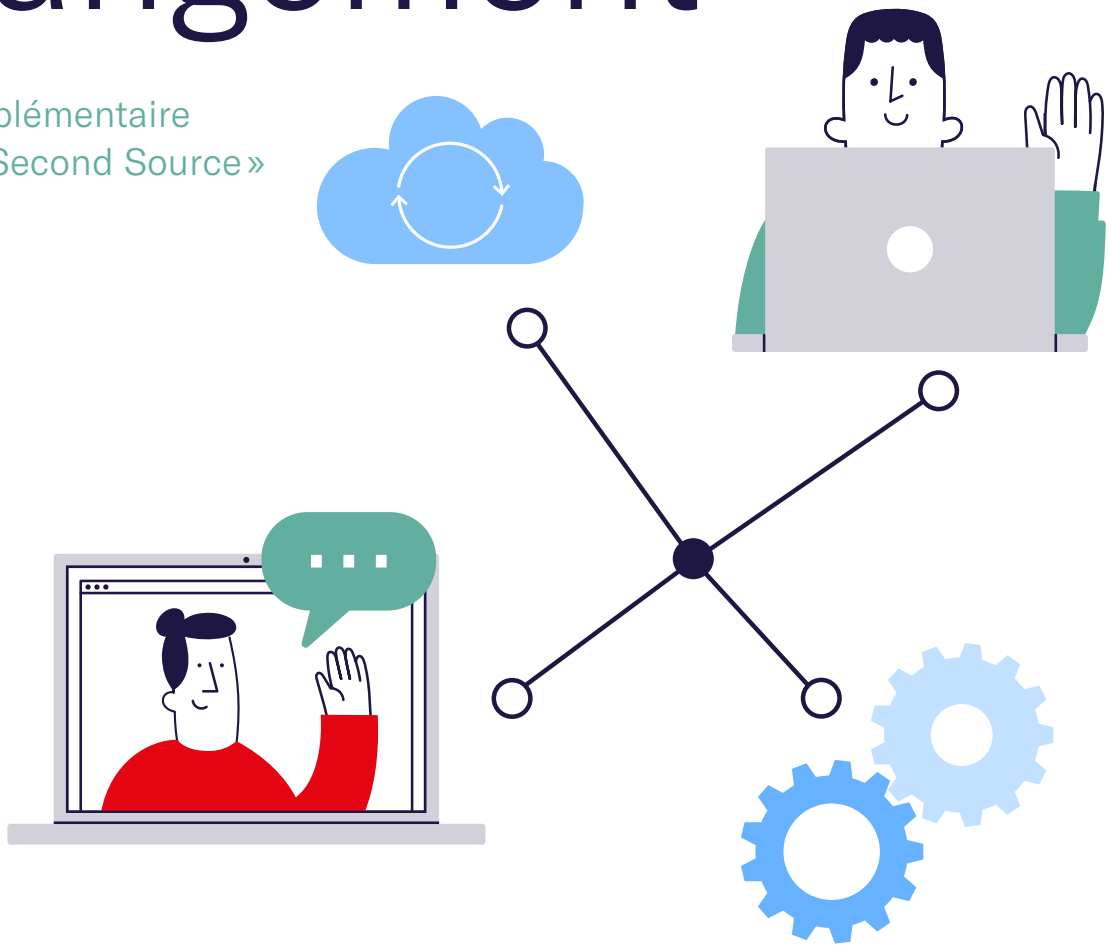
Digitale Verwaltung Schweiz
Administration numérique suisse
Amministrazione digitale Svizzera

Alternatives à M365 et conséquences en cas de changement

Étude complémentaire
à l'étude « Second Source »



Septembre 2026

Alternatives à M365 et conséquences en cas de changement

Étude complémentaire à l'étude « Second Source »

