Dependence on Individual Software Vendors
Strategic Market Analysis

Final Report
August 2019
Contents

1 Executive Summary ................................................................. 3
2 Initial Situation and Purpose of the Report............................... 5
3 Definition of Assessment Basis .................................................. 6
4 Analysis of the Software Market ................................................ 8
   4.1 Market Concentration as a Driver of Dependence............... 8
   4.2 Market Trends as a Driver of Dependence ......................... 12
5 Assessment of Dependence Factors and Pain Points .................. 14
6 Similar Projects ...................................................................... 19
   6.1 Leading Strategies .......................................................... 19
   6.2 Success Factors .................................................................. 22
7 Courses of Action to Reduce Dependence ................................. 25
8 Recommended Further Action ................................................... 27
9 Legal Notice ........................................................................... 30
1 Executive Summary

The German Federal Administration (Bundesverwaltung) makes wide use of standard products from commercial software vendors. The high supplier power of these vendors has led to a situation where some of them do not or only partially address their customers’ requirements, for example the increased need for information security in the public sector. This potential limitation to the public administration’s digital sovereignty\(^1\) is not only a cause for concern for Germany’s Federal Government and its Federal States (e.g. Schleswig-Holstein), but also for other countries (such as the Netherlands or the Republic of Korea). The Federal Administration considers it important to conduct a prompt analysis of the dependence on software vendors so appropriate steps to ensure its digital sovereignty can be taken. Additionally, the Federal Government’s ongoing IT consolidation initiative (“IT-Konsolidierung Bund”, or "IT-K Bund" for short), increasingly centralises the Federal Administration’s software portfolio by expanding the use of standard products. This process may further aggravate the situation, but at the same time also offers a good opportunity to selectively manage the development and use of software to reduce existing dependence.

The aforementioned situation is the subject of this strategic market analysis, which PwC Strategy& (Germany) GmbH conducted on behalf of the Federal Ministry of the Interior, Building and Community (Bundesministerium des Innern, für Bau und Heimat – "BMI"). The analysis is mostly based on interviews and workshops with specialists from the PwC/Strategy& network, external knowledge holders as well as employees from various departments of the Federal Administration, combined with extensive research based on internal and external data. On this basis, dependence is first evaluated along a defined software stack\(^2\), followed by an analysis of the software market. The final step is an assessment of the dependence on individual software vendors. This is done by assessing factors that favour dependence and by identifying (potentially) negative consequences (referred to as “pain points”). Similar projects to reduce dependence that might point to potential success factors complement the analysis. All of this will provide options for potential courses of action as well as recommendations concerning the future approach to be adopted by the Federal Administration.

\(^1\) Definition of digital sovereignty: “Ability and opportunity of individuals and institutions to execute their role(s) in the digital world independently, intentionally and safely” from "Kompetenzstelle Öffentliche IT (OFIT)", 2017. Digitale Souveränität. Accessed on 10 August 2019. <https://www.ooffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t>

\(^2\) A software stack is a set of software components that build on each other.
Findings in short:

- The Federal Administration is heavily dependent on a small number of software vendors throughout all layers of the software stack. This applies particularly to Microsoft, whose products are widely used and closely interconnected (e.g. Outlook, Exchange and Windows Server). For that reason, this study examines in detail products that are particularly widely used: Microsoft Office, Windows and Windows Server.

- Currently, the market is concentrated around a small number of software vendors, which tends to encourage dependence. The strategic direction taken by these vendors is threatening to aggravate this dependence even further in future. The strategic direction in question includes the continuous expansion of the vendors’ own digital ecosystems, the accelerating transition from on-premises to cloud-based solutions, and their greater attention to the development of open-source software (OSS)\(^3\). In addition to market-leading products, there are, however, other proprietary\(^4\) and open-source alternatives on the market, some of which are comparable in terms of performance.

- As the results of this analysis show, the dependence on Microsoft products in particular leads to pain points for the Federal Administration, which run counter to the strategic objectives of the Federal Government’s strategic IT goals. Pain points regarded as particularly critical are limited information security and legal uncertainty (concerning data protection), both of which threaten the state’s digital sovereignty.

- National and international examples show that many organisations are already using, or considering the use of, alternative solutions in order to reduce their dependence on individual software vendors. Many of them aim to replace Microsoft products with open-source solutions. The analysis of selected projects has identified possible success factors for the pursuit of such alternative solutions.

In general, there are four courses of action for reducing dependence:

1. Establishing basic conditions, e.g. action plans, guidelines or legislation on product diversification.

2. Negotiating with vendors to achieve the necessary product adjustments/contract amendments (cooperation at EU level possible).

3. Diversifying with other proprietary software by complementing or replacing products in use.

\(^3\) Within the scope of this study, “open-source software” (OSS) refers to free and open-source software (also called “FLOSS”). The special case of open-source proprietary software is not part of this analysis.

\(^4\) Within the scope of this study, “proprietary” software refers to software that is developed and licensed by commercial vendors and whose source code is not in the public domain.
4. Building or using OSS alternatives based on the needs of the Federal Administration.

Irrespective of the course of action adopted, next steps should be taken swiftly to ensure Germany’s digital sovereignty and to prevent dependence and (potentially) negative consequences from growing worse. A sustainable solution for the entire Federal Administration must be closely harmonised with ongoing initiatives such as IT-K Bund.

2 Initial Situation and Purpose of the Report

Large parts of the Federal Administration’s software portfolio consist of proprietary standard software, and its use is intended to be continued in the future following the IT consolidation under the federal government’s IT-K Bund initiative. This will aggravate the dependence on individual software vendors and give them more opportunities to use this to their advantage. Other public-sector purchasers in Germany and abroad have also identified this as a risk and are working towards a solution. Schleswig-Holstein, for example, has adopted an open-source strategy to reduce the share of proprietary software products and thus its dependence on individual vendors. The Dutch government has examined the information security of dominant standard software and entered negotiations with the vendor. Both France and the Republic of Korea have decided to introduce OSS. The current debate around the consequences of US sanctions imposed on Huawei also illustrates the problems associated with a dependence on foreign software vendors. Against this background, the issue must be looked at specifically regarding the Federal Administration’s digital sovereignty and information security. However, the project also offers an opportunity to realign the Federal Administration’s software portfolio and thus counteract this development. National and international examples show possible alternative solutions.

