AUTONOMY TRACK · PRACTICAL GUIDE

A Practical Guide to Assessing Digital Sovereignty

25 questions for provider assessment.
With checklists and templates for informed decisions.

Andreas Heß

Founder of Autonomy Track

hello@autonomytrack.eu
+49 160 922 322 55
https://autonomytrack.com

© 2026 Andreas Heß. All rights reserved.

Free to print, complete and share within the same organisation for its own assessments and procurement. No sharing with third parties, further development or integration into other content or systems. Rights in your own entries and uses permitted by mandatory law remain unaffected.

Subject to the Autonomy Track Content Licence:

https://autonomytrack.com/autonomy-track-content-licence/

Contents

How This Guide Helps . . . 3

1. Digital sovereignty is not a yes-or-no attribute . . . 4

2. Why Evidence Is Essential . . . 5

3. The Five Dimensions . . . 6

4. How to Use This Guide . . . 6

5. Dimension A - Legal Framework & Control . . . 8

6. Dimension B - Data & Operations . . . 9

7. Dimension C - Technology & Supply Chain . . . 11

8. Dimension D - Portability & Provider Switching . . . 12

9. Dimension E - Evidence & Reliability . . . 13

10. From Findings to Decisions . . . 15

11. Example: One Platform, Two Use Cases . . . 16

12. Regulatory Context . . . 17

13. When should you reassess? . . . 18

14. The Most Important Rule . . . 18

Appendix A: 25-Question Checklist . . . 19

Appendix B: Evidence Checklist . . . 21

Appendix C: Decision Template . . . 22

Sources and Further Reading . . . 26

© 2026 Andreas Heß · Autonomy Track

How This Guide Helps

Digital sovereignty cannot reliably be assessed with a single question:

- Are the data held in Europe?
- Is the provider European?
- Is there an ISO certification?
- Can I export my data?

Each of these questions can be relevant. None is sufficient on its own.

What matters is whether an organisation can **identify** its technological dependencies, **substantiate** the key claims, **assess** the consequences for its specific use case, and **make and implement** an informed decision.

This guide helps with that process.

It is not a certification scheme, a provider ranking or legal advice. Nor does it replace a regulatory or risk-based assessment of an individual case. It offers a structured starting point for a question that is often addressed too abstractly in practice:

> **How dependent are we on a provider, and is that dependency acceptable for this specific use case?**

© 2026 Andreas Heß · Autonomy Track

1. Digital sovereignty is not a yes-or-no attribute

Digital sovereignty is often discussed in terms of origin, data centre location or data protection. These factors matter, but they form only part of the picture.

An organisation can store all its data in Germany and still depend heavily on:

- Proprietary APIs
- An identity platform that cannot be replaced
- Global administration or support structures
- A single technology or licence supplier
- Proprietary data formats
- A lack of expertise to switch
- A contract without robust provisions for provider switching
- An architecture that can be replicated outside the provider only with substantial effort

Conversely, a dependency is not automatically a problem.

A highly integrated platform service can deliver substantial functional and commercial value. For a less critical use case, deliberately accepting greater dependency may be a rational choice.

The better question is therefore not:

> Is the provider sovereign?

But:

> What dependencies exist, which are material to our use case, and what informed decision do we make about them?

© 2026 Andreas Heß · Autonomy Track

2. Why Evidence Is Essential

Sovereignty and security assessments often start with provider claims:

- “Data stays in the EU.”
- “Sovereign cloud in the EU.”
- “Customer-controlled encryption.”
- “Switch providers at any time.”
- “ISO 27001 certified.”
- “Audited against C5.”

These statements may be accurate and relevant. Initially, however, they are **provider claims**.

A sound decision requires at least four distinct levels of consideration:

Provider claim	What does the provider claim?
Evidence	What evidence supports the claim?
Reliability	How was the evidence produced, how current is it, and what conclusions can reliably be drawn from it?
Suitability for the use case	Does the evidence cover the relevant requirements, the service under review and the required period?