Date	18 septembre 2026
Auteurs	Eraneos Switzerland (Severin Kefer, Lioba Gasser, Nicolas Marxer, Jean-Jacques Pittet, Marc Raum, René Fitterer)
Mandante	Secrétariat de l'Administration numérique suisse (Andreas Burren)
Participants	Dominik Freitag, canton d'Argovie ; Alain Meyenberg, canton de Berne ; José M. Sánchez Knaack, canton de Genève ; Falko Gieldanowski, canton de Soleure ; Urs Bühler, canton de Bâle-Campagne ; Fabian Schmid, Principauté de Liechtenstein ; Greg Hernan, Secrétariat de l'Administration numérique suisse

Table des matières

1 Condensé

La présente étude « Alternatives à M365 et conséquences en cas de changement » fait suite à l'étude « Seconde source » publiée en avril 2025. Elle offre aux décideurs de l'administration publique une base factuelle pour évaluer en toute connaissance de cause un éventuel remplacement de Microsoft 365 (M365) par une autre solution.

Elle s'adresse aux responsables politiques et techniques de la Confédération, des cantons, des villes et des communes ainsi qu'aux spécialistes des acquisitions, de la numérisation et de la protection des données.

Elle ne remplace pas une évaluation spécifique à une organisation, mais permet une compréhension commune des interactions à prendre en considération lors de l'évaluation des solutions alternatives à M365.

1.1 Contexte et mandat

Cette étude complémentaire fait suite à l'étude « Second Source » du groupe de travail Cloud Governance et Workplace de l'Administration numérique suisse (ANS), publiée en avril 2025. Eu égard au débat sociétal et politique persistant sur l'utilisation de M365, un groupe de responsables informatiques cantonaux a suggéré une analyse approfondie des conséquences d'un changement. Le secrétariat de l'ANS a ensuite mandaté l'étude.

Les coûts directs liés à M365 ne constituent pas à eux seuls la principale motivation ; il convient également d'examiner dans quelle mesure les dépendances structurelles à certains prestataires influent sur la capacité d'action de l'administration au sens de la souveraineté numérique. L'accent est mis sur les principales fonctions bureautiques et collaboratives modernes, les courriels, le calendrier, l'archivage des documents, la coopération et les conférences audio et vidéo, ainsi que sur les intégrations pertinentes dans l'écosystème M365, à savoir la gestion des identités et des accès ainsi que la sécurité et la conformité. Les produits Microsoft ne relevant pas du portefeuille M365 et les services d'infrastructure et de plateforme du nuage Azure n'ont pas été examinés.

1.2 Procédure et méthodologie

L'étude complémentaire examine le remplacement éventuel de M365 sous quatre aspects : technique, organisationnel, réglementaire et financier. La souveraineté numérique n'y est pas abordée de manière autonome, mais comme une dimension transversale ancrée dans les quatre domaines analysés. Ces quatre aspects ne donnent donc pas une définition de la souveraineté numérique. Ils permettent en revanche de mieux évaluer les conséquences qu'entraînerait un changement de niveau de souveraineté.

Pour garantir la pertinence pratique et la transférabilité des résultats de l'étude, deux unités de taille différente ont fait l'objet d'une analyse approfondie : une administration cantonale employant près de 6000 personnes et une administration de taille moyenne d'environ 1500 personnes. Les résultats ont été comparés à l'aide d'un questionnaire standardisé à cinq autres administrations cantonales en qualité de partenaires de validation.

Pour obtenir une évaluation solide, une solution alternative concrète (openDesk de ZenDiS) a été étudiée de manière détaillée à titre représentatif. Sélectionnée uniquement comme illustration d'une suite logicielle dont le code source est ouvert, elle ne constitue pas une quelconque recommandation. La méthodologie et les enseignements peuvent toutefois être transposés à d'autres solutions alternatives.