Based on interviews and workshops with specialists from the PwC/Strategy& network, external knowledge holders, various departments of the Federal Administration, as well as extensive research and data analysis, the market analysis comprises the following parts:

- Definition of an assessment basis for evaluating existing dependence and pain points and limitation of the scope of the study
- Survey of the software market in terms of vendor concentration and the strategies of vendors dominating the market
- Assessment of existing dependence and the resulting pain points for an observation period up to 2025, based on the IT-K Bund initiative

---

• Analysis of comparable projects to reduce dependence on software vendors and formulation of potential success factors

• Formulation of strategic courses of action with due regard for the Federal Administration’s IT target vision

Based on this market analysis, recommendations will be presented on what steps to take next in handling dependence on software vendors that dominate the market.

3 Definition of Assessment Basis

It is necessary to define an assessment basis before dependence can be analysed. That basis is used to assess the causes and risks of dependence in order to identify and evaluate pain points for the Federal Administration.

Since dependence can arise in all areas of software applications, the assessment basis needs to be applicable to different software products.\textsuperscript{6} The various products can be arranged in categories by means of a layer model. Each software is allocated to a layer in accordance with its functional properties.\textsuperscript{7} A software stack is a set of software components that build on each other; it breaks down into various front-end layers, such as applications and desktop operating systems, as well as back-end layers, such as databases and server operating systems.

Similar to the rough concept of the IT-K Bund initiative, the applications are broken down into specialist applications and cross-sectional IT.\textsuperscript{8} In this study, specialist applications are handled separately in the software stack, because they are used at the discretion of individual departments rather than across the entire Federal Administration. In addition, office software is considered separately from other cross-sectional IT applications, since it is part of every standard IT workstation throughout Germany and should therefore be examined with particular focus as part of the dependence analysis (see Figure 1).

\textsuperscript{6} Dependence may also arise for hardware such as routers, but this is not the focus of this analysis.

\textsuperscript{7} Each of the layers has various product segments (product groups).

\textsuperscript{8} BMI, 2017. \textit{Projekt-Glossar IT-Konsolidierung Bund} (IT-K Bund project glossary), version 1.0 (preliminary).
Under the IT-K Bund initiative, a survey of the software used in a large number of Federal Agencies is conducted once per year. The survey shows that Microsoft products, for example, are used in all layers of the software stack. This applies specifically to office software, desktop and server operating systems, where 96% of all direct authorities use Microsoft Office and Windows, and 69% use Windows Server (see Figure 1). As high levels of product concentration, software use across layers and data exchange between different software solutions generally favour dependence, this report primarily focuses on office software, desktop and server operating systems.

In addition, the agreed license terms and installed software clients of the Federal Administration also point to potential dependence on other leading software vendors, especially Oracle and SAP. However, this mainly applies to individual product segments (DBMS and ERP) at the platforms and cross-sectional IT layers, and the available data suggests that they are used less widely. This report therefore focuses on Microsoft. It is advised that the Federal Administration conduct more in-depth analyses and expand the scope to include other IT providers.

The framework in Figure 2 shows the link between dependence factors, actual dependence and the resulting pain points. Dependence can therefore be the result of the technical properties of the IT landscape, processes with a strong software focus, and this gives rise to a locked-in relationship, which is perceived as negative. (See Diller et al., 2010. Management von Kundenbeziehungen: Perspektiven-Analysete Strategien-Instrumente (Managing customer relationships: perspectives – analyses – strategies – tools). Springer-Verlag.)

---

9 Microsoft Dynamics, SQL and System Center Configuration Manager are further examples of cross-sectional IT, platforms and infrastructure-related applications.

10 BMI, 2018. IT-K Bund Ist-Aufnahme. (IT-K Bund status quo)

11 Based on the current procedure for assessing dependence and pain points, it is recommended to also analyse other vendors (especially SAP, Oracle) in more detail.

12 Dependence means that a customer is reliant on the products/services of a particular vendors, and this gives rise to a locked-in relationship, which is perceived as negative. (See Diller et al., 2010. Management von Kundenbeziehungen: Perspektiven-Analysete Strategien-Instrumente (Managing customer relationships: perspectives – analyses – strategies – tools). Springer-Verlag.)
staff trained in and accustomed to using particular software, contract clauses and general market conditions. Dependence means a loss of control and may have a negative impact on information security (e.g. limited availability, confidentiality, integrity), legal compliance (e.g. with the GDPR or licensing provisions) and finances and, consequently, severely limit the flexibility and innovation capability of the party concerned. These factors create a framework that serves as the basis for assessing dependence factors and pain points.

Figure 2: Framework for assessing dependence factors and pain points

4 Analysis of the Software Market

The current structure of the software market fosters dependence on individual vendors. Above all, this is attributable to high and still rising levels of market concentration along several layers. At the same time, vendors are increasingly gaining market power through their business strategies.

4.1 Market Concentration as a Driver of Dependence

Currently there are high or very high levels of market concentration in almost all layers of the software stack\(^\text{13}\), with Microsoft products dominating many of the layers. In the office software, desktop and server operating system layers in particular, Microsoft products are leading the market with a considerable edge. On the other hand, SAP and Oracle mainly dominate individual layers or product segments (ERP or DBMS). The most relevant results of the analysis are presented below, beginning with the office suite product segment in the office software layer.