For example, a certificate may be valid and current but cover only a particular legal entity, region or part of the service.

An audit report may provide high-quality evidence without automatically covering all of an organisation’s requirements.

A contract may guarantee a data location without ensuring technical portability.

Therefore:

> **Do not simply check whether evidence exists. What matters is its relevance, currency and scope for the service under review.**

© 2026 Andreas Heß · Autonomy Track

3. The Five Dimensions

The guide structures the assessment around five dimensions:

1. **Legal framework & control**
2. **Data & operations**
3. **Technology & supply chain**
4. **Portability & provider switching**
5. **Evidence & reliability**

These five dimensions are deliberately practical.

They do not replace regulatory frameworks. The European Commission's Cloud Sovereignty Framework, for example, uses 48 criteria across eight sovereignty areas. The approach used here gives organisations an accessible starting point and prepares the ground for an informed technology decision.

4. How to Use This Guide

Step 1 - Define the scope

Do not assess "the provider" in the abstract.

First define:

- Which service or product you are considering
- Which legal entity is the contracting party
- Which internal processes depend on it
- How critical the use case is
- Which data are processed
- Which countries and jurisdictions are relevant
- Which regulatory or internal requirements apply
- When the contract is renewed or a new decision is due

The same provider may lead to different decisions for two different use cases.

Step 2 - Answer the questions

Work through the 25 questions in this guide.

© 2026 Andreas Heß · Autonomy Track

Step 3 - Link the evidence

For each relevant question, assess the evidence as well as the answer.

Use four evidence statuses:

- **Verified** - sufficient, current evidence is available.
- **Partially verified** - evidence exists but is incomplete, outdated or not fully relevant.
- **Unknown** - sufficient evidence is not available.
- **Not applicable** - the question is demonstrably irrelevant to the defined scope.

Where reliable evidence is missing, the claim remains unconfirmed. Document the outstanding question, the evidence required, an owner and a deadline for clarification.

An evidence gap neither proves that a requirement is met nor automatically demonstrates a breach. For critical requirements, it may nevertheless justify deferring a decision or introducing interim safeguards.

“Verified” describes the evidential basis of a claim. A demonstrated weakness can also be verified. Whether the situation is acceptable is assessed separately afterwards.

Step 4 - Assess the significance of the impact

Ask:

> What would this finding mean for this particular use case?

First describe the specific consequences, such as operational interruption, data loss or additional switching costs. Then classify their severity as **low, medium, high or critical** and explain the rating. This does not replace a full risk assessment, which also considers likelihood and existing safeguards.

Step 5 - Make a decision

Record the decision and its rationale. Several options can be combined:

- Accept
- Reduce
- Limit the consequences
- Develop alternatives
- Renegotiate
- Migrate
- Replace
- Bring activities in-house

© 2026 Andreas Heß · Autonomy Track

5. Dimension A - Legal Framework & Control

A1 - Contracting Party and Ownership/Control Structure

Question: Can we identify the contracting entity, controlling companies and relevant ownership or control relationships?

Why it matters

The brand name is not the only relevant factor. Corporate structure and control influence, for example:

- Governing law
- Disclosure and production obligations
- Contract enforcement
- Strategic dependency
- Risks arising from a change of ownership

Possible Evidence

Contract / order form · Commercial or company register · Group structure · Provider's legal notice · Ownership information

A2 - Relevant Jurisdictions

Question: Which jurisdictions may materially affect the provider, service, administrative access or disclosure obligations?

Why it matters

Data storage location does not automatically establish which legal regimes may affect contracting parties, parent companies, support organisations, operators or subcontractors.

Possible Evidence

Contractual terms · Data protection agreement · Legal and transparency information · Corporate structure · Government request policies

A3 - Contractual Control and Change Rights

Question: Do our contracts provide sufficient rights concerning audits, material changes, the use of subcontractors, termination, data return and provider switching?

Why it matters

A technically available option is less reliable for critical requirements if it exists only as a marketing claim or is not secured contractually.

