Germany's government cloud have already been converted into machine-readable guidelines ("policies") and applied to container clusters at eight different data centres in Germany and Austria. Compliance with the policies was verified using conformity tests, and several OS applications were provided in compliance with the policies at the various cloud locations. In addition, further outcomes were taken into account during the ongoing process of developing the standards for Germany's government cloud further and fleshing out their details, and incorporated into the present document (the first update of the framework).[73]

During the first PoC, a new model of cooperation between the participating service providers of public administration IT emerged, which also encompasses in particular the joint work on projects on the OS platform for the public administration (Open CoDE). The ongoing implementation of Germany's government cloud is progressing within the framework of PoC 2.0 for Germany's government cloud, on the basis of this cooperation and the outcomes of the first PoC for

---

[71] See https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-rat/beschluesse/beschluss_2023_03_DVS_Anlage_Rahmenkonzept.pdf?__blob=publicationFile&v=3

[72] See https://www.it-planungsrat.de/beschluss/beschluss-2023-09-al - "Concept for the Architecture Board of Germany's Government Cloud".

[73] A detailed results document for the first PoC for Germany's government cloud is available at https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/220420_PoC-Ergebnisdokument_Langfassung_AG_Cloud_vf.pdf

Germany's government cloud. The key goals for PoC 2.0 for Germany's government cloud, which took place in 2022, were as follows:

- completion of work to define the technological basis for the provision of development and container environments within Germany's government cloud;
- qualification of the service providers of public administration IT to offer the first services that comply with the standards for Germany's government cloud;
- continued establishment of active cooperation between the service providers of public administration IT in OS projects; and
- definition of standardised requirements imposed on software vendors in connection with the delivery of container solutions.

With PoC 3.0, which is to take place in 2023, cooperation with the service providers of public administration IT is to be reinforced and the results of the first and second PoCs for Germany's government cloud are to be optimised and further developed in view of the implementation project for Germany's government cloud.

The following work packages will be implemented in PoC 3.0:

- image signatures and signed commits;
- continuation of policy development;
- continuation of development of pilot deployments into deployments in line with the standard for Germany's government cloud;
- framework for compiling images that are compliant with Germany's government cloud on Open CoDE: security & licensing;
- provision of KaaS products in the cloud service portal that provide the option of switching vendor;
- development of detailed standards and preliminary work for IT baseline protection modules or user-defined modules for the Kubernetes environments in Germany's government cloud;
- continuation of identity and access management (IAM);
- standardised process with Open CoDE: security & licensing;
- governance for work with documents / knowledge management; and

- trials of cloud service integration.

6.3 Implementation project for Germany's government cloud

It was noted in the minutes of the 41st meeting of the IT Planning Council that the implementation of the government cloud strategy for Germany was to be adopted.[74] The implementation of Germany's government cloud was to be promoted by the Federation and certain federal states, and was to be supported by the FITKO (the body for federal IT cooperation), the govdigital alliance, and relevant IT service providers.

The core objective of the time-restricted implementation project is to bring Germany's government cloud, with the associated infrastructure and bodies, into production as soon as possible. At the same time, the project aims to bridge the time until the FITKO can take on the central role of the coordination body.

Work will begin on creating the structure of Germany's government cloud and the coordination body of the government cloud when the implementation project starts. The coordination body is to be responsible for the cloud service portal and is to take on additional organisational tasks for Germany's government cloud.

6.4 Processing data classified as VS-NfD (restricted)

In the future, Germany's government cloud aims to provide cloud services that can process data classified up to the level of VS-NfD. If a federal authority or federal institution under public law (service) wishes to use a cloud service to process data up to the level of VS-NfD, this is subject to additional requirements in accordance with the General Administrative Regulation on Physical Security (*Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz*, VSA) for both the IT service provider and for the authority which is the customer.

Both the operator and the authority which is the customer must authorise their IT systems for use with and processing of classified information in accordance with section 50 of the General Administrative Regulation on Physical Security. According to section 50 (5) of the General Administrative Regulation on Physical Security, one operator (either the IT service provider

[74] See https://www.it-planungsrat.de/beschluss/beschluss-2023-19

themselves, if this is a service, or another body, in the case of an IT service provider under private law) takes on responsibility for the overall authorisation of the IT system for classified information as one of its key roles.

A uniform level of information security and confidentiality must also be ensured when federal states and municipalities are involved; the advice given by the relevant body is therefore to consider the General Administrative Regulation on Physical Security of the Federation as binding for all those involved.