\(^\text{13}\) (Very) high market concentration means: a company with a market share of >40% (>60%) or up to three companies with a market share of >50% (>80%); pursuant to section 18 of the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen – “GWB”)
Microsoft has a market share of around 84% in the office suite product segment\(^{14}\) (see Figure 3) and will likely retain this share due to the wide distribution\(^{15}\), high usability and large functional scope of its products. At the same time, trends are beginning to emerge that could reduce dependence on this vendor in the office suite segment. First, Google is establishing itself as a competitor, especially in the enterprise segment. The increasing relevance of cloud-based (SaaS) and mobile/multi-device-capable office suites favours this development. Second, open-source solutions – alongside proprietary products – are attracting more and more users. Here, the open-source LibreOffice suite is the most widely used non-proprietary alternative\(^{16}\) to Microsoft’s and Google’s products. It is mainly used in the public sector and in smaller companies. Since revenue figures are not available and distribution cannot be reliably measured, the market share is unknown, but the number of active MS Office licences and information provided by LibreOffice suggest an estimated market share in the lower single-digit percentage range.


\(^{15}\) High habituation effect

\(^{16}\) There are a number of distribution companies such as Collabora. Collabora Online also offers a cloud-based variant of LibreOffice.
In the desktop operating system segment (desktop operating system layer), Microsoft’s Windows operating system also dominates the market, accounting for a market share of 81% based on revenue in 2017 (see Figure 4). Products competing with Windows are primarily Apple’s MacOS operating system as well as various Linux distributions.

17 iWork (Apple’s office suite) is available free of charge (no revenue figures) and pre-installed in some products
The increasing use of thin clients\textsuperscript{19} could lead to new software vendors establishing themselves in the market, thus reducing dependence on individual vendors. Linux’s share of the market for thin-client operating systems is growing rapidly, pointing to greater market relevance in the future. Although this will reduce dependence in the front-end segment, dependence in the back-end segment may continue to play a role.\textsuperscript{20}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{market_share.png}
\caption{Market analysis summary of the desktop operating system segment}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{msd.png}
\caption{Microsoft’s sole market-dominant position due to Windows}
\end{figure}

In the server operating system segment, the relevance of Microsoft products is mainly attributable to their dominance in the front end (i.e. office software and desktop operating systems). In contrast, front-end-independent server and infrastructure systems primarily feature Unix or Linux’s open-source software.

Another factor is that cloud-based models, especially for server operating systems, are becoming increasingly popular since they use PaaS and IaaS instead of in-house


computer centres, leading to market growth for the respective cloud solutions.\textsuperscript{21, 22} Products used here include Microsoft’s Azure and a number of Linux-based solutions.

In sum, there is a greater spread across the various vendors of server operating systems, even though Microsoft is the leading vendor by revenue.\textsuperscript{23} When considered across layers, it becomes clear that there is only a small number of alternative vendors, which means that the structure of the market per se favours dependence. Significant alternatives are mostly found in the area of open-source software.

4.2 Market Trends as a Driver of Dependence

Various IT trends, such as the workplace of the future\textsuperscript{24} or cloud computing are set to have a fundamental impact on the future use of IT. Software vendors are responding to these trends and are actively involved in shaping them. By developing new products or taking over competitors, they can exercise greater control over the market and further strengthen their market position. These market developments, especially in the areas of digital ecosystems, digital platforms and open-source software, could have a major impact on future dependence.

Digital Ecosystems

Vendors of software solutions are forming "digital ecosystems" by entering into partnerships (e.g. start-up development programmes, agreements between software vendors and IT service vendors or joint development programmes) or by trying to expand their coverage of the software stack through acquisitions. SAP and Microsoft in particular have turned their strategic focus on these kinds of partnerships and are building extensive ecosystems with their own core solutions at the centre. This fosters synergies between vendors and strengthens their market power in the process. The flip side is that it also promotes or even requires the use of a small number of centralised solutions – and thereby increases dependence. Microsoft, for example, uses a number of formats, such as the Partner of the Year award or the ScaleUp


\textsuperscript{23} Market analysis based on revenue can only provide a very distorted view, because many of the operating systems used do not generate any revenue if they are based on open-source software.

\textsuperscript{24} The workplace of the future describes how future technologies will influence and change the way of working (e.g. the rising trend towards mobile working, increased flexibility and new ways of collaborating).
programme, to win partners wanting to collaborate on shared solutions or to integrate Microsoft applications into their solutions. This trend may lead to a situation where products from third-party vendors will only deliver their full benefit if they are used in combination with Microsoft products.

**Digital Platforms**

Many vendors are switching their product portfolios to digital platforms based on cloud computing. As a result, products that were previously available separately can only be consumed as part of an integrated cloud-based platform. Given the lack of alternative products, this change forces customers to adapt their IT landscape to facilitate the use of cloud offerings in the future.

Microsoft strongly focuses on this approach. It has established the “Intelligent Cloud” as one of three central pillars of its business model and prioritises investments in products of this segment. While enhancements of the traditional on-premises product range only play a secondary role, new functionalities are added to Microsoft’s 365 product range at short intervals. This favours a linkage between Dynamics 365 and Office 365 functionalities based on AI-driven applications on an Azure cloud without separate data silos. In addition, the increased focus on cloud-based offerings also allows the respective vendors to gain easier access to user data.

Although digital platforms offer customers functional benefits, such as an integrated data view, they generally also increase dependence on the respective software vendors, since solutions can no longer be bought separately and subsequently combined.

**Open-source Products**

Due to a rising demand for secure and customisable solutions, open-source products are used increasingly frequently across all layers of the software stack and are thus gaining importance in the software market. This is why more and more commercial software vendors are penetrating the open-source sector. That goal is achieved, among other ways, through acquisitions, such as that of Red Hat by IBM, the integration of open-source solutions into proprietary products (e.g. virtualized Linux in the new version of Windows 10) or the involvement in the development of open-source solutions (e.g. Microsoft’s cooperation with SUSE).

---

25 Moreover, there are signs of a price increase for on-premises products.
28 Monetisation in OSS, especially by providing consulting, development and support services.
Although the increasing involvement of vendors of proprietary solutions in the open-source market could potentially lead to innovation and wider use of these solutions, it also comes with risks. For example, it is conceivable that influence could be exerted on enhancements of open-source solutions, e.g. by deploying appropriate financial resources or by lobbying the developer community. Oracle’s behaviour regarding mySQL, JAVA and OpenOffice (following the acquisition of Sun) shows how commercial software vendors are trying to control the developer community and the enhancement of open-source solutions. In the cases referred to above, the influence exerted led to the breakup of OpenOffice (mySQL went to MariaDB\textsuperscript{30}, OpenOffice to LibreOffice\textsuperscript{31}) and caused it to lose importance.