Possible Evidence

Master agreement · Data processing agreement · Service agreement · Audit clauses · Subcontractor clauses · Switching and transition clauses

© 2026 Andreas Heß · Autonomy Track

A4 - Critical Third Parties and Subcontractors

Question: Do we know the third parties and subcontractors without which the service could not operate as required?

Why it matters

A provider may itself depend on hyperscalers, network services, identity services, proprietary software, security services or outsourced operations.

Possible Evidence

List of subcontractors · Architecture · Supply chain documentation · List of critical subcontractors

A5 - Change of Control or Business Model

Question: What happens if the provider's ownership, control, critical subcontractors or strategic direction change?

Why it matters

An arrangement that is acceptable today may change materially following an acquisition, restructuring, outsourcing or a change in hosting model.

Possible Evidence

Change-of-ownership clauses · Notification rights · Special termination rights · Governance and accountability documentation

6. Dimension B - Data & Operations

B1 - Storage and Processing Locations

Question: Do we know where primary data, backups, logs, metadata and disaster recovery copies are stored or processed?

Why it matters

"Operated in Germany" or "Data stored in the EU" may refer to only part of the service.

In particular, check:

- Production data
- Backups
- Telemetry
- Logs
- Support data
- Metadata
- Disaster recovery copies

Possible Evidence

Data flow diagram · Architecture · Region documentation · Backup and disaster recovery documentation · Contractual commitments

B2 - Privileged Access and Support

Question: Who can access customer environments or data with privileged rights or for support purposes, from where and under which controls?

Why it matters

Operational access may be just as relevant to a sovereignty decision as storage location.

Possible Evidence

Identity and privileged access design · Support model · Role descriptions · Access logs · Emergency access procedures

B3 - Cryptographic Control

Question: Who controls the keys, and can the provider or an upstream party technically access plaintext?

Why it matters

“Encryption at rest” does not answer who controls the keys.

Possible Evidence

Key management and secure key storage architecture · Key management model · Technical documentation · Contractual commitments · Access control design

B4 - Operational Autonomy and Recovery

Question: Which people, technical control planes, external services and locations are required to operate and recover the service?

Why it matters

A service may store data in Europe while relying on global control planes, central support teams, irreplaceable third-party services or external licence servers for operations or recovery.

Possible Evidence

Operating model · Service architecture · Support locations · Business continuity and disaster recovery documentation · Dependency overview

B5 - Deletion, Retention and Operational Evidence

Question: Can the provider demonstrate retention and deletion transparently and provide sufficient operational evidence for material commitments?

Possible Evidence

Retention policy · Deletion process · Deletion confirmation · Audit logs · Change records · Security incident documentation

© 2026 Andreas Heß · Autonomy Track

7. Dimension C - Technology & Supply Chain

C1 - Proprietary Dependencies

Question: Which proprietary technologies, interfaces, data formats or managed services are required for the application to function?

Why it matters

Proprietary features are not inherently bad. They can reduce development time, improve security, increase scalability or simplify operations. They can also increase switching costs.

The aim is therefore not “no lock-in”, but **deliberately chosen lock-in**.

Possible Evidence

Architecture diagram · API inventory · Service catalogue · Dependency overview

C2 - Standards and Interoperability

Question: Which open, documented or widely supported standards and interfaces enable integration with other systems or replacement of a solution?

Possible Evidence

API documentation · Protocol/format documentation · Conformity statements · Technical tests

C3 - Upstream Technology Dependencies

Question: Which technology providers does the provider need to operate, update, patch or develop the service?

Why it matters

A European company may be heavily dependent on individual external platforms or software suppliers for its technology.

Possible Evidence

Technology architecture · Licence dependencies · Platform description · Software supply chain documentation

C4 - Portability of Configuration and Automation

Question: Can configurations, infrastructure definitions, policies and automation be reproduced outside the provider?

Why it matters

A full data export offers limited help if role models, workflows, infrastructure, policies and integrations must be rebuilt from scratch.