1.3 Principaux enseignements de l'étude

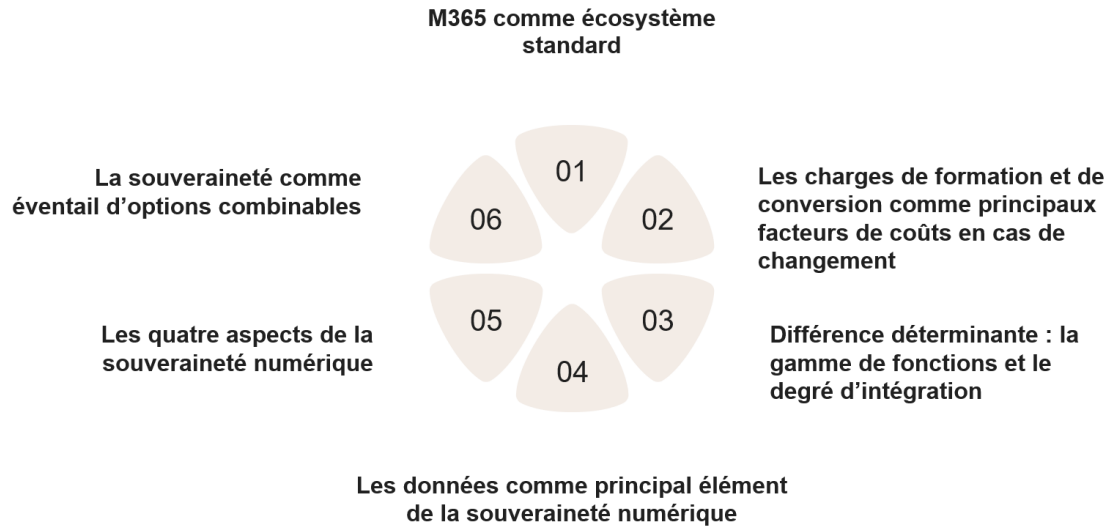


Figure 1 : Principaux enseignements de l'étude

1. Remplacer M365 par une autre solution implique non seulement de changer de produit, mais également de passer d'un écosystème à un autre. Or, celui-ci englobe aussi les différents fournisseurs : il n'existe actuellement guère de prestataires capables de couvrir de manière comparable l'univers M365. L'utilisation actuelle de M365 résulte de l'intégration d'un écosystème numérique qui a été systématiquement développé année après année. Les applications spécialisées, l'architecture informatique et les méthodes de travail du personnel se fondent toutes sur sa logique opérationnelle. Par conséquent, la dépendance existante n'est pas uniquement d'ordre technologique ; elle est également sociotechnique et organisationnelle. Les développements observés en Allemagne révèlent néanmoins que le marché des solutions à code source ouvert progresse au poste de travail et que des écosystèmes alternatifs peuvent être mis en place progressivement (voir point 2.1). Il est en principe possible de changer d'écosystème.
2. Dans le scénario étudié, la principale charge directe recensée d'un changement découle du temps de formation et de conversion induit. Les coûts uniques les plus importants ne résultent pas de la migration technique, mais du temps durant lequel le personnel est formé et ne peut dès lors pas accomplir ses tâches spécialisées. En l'espèce, les

partenaires de l'étude tablent sur quatre à cinq jours par personne, pour autant que les fonctions existantes soient intégralement remplacées. S'y ajoutent des coûts indirects sous la forme de pertes de productivité, qui vont au-delà du temps de formation effectif : après le changement, il faut s'attendre à une période de moindre productivité jusqu'à ce que le rythme de travail habituel soit de nouveau atteint, période durant laquelle les procédures usuelles doivent être réapprises et les routines, rétablies. Ce poste de coûts est peu pris en compte dans le débat actuel, car il n'est pas aussi visible que les coûts classiques d'un projet, d'une licence ou d'une acquisition.