The efforts of the major vendors in the open-source segment do not increase the dependence of their users directly. Ultimately however, the influence these vendors have on open-source development will increase, adding to the risk that software that was previously open-source will become proprietary in the long term due to acquisitions.

In sum, there is evidence that current market developments foster dependence on major software vendors, the main reason being their high market share. This dependence may even be aggravated by future market trends, such as the creation of digital ecosystems, the offer of cloud-based platforms and influence exerted on open-source software. Although these changes have the potential to extend the range of solution functionalities, they also strengthen the position of vendors dominating the market along the stack, and thus ultimately pose a risk to IT users such as the Federal Administration, for example by affecting their freedom in designing their own IT landscape.

5 Assessment of Dependence Factors and Pain Points

The analysis of the Federal Administration’s IT follows the framework presented in chapter 2, which differentiates between dependence factors and resulting pain points. The analysis focuses on the layers of office software, desktop and server operating systems, where Microsoft products are deployed to a very large extent (see chapter 3). Due to the prevalence of Microsoft products in the Federal Administration and their dominant market position (see chapter 4) in the corresponding layers and product segments, this part of the study focuses on Microsoft Office, Windows and Windows


Ten assessment criteria are examined for each of these products (see Table 1). This qualitative assessment is based on reviews of internal data of the Federal Administration, research using external data (e.g. analyst reports, studies), interviews with employees of the Federal Administration, specialists from the PwC/Strategy& network and external knowledge holders, as well as feedback provided by project participants. Since all the products are offered by Microsoft and are often procured through standardised contracts, there are some similarities in the assessment of dependence factors and pain points. In view of the consolidation of services by 2025 envisaged under the IT-K Bund initiative, the analysis covers a period of six years and, in addition to the status quo of IT in the Federal Administration, also takes into account the target IT, future product versions, and strategies pursued by software vendors.

<table>
<thead>
<tr>
<th>Dependence factors</th>
<th>Office software</th>
<th>Desktop OS</th>
<th>Server OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT landscape</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Processes</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Personnel</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Contract*</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Market</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Pain points</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limited information security</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Legal uncertainty</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Limited cost control*</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Limited flexibility</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Externally influenced innovation</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 1: Key ratings in the dependence analysis for the layers reviewed

The analysis shows that the Federal Administration’s dependence on Microsoft products is caused by a number of different factors and leads to numerous critical pain points. Table 1 summarises all the dependence factors and pain points considered for Microsoft Office, Windows and Windows Server; they are described in more detail below.

Dependence on Microsoft products in the layers reviewed is driven by different dependence factors:

- **IT landscape**: Microsoft Office, Windows and Windows Server are widely used in the Federal Administration. Limited access to the full source code, proprietary Office file formats and frequently modified interfaces make it difficult to achieve compatibility with other software. In addition, Microsoft integrates its software products closely with each other. For example, Outlook\(^{32}\), Exchange and Windows

\(^{32}\) E.g. Outlook integration in connection with “E-Akte”, the Federal Government’s electronic archiving system
Server build on each other, sometimes without open interfaces, and should be used together to ensure optimum functionality and performance and enable higher levels of security. Closed products and strong interlinks create high levels of technical dependence, which will persist in the future since the software is intended to be part of the Federal Administration’s consolidated IT landscape.

- **Processes**: Process-related dependence only exists to a limited degree, since most of the Federal Administration’s organisational procedures are not specifically tailored to Microsoft software. Dependence arises when certain specialist applications or modifications, for example numerous macros in the Federal Ministry of Finance (Bundesministerium der Finanzen – BMF), are technically based on Microsoft Excel or Microsoft Word and, as a result, influence work processes. Apart from this, mainly IT operating processes are tailored specifically to Microsoft Windows and Windows Server.

- **Personnel**: Since most of the Federal Administration’s employees use Microsoft Office and Windows in their daily work and often also in their private lives, they have developed the requisite skills and have become very accustomed to the user interface functions. Furthermore, IT staff members have been trained to use Microsoft products and therefore have the corresponding know-how. The migration to different software would entail considerable training requirements and a need for change management. As a result, there is a high affinity towards Microsoft products among staff members.

- **Contract**: Some key contractual terms and conditions are negotiated directly with Microsoft, as a bundle for the Federal Government, the Federal States and local authorities. Public tender procedures via distributors are subsequently used for procurement. This strengthens the Federal Administration’s negotiating position and brings financial advantages. It is possible that the Federal Administration’s negotiating position will deteriorate due to licensing changes under Microsoft’s "cloud first" approach and the product bundling strategy being pursued. Consequently, the contract factor should be seen as a moderate dependence factor.

- **Market** (see chapter 4): Microsoft dominates the office software, desktop and server operating system layers as a result of its (very) high market share. Its market position is additionally boosted by an extensive ecosystem of third-party vendors. Even though there are some comparable alternative solutions, they are not very widespread due to the market situation, and this leads to a very high dependence on Microsoft products.

The high dependence on Microsoft products in the layers under review has led to a number of **pain points** for the Federal Administration:

- **Limited information security**: Since the source code is not fully accessible, the Federal Administration has only limited options for examining the information
security of Microsoft software. For example, new product versions contain telemetry components, which record and collect metadata.\textsuperscript{33,34} In this process, data is transferred to and stored on Microsoft servers and could subsequently find its way to US authorities.\textsuperscript{35} This can happen because, pursuant to the CLOUD Act, US prosecuting authorities can obtain a warrant to search servers controlled by a US company, even if the servers are not actually located in the USA. However, the CLOUD Act also allows for the lodging of an appeal against such a move. Under Microsoft's "cloud first" strategy, existing on-premises solutions are increasingly being replaced with cloud-based services. A potential remote shut-down of cloud-based products or even the remote disabling of on-premises licences could severely restrict the availability of software. The restriction of information security due to these factors is an extremely critical pain point.