Possible Evidence

Infrastructure as code · Policy export · Configuration API · Automated deployment workflows · Operational runbooks

© 2026 Andreas Heß · Autonomy Track

C5 - Skills and Ecosystem

Question: Do we have, or can we realistically obtain, the capabilities and partners needed to operate an alternative?

Why it matters

A lack of expertise, staff or suitable service providers can also make switching difficult. A technically available alternative becomes usable only when operations and transition are supported organisationally.

Possible Evidence

Skills inventory · Partner/service provider market · Training needs · Operating model · Skills assessment for alternatives

8. Dimension D - Portability & Provider Switching

D1 - Complete Export

Question: Can all required data, metadata, configurations and relevant artefacts be exported in a usable, machine-readable form?

Why it matters

An export may appear to be available yet omit relationships, versions, audit data, permissions, metadata or configuration.

Possible Evidence

Export documentation · Test export · Format specification · APIs · Migration tools

D2 - Switching Process and Support

Question: Is there a documented switching process covering timelines, responsibilities, support, data retention and known costs?

Possible Evidence

Contract · Exit plan · Switching assistance clauses · Retention and deletion rules · Price lists

D3 - Realistic Target Option

Question: Is there at least one realistic alternative provider, architecture or in-house solution?

Why it matters

A contractual right to switch has little value if there is no realistic technical or organisational destination.

Possible Evidence

Target architecture · Comparison of alternative providers · Proof of concept · Compatibility analysis

© 2026 Andreas Heß · Autonomy Track

D4 - Effort and Operational Impact of Switching Providers

Question: Do we know the likely duration, costs, skills, operational interruptions, data transfer effort and operational risks of switching providers?

Why it matters

Material dependency often becomes apparent in the actual costs of switching.

Possible Evidence

Effort estimate · Cost model · Data volume/network calculation · Resource plan · Migration runbook

D5 - Tested Provider Switching

Question: Have export, recovery, failover or migration been tested and documented in a scenario relevant to switching providers?

Why it matters

Documentation or an export function alone does not demonstrate a successful switch. Record which part of the transition was actually tested, the result and the steps still outstanding.

Possible Evidence

Test report · Review and improvements · Operational runbook · Migration log · Action list

9. Dimension E - Evidence & Reliability

E1 - Evidence for Critical Claims

Question: Is there current evidence for every claim that materially influences our decision?

Why it matters

A completed questionnaire is not yet a verified fact.

Classify material claims as:

- Provider claim
- Contractual commitment
- Technical evidence
- Independent audits
- Own test

E2 - Scope of Independent Audits

Question: What audits, attestations or certifications exist, and do the legal entity, service, region, period and scope match our use case?

Possible Evidence

Certificate, including scope · C5 report/attestation · SOC report · Statement from the auditor · Accreditation information

© 2026 Andreas Heß · Autonomy Track

E3 - Contract and Marketing

Question: Are material commitments on location, access, portability, transition and control adequately reflected in the contract?

Why it matters

A product page can change. Critical requirements need more robust safeguards.

E4 - Currency and Change Notifications

Question: Do we know how old the evidence is, when it will be renewed and how we will learn about material changes?

Possible Evidence

Reporting period · Certificate validity · Change log · Notification clause · Review record

E5 - Evidence Gaps and Accountability

Question: Are unknowns documented with an owner, a next step and a review date?

Why it matters

Outstanding evidence questions need an owner and a next step. Otherwise, a provisional assumption can quietly become the basis for a decision.

© 2026 Andreas Heß · Autonomy Track

10. From Findings to Decisions

Choose the action that fits the dependencies identified, their consequences and the available alternatives. Document the rationale, residual risks, responsibilities and a review date. Several options can be combined.