7 Annex

7.1 Definition of the requirement levels for the standards

Each standard for cloud locations has a requirement level which is expressed in the form of a modal verb and which serves as guidance for implementation. The definitions below are specified in accordance with RFC 2119[75] (Key words for use in RFCs to Indicate Requirement Levels). RFC 2119 is also used in the BSI's[76] *IT-Grundschutz* Compendium and the Federal Government's IT Architecture Guideline.[77]

MUST – this word means that the requirement must absolutely be met (unrestricted requirement/binding specification).

SHOULD – this word means that a requirement must normally be met, but that there may be reasons to ignore it; this must be carefully weighed up and sound reasons provided.

MAY – this word means that an item is a permitted option.

MUST NOT – this phrase means that something must not be done under any circumstances (unrestricted prohibition).

[75] Request for Comments, see https://datatracker.ietf.org/doc/html/rfc2119

[76] See https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6

[77] See https://www.cio.bund.de/SharedDocs/kurzmeldungen/Webs/CIO/DE/startseite/2022/09_architekturrichtlinie.html

7.2 Glossary

The following glossary is intended to standardise usage of the most important terms, and includes terms of particular relevance to this document:

- **Application level gateway** – an "application level gateway" (ALG) offers the functionality of a security gateway at the application level. ALGs also implicitly perform functions located in ISO/OSI Layers 1 through 3. ALGs, also referred to as security proxies, cut off the direct flow of data between the source and the destination. When a client on one side of the proxy and a server on the other side of a proxy communicate, the proxy receives the requests from the client and forwards them to the server. The proxy operates in the same manner with data flowing in the other direction, i.e. from the server to the client. In this case, communication between the two computers is only possible indirectly via the proxy. This form of communication allows a proxy to filter out certain protocol commands, for example.
- **Architecture board** – (future) body that is primarily responsible for the (further) development of existing and new standards for Germany's government cloud and that exists independently of the coordination body.
- **Audit system** – an audit is carried out to investigate whether processes, requirements and guidelines meet the necessary standards. The audit system ensures that audits can be carried out with the highest possible level of automation.
- **Change** – a modification or update to an IT solution.
- **Cloud computing** – the term "cloud computing" refers to the process of offering, using and billing IT services that are dynamically adapted to the customer's requirements via a network. These services are only offered and used by means of defined technical interfaces and protocols. The range of the services offered within the cloud computing framework covers the entire spectrum of information technology, including infrastructure (e.g. computing power, storage space), platforms and software (definition in line with the BSI[78]).

[78] See https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html

- **Cloud integrators** – service providers of public administration IT that configure the services offered by cloud providers outside the administration to be compatible with the standards of Germany's government cloud, and therefore make them available for Germany's government cloud on a legally compliant basis.
- **Cloud location** – the term cloud location refers to the data centres operated at Federal Government, federal state and municipality level and by their IT service providers that provide IT infrastructure and make available computing capacities within Germany's government cloud. It is not necessary for the whole infrastructure of the data centres to form part of Germany's government cloud; sub-areas may also be used.
- **Cloud service portal** – the future central port of call for the public administration and its IT service providers for managing cloud services. It is intended to allow its users to order and cancel cloud services, for example IaaS or SaaS services, and to access information on the cloud services that are provided. A detailed concept for the cloud service portal is currently being produced.
- **Code repository** – the central management environment in software development for the versioning of source code, including a documentation function.
- **Compliance** – the term "compliance" means ensuring that actions are carried out in accordance with laws and guidelines.
- **Container as a service** – container as a service (CaaS) is a form of container-based virtualisation that provides the runtime environment, orchestration tools and underlying infrastructure resources through a cloud computing provider (definition in line with IONOS[79]).
- **Container cluster** – in Kubernetes, clusters are computer networks responsible for operating containerised software solutions.
- **Container environment** – a technical platform for the operation and management of container clusters (examples of the relevant technologies are OpenShift and Rancher). The container environments considered in this context are based on the Kubernetes standard.

[79] See https://www.ionos.de/digitalguide/server/knowhow/caas-container-as-a-service-anbieter-im-vergleich/

- **(Container) image** – a file with executable code that can generate a container. It is a packaged application that still contains the software modules necessary for the application. Container images are immutable and can be deployed in any container or system environment.
- **Containerisation** – the packaging of software code into packages that contain all of the required components, such as libraries, frameworks and other dependencies, and that are isolated in their own containers.
- **Continuous deployment** – a software development approach in which changes to the software are released into the current software or into production on an automated basis in line with fixed criteria. This allows continuous delivery of the software.
- **Continuous integration** – a software development approach in which new program parts are tested and merged immediately instead of only once a day, for example.
- **Crypto module** – the term "crypto module" refers to a product that offers the security function specified in a given crypto concept. Such products may consist of hardware, software, firmware, or a combination thereof. In addition, components such as memory, processors, buses, and power supplies are necessary to implement crypto processes. A crypto module may be used in a wide variety of IT or telecommunication systems in order to protect sensitive data and information (definition in line with BSI[80]).
- **Demilitarised zone** – a specially monitored network that is placed between the external network (internet) and the internal network. It serves as a buffer zone of sorts, enforcing strict communication rules and firewalls to separate the networks from each other.
- **Deployment** – the provision of software for installation and configuration on PCs and servers using semi-automated or fully automated processes.