- **Legal uncertainty**: The metadata that can be transferred via the telemetry component (also referred to as "diagnostic data") may also contain personal data. Users do not have sufficient insight into the collection of data and only limited control over the data itself.\textsuperscript{36} Although the telemetry component can technically be turned off, doing so could compromise the support for and the full functionality of Microsoft products in certain circumstances.\textsuperscript{37,38} Accordingly, the telemetry components as currently implemented in a number of Microsoft products are posing a legal risk in terms of compliance with the GDPR, since there is not enough transparency yet over how the data is processed.\textsuperscript{39}

- **Limited cost control**: At present, it is relatively easy to manage licence fees, because Microsoft is giving comparatively high discounts and is granting long-term software licences. In 2018 however, Microsoft increased its licence fees (by up to 30\%), especially those for on-premises products with device-based licences. Moreover, some licensing models have been adjusted in recent years, for example by introducing user-based licences for Windows (2014) and processor core-based licences.


\textsuperscript{34} Nas, S. & Roosendaal, A., 2018. DPIA Diagnostic Data in Microsoft Office ProPlus. Privacy Company.


\textsuperscript{39} As a response to violations of the GDPR identified in Office Pro Plus (2016/365) by the DPIA study, Microsoft promised to provide access to the telemetry and configurations in future. This may help to reduce the legal uncertainty.
("core") licenses for Windows Server (2016). Licences for cloud-based products, which Microsoft increasingly offers, can only be obtained for a limited period of time on a subscription basis. Through its product-bundling and cloud strategy, Microsoft is trying to motivate the Federal Administration to make greater use of these subscription-based licensing models, which would make it more difficult for the Federal Administration to control future adjustments to fees and licensing models. For this reason, limited cost control is a moderate pain point.

- **Limited flexibility**: Since some interfaces are proprietary and subject to change, Microsoft software (e.g. Exchange) can often only be connected to products from third-party vendors at an additional cost and with limited functionality. However, as a result of embedding the Linux kernel in Windows, compatibility will improve in future, as the relevant applications will then also be able to run on Windows and allow for a more flexible use of Windows-based systems. Despite its only partially accessible source code, Microsoft Office offers extensive options for customising the products to individual needs by means of VBA or add-ins. Overall, limited flexibility therefore is a minor pain point.

- **Externally influenced innovation**: By and large, Microsoft products meet the functional requirements of the Federal Administration. However, this may change as Microsoft shortens its release cycle frequency and focuses on cloud-based digital platforms, because updates are released at ever shorter intervals. These dynamics leave less time for the Federal Administration to check and respond to product updates. This gives Microsoft a growing influence on innovation cycles. The Federal Administration is generally aware of the risks of not having enough preparation time to respond to such product innovations (e.g. discontinued functions) promptly. Under its "cloud first" strategy, Microsoft is trying – for example, by means of price incentives, product bundling and price increases for local solutions – to encourage more customers to migrate to cloud-based solutions. Against this background, it can be expected that support for on-premises products – and the corresponding innovations – will be scaled back or discontinued over the next few years. Moreover, the expanding "as-a-service" offering means that fewer IT-qualified personnel will be needed for the daily operation of IT systems. This could lead to a decline in skills, which may reduce the Federal Administration’s IT innovation capability in the long term. As a consequence, the Federal Administration’s innovation capacity is increasingly influenced by Microsoft products.

The analysis shows a high dependence on Microsoft’s Office, Windows and Windows Server products within the Federal Administration. This gives rise to critical pain points. The dependence is primarily attributable to a strongly interconnected IT landscape, usage habits of employees and Microsoft’s dominant market position. This high degree of dependence has a particularly critical effect on information security and legal certainty (for data protection), which will potentially be put at risk by, above all, the roll-out of cloud-based solutions and the transmission of telemetry data. In addition,
Microsoft has a growing influence on pricing and innovation. Ultimately, these pain points will jeopardise the digital sovereignty of the Federal Administration. Without corrective action, this critical situation will persist beyond 2025, driven by, among other things, the activities under the IT-K Bund initiative.\(^{40}\)

Consequently, the Federal Administration should take prompt steps to reduce its dependence in order to retain control of its own IT and innovation for the long term, ensure appropriate information protection, and manage IT costs. Similar projects providing some significant insights in this context are considered below.

6 Similar Projects

Many organisations seek to reduce their dependence on individual software vendors and have already embarked on projects to achieve this. A more detailed analysis of these projects has identified strategies and success factors.

The analysis is based on over 60 similar projects.\(^{41}\) Over 80% of them originate in the public sector (e.g. the EU, France, Schleswig-Holstein, the city of Barcelona). The projects strongly focus on the office software (approximately 70% of projects) and desktop operating system (approximately 40% of projects\(^{42}\)) layers. For both these layers (as well as others), the primary objective is independence from Microsoft products. Over half of the projects were launched in or before 2014, and at least half of them are still being implemented.

6.1 Leading Strategies

The projects investigated essentially pursue four strategies in order to reduce dependence and the resulting pain points.

\(^{40}\) See the chapters entitled "Initial Situation" and "Market Assessment"

\(^{41}\) In addition to extensive desk research, the sources used included, among others, research agencies and databases (e.g. Gartner, Factiva, EU Open Source Observatory), PwC-internal sources as well as contacts from within the PwC network with international governments and corporate groups. For more in-depth analysis of projects, tens of interviews were conducted with users (persons in charge of prioritised projects, IT user associations), vendors (of proprietary and free software) and third parties (open-source associations).

\(^{42}\) Focus on more than one layer per project is possible.
Strategy 1: Establish basic conditions

Particularly in the public sector, concrete steps to replace software are often preceded by the creation of necessary basic conditions. Among other things, this comprises declarations of intent (e.g. for the use of free software), concepts and action plans for an actual replacement, or new laws. These measures are intended to support other players (authorities, companies, citizens) in achieving independence.