Accept	Deliberately accept a known dependency where the benefits and effort justify it and mandatory requirements remain satisfied. Document the rationale and review the decision regularly.
Reduce	Reduce the dependency deliberately, for example through open interfaces, exportable configurations or stronger in-house expertise.
Limit the consequences	The dependency remains. Backups, recovery procedures or additional controls limit potential harm.
Develop alternatives	Additional providers, available capacity or in-house expertise create options. Check whether the alternatives actually have different dependencies.
Renegotiate	Improve contractual rights and services, for example for data return, switching assistance or notification of changes.
Migrate	Move the application and data to another environment. First check whether the target environment meets the relevant requirements and what new dependencies arise.
Replace	Replace a product or provider. Consider functionality, transition, data migration and ongoing operation of the new solution.
Bring activities in-house	Operate or control a previously outsourced activity in-house. The necessary skills, staff, resources and responsibilities must be secured over the long term.

The decision template in the PDF appendix brings the assessment, rationale and actions together.

© 2026 Andreas Heß · Autonomy Track

11. Example: One Platform, Two Use Cases

This fictional example shows how the same technical finding can lead to different decisions depending on use. It does not assess a specific provider.

Starting Point

An organisation uses a cloud collaboration application. The review identifies the following:

- The contracting party is a European company. Under the contract, customer data are held in an EU region.
- Operations and technical control depend partly on other providers outside the EU.
- Customer-managed keys are available. They do not exclude technical access by the provider at every processing stage.
- Primary data can be exported. Some logs, permissions information and configurations cannot be transferred in full.
- Switching assistance is covered by the contract. A complete switch has not yet been tested.
- Independent audit reports are available. Whether they cover the current service and present use remains to be clarified.

Use Case A: General Internal Collaboration

Assessment: The application supports everyday processes of moderate criticality. Particularly confidential data are not processed in this use case.

Possible decision: Provisionally accept the known dependencies and limit their consequences, provided mandatory requirements are met. Resolve outstanding evidence questions within defined deadlines.

Next steps:

- Check regular exports and their reusability.
- Request current evidence for the service actually used.
- Conduct a switching test before the next contract renewal.

Use Case B: Critical Processes Involving Confidential Data

Assessment: A prolonged outage or unauthorised access would have serious consequences. The outstanding questions about access capabilities and recovery are decisive for this use case.

Possible decision: Approve this use only once the defined requirements are demonstrably met. Otherwise, select a suitable alternative.

Next steps:

- Check the effectiveness of additional access controls and encryption methods.
- Obtain the necessary evidence and contractual commitments.
- Test an alternative environment, including transition and operations.

Outcome: The provider is the same. Criticality, data and requirements differ. A blanket provider assessment cannot replace this judgement.

© 2026 Andreas Heß · Autonomy Track

12. Regulatory Context

This guide does not provide a complete mapping of legal requirements to individual assessment questions. However, several current frameworks show why provider dependency, supply chains, evidence and switching are increasingly concrete management responsibilities.

EU Cloud Sovereignty Framework

In June 2026, the European Commission published additional implementation guidance for its Cloud Sovereignty Framework.

The approach uses 48 criteria across eight sovereignty areas, supplemented by sovereignty scores and assurance levels.

For provider assessment, this means that control, technology dependencies and operational capabilities matter alongside data location.

DORA

Regulation (EU) 2022/2554 has applied since 17 January 2025.

Financial entities within its scope need exit strategies, among other measures, for ICT services supporting critical or important functions. The corresponding exit plans must be documented, adequately tested and reviewed regularly. Alternative solutions and transition plans also form part of the approach.

DORA does not apply to every organisation. Its underlying principle is nevertheless useful in practice:

> Critical provider dependency should be examined before notice of termination is given.

NIS2 and the German BSIG

NIS2 expressly includes supply chain security and relationships with direct suppliers and service providers as part of cybersecurity risk management.

Section 30 BSIG sets out corresponding requirements for essential and important entities in Germany.

This is neither a general legal obligation for every organisation nor a complete definition of sovereignty. It does show that supplier and provider dependencies are part of sound risk management.

EU Data Act

The Data Act sets out requirements for switching between data processing services and for portability.