[80] See https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_1_Kryptokonzept_Edition_2021.pdf?__blob=publicationFile&v=2

- **DevOps approach** – an approach that involves combining the development, quality assurance and operation of IT systems and solutions.
- **Digital sovereignty** – the abilities and opportunities of individuals and institutions to perform their role(s) in the digital world in an independent, self-determined and secure fashion (definition in line with the Competence Centre for Public IT[81]).
- **Emergency changes** – changes that must be implemented immediately, for example to resolve a major incident (definition in line with ITIL[82]).
- **Firewall** – a firewall is a system consisting of software and hardware components that is used to securely connect IP-based data networks (definition in line with the BSI[83]).
- **Germany's government cloud** – the standardised, federal cloud infrastructure of the Federal Government, federal states and municipalities on the basis of the government cloud strategy adopted by Germany. Germany's government cloud is to be considered separately from Germany's government cloud strategy.

  The strategy applies specifically to long-term, strategic topics. Topics related to the immediate implementation of Germany's government cloud strategy are referred to simply as Germany's government cloud. Since March 2023, the Sub-Working Group on Technology and Operations has applied the policy that, when in doubt, reference should be made to Germany's government cloud rather than Germany's government cloud strategy.
- **Germany's government cloud strategy** – strategy intended to introduce common standards and open interfaces for public administration cloud solutions as a means of establishing an interoperable and modular federal cloud infrastructure across the board. The primary goal of Germany's government cloud strategy is to provide the option of using cloud services and software solutions on a multi-cloud or multi-location and reciprocal basis; the standardised, modular IT architectures aim to reduce critical dependencies on

[81] See https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souveränität

[82] See https://wiki.de.it-processmaps.com/index.php/Change_Management

[83] See https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.pdf?__blob=publicationFile&v=2

individual vendors. The term applies specifically to long-term, strategic topics. Topics related to the immediate implementation of Germany's government cloud strategy are referred to simply as Germany's government cloud. Since March 2023, the Sub-Working Group on Technology and Operations has applied the policy that, when in doubt, reference should be made to Germany's government cloud rather than Germany's government cloud strategy.

- **Helm charts** – the packaging format of the package manager, consisting of a collection of data and instructions describing the Kubernetes resources and dependencies of the specific Kubernetes applications.[84]
- **Incident** – a security incident or malfunction of an IT solution.
- **Kubernetes master** – a Kubernetes cluster is based on a set of machines. These are divided into master nodes and worker nodes. The Kubernetes master consists of three processes that are run on a single node in its cluster, referred to as the master node.
- **Kubernetes worker** – a Kubernetes cluster is based on a set of machines. These are divided into masters and workers. The workers provide the resources for executing the container applications. Each cluster must include at least one worker.
- **Messaging** – software that facilitates text-based or character-based communication in real time.
- **Multi-cloud** – the use of multiple cloud services from various cloud service providers in a single heterogeneous architecture by a cloud service customer.
- **Namespace** – a virtual cluster within a Kubernetes cluster. In the context of Kubernetes, namespaces are a mechanism for isolating resource groups within a cluster. More generally, namespaces are used for grouping or structuring in the field of information technology.
- **Normal changes** – all changes that are not standard changes or emergency changes (definition in line with ITIL[85]).

[84] See https://www.cloudcomputing-insider.de/was-ist-helm-a-921110/

[85] See https://wiki.de.it-processmaps.com/index.php/Change_Management

- **Open source and open source software** – solutions that are generally licensed for use, adaptation and circulation free of charge, and for which the source code of the software is made publicly available.
- **OS platform for the public administration (Open CoDE)** – (internet) platform for the public administration that consists of a central and searchable directory of open source projects relevant to the administration, a code repository allowing the storage of open source code and participation in projects, as well as a discussion forum. The code repository is a standardisation area of Germany's government cloud and is intended to facilitate the central storage and mirroring as well as reuse of source code, together with its documentation.
- **Packet filters** – software programs allowing simpler firewall concepts for the selection of digital signals.[86]
- **P-A-P structure** – "packet filter – application level gateway – packet filter", which is the BSI's recommendation for a three-stage firewall or security gateway system.
- **Pipeline** – the CI/CD pipeline is used to execute automation steps for the provision of new software versions.
- **Platform operator** – the platform operator operates the IT infrastructure at the cloud location and provides the software operator with tools for manual and/or automated orchestration.
- **Public administration information network** – this is an information network that is to be established among Federal, state and municipal institutions and the providers of IT applications. The Federal Agency for Public Safety Digital Radio plays the role of central network operator in the information network, and also provides the network-related services.