Examples of this strategy include the European Commission’s OSS strategy, e.g. in the context of tender processes or the provision of software developed in-house as open-source. The UK government has also deliberately switched to open-source software by making it mandatory, among other things, to publish the code of software developed in-house. In Germany, by adopting a strategic position on FLOSS, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – "BSI") has laid the foundation for distributing the corresponding software (e.g. Gpg4win) more widely and makes such software available. Another example is the guideline for the Federal Government’s IT architecture, which sets out IT development requirements. In view of the current sanctions, the Russian government is seeking ways to achieve greater independence from Western software vendors as well and uses OSS as part of these efforts.43

Strategy 2: Negotiate

Many organisations try to alleviate their pain points through negotiations. In addition to licence/pricing negotiations, the focus increasingly lies on delivery models (especially cloud-based vs. on-premises solutions) and compliance with information security and data protection requirements. In some cases, political pressure is also applied during

---

the negotiations, for example by presenting expert reports relating to the pain points identified.

For example, the Dutch Ministry of Justice obtained concessions from Microsoft on the collection of telemetry data. The vendor promised to adjust its proprietary products in accordance with the GDPR. The Israeli government negotiated a new contract with Microsoft, having identified cloud-based products as a potential cost risk. The “Microsoft Cloud Deutschland”44 (under the data trusteeship of Deutsche Telekom), which in the meantime has been discontinued for various reasons, shows that negotiated compromises (relating to a private cloud in this case) do not always result in the desired outcome.

**Strategy 3: Diversify with proprietary software**

Although Microsoft dominates the software market in many layers, alternatives can be found for a number of products (see chapter 4.1). Private businesses, in particular, are contemplating a migration to other proprietary solutions. These kinds of decisions are often driven by a desire for different functionality or to accommodate employee preferences (e.g. relating to new approaches to cooperation) and may lead to new, consciously accepted dependence on other (mostly commercial) vendors. Risks can, however, be mitigated by adopting a multi-vendor strategy, under which different products for the same services are bought from at least two vendors. It is also conceivable and possible to develop new products in-house or to establish an additional vendor (depending on the form this takes, there is overlap with strategy 4). Approximately one quarter of the organisations investigated are considering migration to (different) proprietary software.

Airbus, Verizon or Facebook, for example, are replacing (some) Microsoft Office products with cloud-based solutions from Google (G Suite). Other examples include IBM and Google, which addressed the hardware side and, to a large extent, have switched to Apple devices (and the corresponding operating and ecosystem) – partly for reasons of user preference, and partly to improve security. The Russian government uses local software solutions such as MyOffice Mail (original name: мойофис почта) or a Russian cloud.

**Strategy 4: Build and use alternative open-source software**

The most widely used solution identified by this study is the migration to open-source software (in more than half of the cases investigated). In most cases, the focus is on the utilisation of existing solutions, often with few or no modifications. In some cases,

---

44 Low user acceptance was attributable to the fact that it cost around 25% more and offered fewer functions than the Azure Cloud. In addition, after the adoption of the CLOUD Act, uncertainty continued over the actual security of the data. The cloud was discontinued because of insufficient demand.
the switch is made on the basis of in-house developments or participation in OSS communities. OSS projects often go beyond the replacement of individual products. On one hand, there is dependence which should be addressed in a holistic manner (e.g. replacing the ecosystem around Microsoft Exchange, Sharepoint, Active Directory). On the other hand, the decision to opt for OSS and develop the requisite structures and skills often leads to the gradual replacement of other components as well.

Some corresponding examples include initiatives by the Italian Armed Forces or the City of Rome in replacing selected Office installations. Broader approaches have been pursued by the French Gendarmerie, the Federal State of Schleswig-Holstein, the City of Munich, the City of Barcelona, or the Austrian Federal Computing Centre. Many German authorities are now also operating large parts of their back end with OSS (e.g. the BSI).

### 6.2 Success Factors

For these four leading strategies to reduce dependence on software vendors, a number of different success factors (SFs) can be derived. Due to their greater complexity, the focus here is on strategies that deal with the roll-out of new software (strategies 3 and 4, see Table 2). The chances of success of these strategies and the factors to consider in their adoption are illustrated in two brief case studies on the projects in Munich and France which are presented at the end of this chapter. These examples are representative of the interviews and analyses conducted on other projects.

| SF1 | Ensure realistic level of ambition |
| SF2 | Build IT skills |
| SF3 | Ensure user acceptance |
| SF4 | Proceed step-by-step, create moments of success |
| SF5 | Use the community |
| SF6 | Achieve critical user mass |

Table 2: Summary of success factors for strategies 3 and 4: Roll-out of new software.

1. **Ensure realistic level of ambition**: For the migration to another software, clear objectives should be defined (e.g. functionality, information security). The target group should also be defined clearly. Since some objectives conflict with one another, a realistic level of ambition is important. For example, a high level of information security may lead to additional costs (e.g. through a private cloud), or a conscious balance of functional scope and cost may be required (e.g. for switching to a free product with fewer functions).

2. **Build IT skills**: The intended degree of vertical integration must be matched with the required IT capabilities. Extensive in-house development requires the corresponding developer resources. For development carried out externally, points
of contact must be established to coordinate, and interact with, OSS communities, for example. Appropriate skills and in-house staff are required for embedding new solutions in the existing IT landscape and for developing and implementing security concepts or software distribution – regardless of how and where the software is procured. Internal skills are also required to better understand, assess and implement future trends (e.g. by getting actively involved in OSS communities) in order to reduce dependence on the innovation initiatives of major software vendors.

3. **Ensure user acceptance**: Long-term success in the migration to alternative software can only be achieved jointly with end users. A significant factor in this regard is the functionality of the software. For core activities, the new product should be at least equivalent to or, for best results, even easier to use than the software to be replaced. In this context, it is helpful to define the users’ most relevant process steps when introducing the product and to leave less critical functionalities aside. In addition, agile approaches, including early testing of solutions together with users, will help to improve acceptance of the new software. Change management should also be used to create transparency (e.g. about potential start-up problems) and shared objectives should be formulated together with users. To improve acceptance further, comprehensive training is needed.