3. La différence entre M365 et les solutions alternatives tient moins à la palette de fonctions qu'au degré d'intégration. L'exemple d'openDesk révèle que ces solutions peuvent proposer les principales fonctions de base. En l'état actuel des choses, une comparaison directe montre que M365 offre toutefois une palette de fonctions plus étendue et un degré d'intégration natif supérieur. De plus, ces solutions alternatives présentent encore des lacunes, notamment dans les domaines suivants : sécurité et conformité, informatique décisionnelle, développement *low code* et automatisation, gestion des appareils mobiles et fonctions d'intelligence artificielle (IA) intégrées en continu. Ce qui est disponible nativement, de manière standardisée et avec une charge raisonnable est déterminant pour l'évaluation ; l'évolutivité future et les capacités de production utilisables actuellement ne doivent par conséquent pas être mises sur le même plan lors de l'analyse. Par ailleurs, une approche modulaire ouverte accroît la marge de manœuvre pour réduire les dépendances vis-à-vis des fabricants, mais accentue la complexité de l'écosystème.
4. Les données sont au cœur de la souveraineté numérique. La capacité d'une unité administrative à conserver le contrôle de ses données est un aspect important de sa souveraineté numérique. Elle est mesurée en examinant la disponibilité, l'intégrité et la confidentialité des données, notamment à l'aune du lieu de stockage, du droit applicable et de la transférabilité. Une solution alternative ne doit donc pas être évaluée sur la seule base de ses fonctionnalités, mais également par rapport à cette garantie du contrôle des données. Les lacunes fonctionnelles demeurent pertinentes et sont appréciées en lien avec le contrôle des données.
5. Les conséquences d'un changement de niveau de souveraineté ne se laissent appréhender que de manière globale. Si les quatre aspects retenus ne définissent pas la souveraineté numérique, ils rendent évaluables les conséquences d'un tel changement. Seule la prise en compte commune de ces quatre aspects (technologique, organisationnel, réglementaire et financier) permet de déterminer si ces conséquences sont supportables. Ces aspects sont en outre subordonnés les uns aux autres : un bénéfice réglementaire au niveau de la souveraineté des données peut avoir des conséquences organisationnelles, se répercuter sur l'architecture d'un point de vue technologique et être mesurable financièrement. Il n'existe actuellement ni définition uniforme et exhaustive, ni bonnes pratiques établies pour cette vue d'ensemble. De plus, la pondération des différents aspects varie d'un cas à l'autre. Une évaluation limitée à un seul aspect comporterait des angles morts et pourrait engendrer des décisions erronées.

6. La souveraineté numérique n’est pas un état que l’on atteint ou que l’on rate complètement, mais peut se décliner à travers un éventail d'options combinables, à différents niveaux d'ambition. Ces options se distinguent par le degré d'indépendance atteint, mais ne doivent pas être comprises comme une hiérarchie entre elles. Ce qui importe, c'est de déterminer quelle option est appropriée pour chaque domaine fonctionnel :
   - Option 1 – Exploitation contrôlée et atténuation des risques : les solutions existantes continuent d’être exploitées en tant que risque connu, évalué et accepté.
   - Option 2 – Mise en place d’options de seconde source : parallèlement à l’exploitation existante, des solutions alternatives peuvent être mises en place en tant qu’environnement de réserve ou de secours.
   - Option 3 – Changement partiel ou total : lorsque cela est justifié sur le plan stratégique, soutenu sur le plan politique et viable sur le plan financier, une transition vers des solutions alternatives peut avoir lieu. Celle-ci peut se faire de manière échelonnée en fonction du profil de risque, par exemple pour des plateformes ou des applications métier spécifiques, ou mis en œuvre de manière systématique dans l’ensemble de l’organisation ou de plusieurs organisations.

   Il revient à chaque administration de décider de manière autonome, dans le cadre de ses objectifs politiques et stratégiques, quelle option est appropriée pour chaque domaine fonctionnel.