[86] See https://www.itwissen.info/Paketfilter-packet-filter-PF.html

- **Security gateway** – a security gateway (often also referred to as a firewall) is a system made up of software and hardware components. It ensures the secure coupling of IP networks by restricting the communications that are technically possible to those defined in a security guideline as appropriate. In this network coupling context, security primarily means that only the intended accesses or data flows between different networks are permitted and that the data transferred are monitored (definition in line with the BSI[87]).
- **Security information and event management (SIEM)** – real-time monitoring and analysis of events, as well as tracking and logging of security data, for compliance or auditing purposes.
- **Service level agreement** – an agreement concluded between the vendor and the customer for quality assurance purposes. The exact performance features and quality grades (service levels) for the product or the service are specified in this agreement.
- **Service orchestration** – the term "orchestration" refers to the automated configuration, management and coordination of computer systems, software solutions and services. In the context of container environments, it refers in particular to the ability to control when containers start and stop, to group containers in clusters, and to coordinate all the processes that constitute a software solution.
- **Service provider of public administration IT** – these are companies, entities or other legal persons that provide IT services for institutions, authorities or governmental organisations and are controlled by the public administration in doing so. This is implemented either through government participation or supervision by public authorities.
- **Simple Mail Transfer Protocol (SMTP) relay** – standard network protocol for sending and relaying e-mails on the internet.[88]
- **Software operator** – as the contractor, the software operator is responsible towards the contracting authority for operating a software solution on the basis of contractual obligations, and manages service orchestration. If possible, the software operator

[87] See https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/S/Sicherheitsgateway.html

[88] See https://www.ionos.at/digitalguide/e-mail/e-mail-technik/smtp-relay/

coordinates the requirements for software operation with the software vendor. It acts as the connecting link between the platform operator and the software vendor.

- **Software vendor** – the software vendor is an entity (in the sense of a legal person) or a loosely connected community (group of developers) that provides the software operator with software (releases).
- **Software solution** – a software solution is application software for a specific defined task, providing a solution to a specific problem faced by a customer.
- **Source code / source text** – a text-based description of software that is readable by humans but written in a programming language. This text describes the software exactly and completely so that it can be translated into machine code by a computer on a fully automated basis.
- **Specialist procedure** – a specialist procedure is the specific technical implementation of an administrative process in one or several information systems. They may be used by one or several authorities internally, but may also permit the involvement of citizens, for example in an application procedure.
- **Standard changes** – pre-authorised, low-risk changes that follow a well-known procedure (definition in line with ITIL[89]).
- **Virtual local area network** – a logical network created on a physical LAN.
- **Voice over IP** (VoIP) – telephone calls that take place via a broadband internet connection instead of the traditional analogue telephone connection, based on the conversion of voice signals and the transfer of these signals as data packages via an IP network.
- **Web proxy** – the web proxy acts as a gateway between a client, for example a web browser, and the application server. In addition to security functions, these proxy servers often also perform functions aimed at improving the I/O behaviour of the web application.
- **Workload** – in the computer environment, a workload is an individual task assigned to physical or virtual systems for processing.

[89] See https://wiki.de.it-processmaps.com/index.php/Change_Management

7.3 List of abbreviations

Abbreviation	English equivalent
ALG	**Application level gateway**
API	Application programming interface
BSI	Federal Office for Information Security
CaaS	Container as a service
CI/CD	Continuous integration/continuous delivery
DBMS	Database management system
IaaS	Infrastructure as a service
IAM	Identity and access management
IP	Internet protocol
IT	Information technology
IT-PLR	IT Planning Council
KaaS	Kubernetes as a service
MVP	Minimum viable product
NdB-VN	Netze des Bundes – Verbindungsetz (Networks of the Federal Government – Interconnecting Network)
ÖFIT	Competence Centre for Public IT
OS	Open source
OSCI	Online services computer interface
OSS	Open source software
OZG	Online Access Act
PaaS	Platform as a service

Abbreviation	English equivalent
PAP	Packet filter – application level gateway – packet filter
SaaS	Software as a service
SCS	Sovereign cloud stack
SIEM	Security information and event management
SLA	Service level agreement
SMTP	Simple Mail Transfer Protocol
VLAN	Virtual local area network
VPN	Virtual private network
VSA	Classified Information Instructions
VS-NfD	Information classified as *VS-Nur für den Dienstgebrauch* (restricted)