4. **Proceed step-by-step, create moments of success**: Once the decision to introduce alternatives has been taken, these should be rolled out step-by-step in order to test the new solution on a technical and organisational level, and to avoid the risks associated with a "big bang" approach. By developing proofs of concept, success can be achieved and announced quickly, which will additionally facilitate the migration. After successful piloting, the solution should be rolled out in the entire organisation. In doing so, it is necessary to clearly define the time horizon. Achieving independence from individual vendors is not a short-term endeavour; it requires time to reach technical and organisational maturity.

5. **Use the community**: In the case of OSS, the community is an integral part of the product and its development, because responsibility often lies not with individual vendors, but is shared by a collective of users, developers and service vendors. In order to make use of and maintain the innovation capacity and manpower of this group, the community should be actively involved in the process (e.g. by inviting it to contribute ideas, development output, financial resources). However, such an approach will require staff, time and investment and must therefore be reflected in the planning process. Solutions that diverge from publicly maintained OSS variants (known as "forks") for use in separate development activities in your own organisation should be avoided, because this will lead to a loss of the skills which the developer community and other users can contribute.

6. **Achieve critical user mass**: The establishment of a user group that is as large as possible will create benefits of scale and visibility. The long-term aim of a full
Migration is to avoid the operation of several systems in parallel in order to cut down the number of interfaces and reduce complexity and IT costs at the same time. Furthermore, a broader user base improves the exchange of experience between users and facilitates collaboration.

**Case study:** Starting in 2003, the City of Munich migrated to an open-source operating system (Linux) and open-source office software (OpenOffice, subsequently LibreOffice). In response to emerging trends, it was decided in the context of Munich’s digital transformation planning in 2017 and 2018 to reverse the migration for economic, technological and strategic reasons.

The main objectives of the introduction of Linux at the time were autonomy and cost savings, although the solution was ultimately not cost-effective due to high development costs and the limitation of its scope to the City of Munich (SF1&6). In addition to major losses of productivity in the departments, IT costs also increased considerably since approximately 1/3 of users in Munich remained on the Windows operating system for the specialist applications they required. This meant that two operating systems had to be permanently supported by the IT department. Another reason was the recruitment of more than ten internal employees for (further) software development (e.g. of the in-house WollMux solution) and maintenance, including the costs entailed (SF2). The parallel operation of different solutions, the functional gap compared to Microsoft products (perceived as very wide) and non-compatibility with other solutions also led to very low acceptance among users (SF3). Although the solution had been successfully rolled out step-by-step via individual user groups (SF4), there was no close exchange with a community, because the City was working with a highly individualised version of Ubuntu. This led to high demand for internal developers and made the solution uneconomical (SF5). The main reasons for reversing the migration were the costs incurred in IT, high productivity losses suffered in the departments, a lack of support for specialised Linux applications, as well as considerable risks, as the entire IT operation of the City of Munich depended on in-house developers. Furthermore, all the City’s cooperation partners had meanwhile abandoned the project, leaving Munich as the last remaining user of the Linux version.
Case study: Since 2004, the French Gendarmerie has been gradually replacing parts of its software stack with open-source software which makes up the majority of the stack today.

Cost savings, which had been the key objective of the project from the outset, have been achieved (SF1). Internal capacities established for using open-source software are responsible for integrating new community updates (e.g. Ubuntu) and modifying existing open-source software (e.g. Android). Since the modifications are mainly limited to the configuration, two additional employees (for Linux and LibreOffice) are sufficient (SF2). The solutions focus on the main core functionalities of the largest user group, the police officers of the Gendarmerie. This group is very mobile, and the focus is therefore on web-based and smartphone applications. The fact that the Gendarmerie’s main application is platform-independent facilitated the switch of the operating system. No special training was required (SF 3). A number of solutions were tested and rolled out over several years, beginning with OpenOffice (subsequently LibreOffice), followed by Firefox, Thunderbird, Linux and other products (SF4). Ubuntu, the Linux distribution used for the desktop operating system, was modified only slightly (in the configuration and packaging) in order to be able to use updates from the open-source community and thus benefit from the community’s manpower and innovative capacity (SF5). With 80,000 users (approximately 90% of the organisation), a critical user mass was reached. However, it was primarily police stations that were migrated, while more than 10,000 administration users continue to work with Microsoft products (SF6).

7 Courses of Action to Reduce Dependence

Similar projects in other organisations have shown which strategies they pursue to reduce dependence and which factors can drive success. Both can be used to identify courses of action the Federal Administration can adopt:

Option 1: Establish basic conditions

Basic conditions are the foundation for any concrete measures to achieve independence from individual vendors. They create the required awareness within the organisation and, at the same time, provide a framework for action for other players (e.g. Federal States, local authorities or private companies). Building knowledge and creating transparency for employees will generally increase acceptance of new products among users. The Federal Office for Information Security has already declared its strategic position on free open-source software (FLOSS) and makes such software available. So far however, few other authorities have followed suit. Such an example shows that, although it is important to create the right basic conditions, they will not produce the desired result unless concrete measures are taken towards implementation.
Option 2: Negotiate

Negotiations with Microsoft on product or contract modifications are another option for reducing dependence. This does not require any technical effort on the part of the Federal Administration. However, this course of action can only produce the desired result if Microsoft is prepared to make concessions and implements them. What is more, negotiations can only alleviate pain points – the underlying dependent relationship with the vendor continues unchanged. Moreover, negotiation results have a time limit, e.g. due to contract durations, and do not solve problems permanently. In addition, contractual arrangements can only be agreed to the extent that the parties are authorised to do so. This applies, for example, to "no spy" clauses. Existing and potential future requirements or prohibitions imposed by law or by the authorities under US law cannot be evaded by the IT vendors based there. The most recent developments in the negotiations between the Federal Administration and Microsoft have, however, raised doubts about whether negotiations alone can bring success. Even after several rounds of negotiations, particularly about the security of cloud-based products, no agreement has been reached. A joint front of the Federal Government and the Federal States could strengthen the Federal Administration’s negotiating position and make this course of action more effective.