For switching governed by the Data Act, switching charges, including related data egress charges, are abolished from **12 January 2027**. This does not mean every data transfer during ongoing use becomes free of charge.

A statutory right to switch does not replace the technical ability to do so.

BSI C5

C5 provides a criteria catalogue for independent audits of cloud services.

© 2026 Andreas Heß · Autonomy Track

The BSI expressly states that a C5 attestation is **not a BSI certification**. It also notes that a C5 attestation alone does not automatically satisfy all requirements of the minimum standard for the use of external cloud services.

When reviewing a C5 report, check in particular the service covered, audit period, attestation type, identified deviations and controls that the customer must implement.

ISO/IEC 27001

ISO/IEC 27001:2022 specifies requirements for information security management systems.

A relevant certification can support the information security assessment.

It does not automatically demonstrate digital sovereignty.

13. When should you reassess?

Reassessment should be triggered in particular by:

- Contract renewal
- Acquisition or change of ownership
- Material change in critical subcontractors
- Change in data or operating locations
- New technical platform/control plane
- Significant security incident
- New regulatory requirements
- Change in application criticality
- New realistic alternatives
- Results of a switching test

14. The Most Important Rule

The goal is not maximum independence at any cost.

The goal is:

> **Make dependencies visible, distinguish evidence from assumptions, and make an informed decision about which dependency an organisation accepts for a specific purpose.**

A documented, well-founded dependency can be a good decision.

A sound decision also identifies uncertainties and outstanding evidence. It specifies who will resolve them and when the assessment will be reviewed.

© 2026 Andreas Heß · Autonomy Track

Appendix A: 25-Question Checklist

Tick a statement only when it is demonstrably satisfied. Explain any items that are not applicable. Record open issues with an owner and deadline. The ticks do not produce a sovereignty score.

Service / provider: _____ Date: _____

Legal Framework & Control

- ☐ A1 The contracting party, controlling companies and relevant ownership structures are known.
- ☐ A2 Relevant jurisdictions for the contract, operations, access and disclosure have been identified.
- ☐ A3 Rights concerning audits, changes, subcontractors, termination, data return and provider switching have been reviewed.
- ☐ A4 Critical third-party providers and subcontractors are known.
- ☐ A5 Changes of ownership and material changes to the business model have been considered.

Data & Operations

- ☐ B1 Storage and processing locations for data, backups, logs, metadata and disaster recovery are known.
- ☐ B2 Privileged access and support paths are understood.
- ☐ B3 Key control and potential plaintext access are understood.
- ☐ B4 Critical operational dependencies and recovery paths are known.
- ☐ B5 Retention, deletion and operational evidence have been reviewed.

Technology & Supply Chain

- ☐ C1 Proprietary technical dependencies are documented.
- ☐ C2 Standards, interfaces and interoperability have been assessed.
- ☐ C3 Critical upstream technology dependencies are known.
- ☐ C4 Configuration, policies and automation have been checked for reproducibility.
- ☐ C5 Skills and the ecosystem for potential alternatives have been assessed.

© 2026 Andreas Heß · Autonomy Track

APPENDIX A · CONTINUED

25-Question Checklist

Service / provider: _____ Date: _____

Portability & Provider Switching

- ☐ D1 Export completeness and usability have been checked.
- ☐ D2 The switching process, support, timelines and costs are documented.
- ☐ D3 At least one realistic target option is known.
- ☐ D4 Time, costs, skills and the operational impact of switching providers have been estimated.
- ☐ D5 A scenario relevant to switching providers has been carried out and documented. Untested steps are explicitly identified.

Evidence & Reliability

- ☐ E1 Material provider claims are supported by traceable evidence.
- ☐ E2 The scope and currency of independent audits have been checked.
- ☐ E3 Critical marketing claims have been compared with contractual commitments.
- ☐ E4 The age of the evidence and notification of changes have been considered.
- ☐ E5 Owners, next steps and review dates are defined for outstanding questions and evidence gaps.