1.4 Ordres de grandeur financiers

Les informations suivantes illustrent les conséquences financières potentielles d’un passage de la plateforme M365 actuellement en place à une alternative basée sur des logiciels libres (OSS) telle qu’openDesk, sur la base d’une analyse approfondie des deux entités étudiées. Selon les résultats de l’étude, les coûts annuels totaux d’une solution alternative comme openDesk sont sensiblement similaires à ceux de la suite de produits M365 actuellement utilisée.
Les économies notables réalisées sur les seuls frais de licence sont largement compensées par les nouveaux postes de coûts, en particulier en raison du développement et de l’exploitation d’une couche de sécurité autonome et des charges d’intégration et d’harmonisation accrues.

Les coûts uniques de transformation ponctuels s’élèvent, dans les deux entités étudiées, à environ sept à huit fois le budget annuel de M365, soit au moins 25 à 30 millions de francs dans la plus grande entité et au moins 9 millions de francs dans celle de taille moyenne, pour une période d’introduction présumée de 4 à 8 ans. Ces ordres de grandeur englobent essentiellement l’adaptation des applications spécialisées et des données, la formation et son appropriation par les collaborateurs, ainsi que le conseil externe et la validation ; ne sont pas pris en compte ici d’autres effets tels que les pertes de productivité après la formation ou les coûts supplémentaires liés à l’exploitation en parallèle pendant la période d’introduction.
Les partenaires de validation de l’étude confirment ce modèle de base. Ces valeurs doivent être considérées comme étant purement indicatives dans le scénario étudié. En fonction des objectifs concrets et de l’architecture système existante, le remplacement ou la mise en place de

capacités en dehors de la suite de base peut engendrer des charges supplémentaires, en particulier dans les domaines suivants : sécurité et conformité, gestion des identités et des accès, gestion des appareils et applications mobiles, conformité des *clients*, déploiement logiciel, centre de surveillance de la sécurité et intégrations plus étendues. Dans des cas précis, les coûts de transformation effectifs peuvent être sensiblement plus élevés. Le principal indicateur financier n'est donc pas tant la différence des coûts courants que la transformation unique et la future volonté politique de prendre en charge des coûts uniques subséquents élevés, voire des coûts récurrents supplémentaires, en vue d'une souveraineté accrue.

1.5 Conclusion

L'étude complémentaire renonce sciemment à formuler une recommandation générale en faveur du passage à une solution alternative ou contre celui-ci. Il en ressort qu'il s'agit non seulement de changer une suite de produits, mais également de migrer d'un écosystème très intégré vers un ensemble de solutions modulaires. En l'état actuel des choses, le remplacement complet de M365 à court terme est irréaliste en l'absence de volonté politique de prendre en charge les coûts supplémentaires induits, l'accroissement notable du personnel ainsi que les réductions et lacunes fonctionnelles significatives.

Il est recommandé aux unités administratives d'étudier la question de manière structurée dans leur propre organisation, en tenant compte non seulement des produits, mais également des écosystèmes, des dépendances, des modèles opérationnels et des conséquences organisationnelles et en analysant de manière approfondie les approches graduelles. L'accent sera davantage mis sur une comparaison de ces facteurs que sur une comparaison technique entre M365 et une solution alternative, afin de déterminer le niveau de souveraineté approprié pour l'unité et la solution adéquate en la matière. L'option retenue reste une décision politique. La présente étude complémentaire se borne à fournir une base objective.

2 Résultats détaillés de l'étude

2.1 M365 comme écosystème standard

L'utilisation actuelle de M365 dans les administrations publiques ne se résume pas à l'emploi de différentes applications et doit être considérée comme une intégration dans un écosystème numérique faisant l'objet d'un développement systématique. C'est l'un des enseignements majeurs de cette étude. Ce développement n'est pas le fruit du hasard ; il résulte d'une approche suivie depuis des années qui privilégie les solutions intégrées, standardisées et dont l'exploitation est relativement efficace. Au fil des ans, une interaction étroite entre la bureautique, la collaboration, l'archivage des documents, la gestion des identités, la sécurité, la conformité, l'autorisation et le système d'exploitation s'est établie. Cette intégration se reflète non seulement dans l'architecture technique, mais également dans les modèles opérationnels, les compétences organisationnelles, les structures de soutien et le travail quotidien du personnel.