Option 3: Diversify with proprietary software

In addition to organisational measures, the Federal Administration could also replace software that creates critical dependence and use other proprietary products instead. In principle, the market offers alternatives in many software layers, but the risk of creating a new dependence remains. Given numerous concerns about information security relating to US software vendors (due to the CLOUD Act and the consequences of the trade embargo against Huawei), this course of action promises only limited success. It would, moreover, make the Federal Administration’s IT landscape more complex and thus conflict with the key objective of the IT-K Bund initiative.

The development of its own proprietary software would therefore also be conceivable, although that would require the creation of extensive development capacities and could probably not be achieved by the Federal Government’s IT service vendors alone. Alternatively, the Federal Administration could make an equity investment in, or acquire, a software vendor. First of all, this would require an appropriate acquisition target and incur a high financial risk, since the software would first have to be developed to an adequate standard. In addition, there is a risk that in-house development will not be able to keep up with the faster pace of innovation in the market.

In general, diversification into proprietary software of other manufacturers could create new dependence, while in-house developments would require high financial investments.
Option 4: Build OSS alternatives

Another possibility to reduce dependence is the use of OSS. Many examples show that such a solution could be workable, provided that the appropriate success factors are observed. The development effort required varies depending on the intended level of vertical integration. The Federal Administration could in many places make use of existing OSS solutions offering extensive functionality, thus limiting its own development effort. However, even if existing solutions are used, the need to build the skills for performing software maintenance and modifications, for interacting with OSS communities, or for managing external service vendors will persist. Under the IT-K Bund initiative, this role could be assumed by the Federal Government’s IT service vendors. Ultimately, this option may conceivably lead to permanent independence from major vendors. If the OSS option is chosen, the large benefits of digital sovereignty are offset by the associated risks: other projects have shown that extensive modifications (e.g. to achieve compatibility with specialist processes) and culture change may be required in the development and use of software.

8 Recommended Further Action

This strategic market analysis provides a framework for assessing dependence on software vendors. The assessment made on this basis shows that the Federal Administration is critically dependent on Microsoft. Possible strategies, success factors and the appropriate courses of action to be adopted by the Federal Administration can be derived from the measures other organisations have taken to reduce dependence on Microsoft. The results of the analysis emphasise the need to act, which requires prompt decisions on how to proceed. With this in mind, it is recommended to analyse the instances of dependence in greater detail and initiate selected actions.

Further in-depth Analysis

Based on the framework provided in chapter 3, dependence and pain points should be analysed in more detail and existing results should be complemented and validated with additional data. In order to identify other critical cases of dependence, the analysis should be expanded to include other vendors.
Adoption of Courses of Action

The following steps are recommended for this purpose:

1. **Assessment and Selection of one or more Courses of Action**

   The available courses of action must be analysed in more detail and rated according to the criteria relevant to the Federal Administration. Significant projects conducted by other organisations should be analysed in greater depth. The decision for adopting a particular course of action can be taken on this basis. Some of the actions can also be combined (e.g. negotiations and building OSS, or the use of OSS to build a proprietary in-house solution). The following two steps will only be necessary if there are plans to replace products.

2. **Technical Analysis and Planning**

   Depending on which course of action is adopted, a more in-depth analysis is needed to establish which activities and consequences the Federal Administration would face, e.g. for its IT architecture, organisation and processes. This process should start with a detailed review of the software stack, e.g. in terms of the products used, possible alternatives, interdependencies or separability. Proof of concept projects will then have to be conducted to test potential technical solutions. On this basis, a concept should be developed and plans drawn up for implementing the solution.

3. **Conception and Implementation**

   The concept, which should include a clear target vision, should form the basis for presenting details of the products to be replaced, the intended level of vertical integration, affected user groups and potential operating models. The concept should take into account the success factors described in chapter 6.2. For example, the potential stages (e.g. the sequence of user groups or products to be migrated to the target solution) should be assessed in terms of their technical and organisational implications and planned accordingly. All stakeholders must be closely involved during both the concept phase as well as the implementation to ensure a critical mass. The stakeholders may include vendors, OSS communities or strategic alliances between the Federal Government and the Federal States or within the EU. Any linkages to the IT-K Bund initiative must also be taken into consideration.

---

45 E.g. coverage of functional requirements, contribution to reducing pain points, risk, feasibility, costs (migration/operation).
Final Considerations

The market analysis shows that the Federal Administration is highly dependent on the software vendor Microsoft. This may have critical consequences which are likely to accumulate further, given the development of the market. As a result, there is an urgent need for action, for which the Federal Administration can take inspiration from a large number of similar initiatives taken by other organisations and apply identified success factors to finding its own solutions. The courses of action mapped out should be assessed and implemented promptly in order to reduce the cases of dependence which were identified as critical. They would be an appropriate tool to achieve the Federal Government’s strategic IT objectives and to ensure the Federal Administration’s digital sovereignty in the long term.
9 Legal Notice

Dependence on Individual Software Vendors – Strategic Market Analysis

Last updated: 23 August 2019

Study commissioned by the Federal Ministry of the Interior, Building and Community (Bundesministerium des Innern, für Bau und Heimat)

PwC Strategy& (Germany) GmbH Kapelle-Ufer 4 10117 Berlin Germany

In case of discrepancies between the German original version and the English translation, the German version shall prevail.
Strategy&

Strategy& is the global strategy consulting business of PwC. We develop individual business strategies for globally leading companies, based on differentiating competitive capabilities.

We are the only strategy consulting business that is part of a global professional services network. We combine our expertise with technology and develop a suitable strategy that can be efficiently implemented.

For us, "strategy, made real" means driving the digital transformation, helping to shape the future and turning visions into reality. 3,000 strategy consultants and over 250,000 PwC employees in 158 countries contribute to this by providing high-quality, industry-specific services in the areas of auditing, tax and management consulting. Please see www.strategyand.pwc.com/de for more information.