Open or not applicable items

© 2026 Andreas Heß · Autonomy Track

Appendix B: Evidence Checklist

Select the documents required. Tick receipt and review separately. “Checked” means that relevance, currency and scope have been assessed. It does not automatically mean that all requirements are met.

Service / provider: _____ Date: _____

Document / evidence	Received	Checked
Contracting party and group/ownership structure	☐	☐
Current service description	☐	☐
Architecture and data flow diagrams	☐	☐
Guaranteed locations for data, backups and disaster recovery	☐	☐
Critical service providers and subcontractors	☐	☐
Support and privileged access model	☐	☐
Encryption and key management model	☐	☐
Shared responsibility model	☐	☐
API, export and portability documentation	☐	☐
Switching/transition process	☐	☐
Termination, retention and deletion terms	☐	☐
Service agreement, business continuity and disaster recovery	☐	☐
Notification rules for material changes	☐	☐
Current audit reports, attestations or certificates, including scope	☐	☐
Example export or migration test, where relevant	☐	☐
Known costs for provider switching, export and switching assistance	☐	☐

© 2026 Andreas Heß · Autonomy Track

Appendix C: Decision Template

1 / 4 · Scope

Service / application and provider

Business owner · Assessment date

Criticality and consequences of an outage

Data categories and protection requirements

Legal and internal requirements

Contract end / next renewal

© 2026 Andreas Heß · Autonomy Track

APPENDIX C · DECISION TEMPLATE

2 / 4 · Findings and Outstanding Questions

Legal Framework & Control

Findings and material dependencies · Evidence / reference

Outstanding questions · Next steps · Owner · Deadline

Data & Operations

Findings and material dependencies · Evidence / reference

Outstanding questions · Next steps · Owner · Deadline

Technology & Supply Chain

Findings and material dependencies · Evidence / reference

Outstanding questions · Next steps · Owner · Deadline

© 2026 Andreas Heß · Autonomy Track

APPENDIX C · DECISION TEMPLATE

3 / 4 · Findings and Outstanding Questions

Portability & Provider Switching

Findings and material dependencies · Evidence / reference

Outstanding questions · Next steps · Owner · Deadline

Evidence & Reliability

Findings and material dependencies · Evidence / reference

Outstanding questions · Next steps · Owner · Deadline

© 2026 Andreas Heß · Autonomy Track

APPENDIX C · DECISION TEMPLATE

4 / 4 · Decision and Implementation

Selected options (multiple selections allowed)

- ☐ Accept
- ☐ Limit the consequences
- ☐ Renegotiate
- ☐ Replace
- ☐ Reduce
- ☐ Develop alternatives
- ☐ Migrate
- ☐ Bring activities in-house

Decision rationale

Accepted residual dependencies and risks

Actions · Owner · Target date

Approval / owner · Date

Next review · Date or trigger

© 2026 Andreas Heß · Autonomy Track

Sources and Further Reading

This guide supports structured technology and provider assessment. It does not replace individual legal advice or a binding conformity assessment.

1. European Commission: Cloud Sovereignty Framework

https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en

2. EUR-Lex: DORA - in particular Articles 28 to 30 and 64

https://eur-lex.europa.eu/eli/reg/2022/2554/oj

3. European Commission: Data Act explained

https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

4. EUR-Lex: NIS2 - Directive (EU) 2022/2555

https://eur-lex.europa.eu/eli/dir/2022/2555/oj

5. EUR-Lex: Implementing Regulation (EU) 2024/2690 on NIS2

https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

6. Gesetze im Internet: section 30 BSIG

https://www.gesetze-im-internet.de/bsig_2025/__30.html

7. BSI: C5 criteria catalogue for cloud services

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

8. BSI: the role of C5 attestations for external cloud services

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/FAQ_MST_Externe_Cloud-Dienste/faq_mst_Externe_Cloud-Dienste_node.html

9. ISO: ISO/IEC 27001:2022

https://www.iso.org/standard/27001

© 2026 Andreas Heß · Autonomy Track