Les évaluations des unités examinées et des partenaires de validation révèlent que cette intégration déploie désormais des effets standardisés. Les applications spécialisées sont liées à l'écosystème Microsoft, les organisations informatiques internes s'appuient sur sa logique d'exploitation et des attentes et modes d'utilisation correspondants sont ancrés au sein du personnel. Loin d'être uniquement d'ordre technologique, la dépendance existante illustre la longue croissance d'une dépendance sociotechnique et organisationnelle en lien avec les solutions techniques.

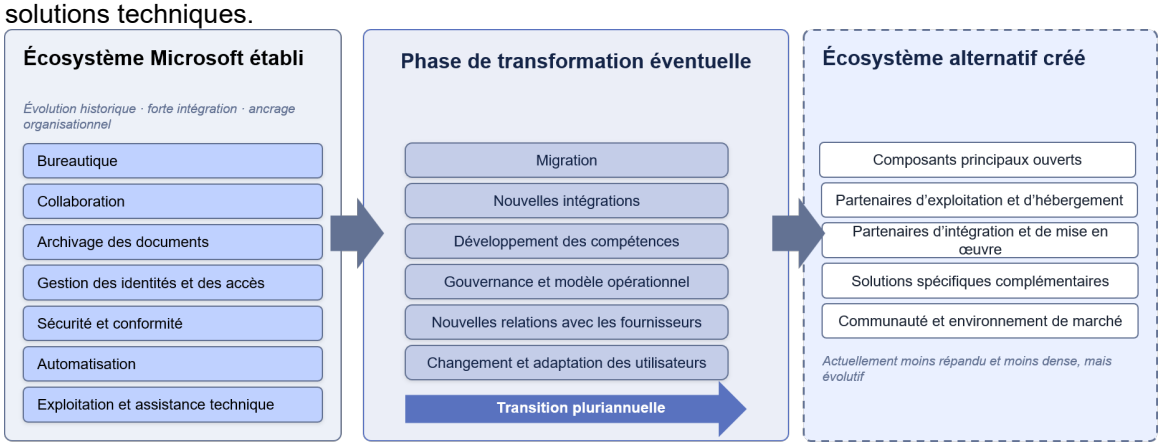


Figure 2: Mutation des écosystèmes

Dans le même temps, l'étude révèle que ces écosystèmes ne sont pas statiques. Mis en place de manière systématique, ils peuvent changer en fonction de l'évolution des conditions politiques, réglementaires et de marché. Les évolutions observées en Allemagne soulignent que le marché des solutions à code source ouvert au poste de travail présente un potentiel de développement considérable et que des écosystèmes alternatifs peuvent être réalisés progressivement. En principe possible, l'adoption d'une solution alternative à M365 ne doit pas être considérée comme un simple remplacement de produit, mais comme une transition à long terme entre un écosystème établi et un nouvel écosystème à développer.

L'utilisation actuelle de M365 illustre un écosystème développé de manière systématique, qui s'est établi non pas par hasard, mais en raison de ses avantages en matière d'intégration, de sa standardisation et de son efficacité opérationnelle. Des écosystèmes alternatifs peuvent se développer, mais cela nécessite du temps, de la coordination et des investissements ciblés.

2.2 Les charges de formation et de conversion comme principaux facteurs de coûts d'un changement

Autre enseignement majeur de l'étude, les principaux coûts d'introduction uniques induits par un changement des fonctions familières aux utilisateurs du poste de travail numérique ne découlent pas en premier lieu des travaux techniques de migration, mais du temps consacré à la formation du personnel, durant lequel celui-ci ne peut pas accomplir ses tâches spécialisées usuelles. Dans les analyses financières des unités examinées, ces charges constituent le poste le plus important des coûts de transformation directs.

Il ne s'agit pas ici, en premier lieu, des charges induites par l'élaboration des documents de formation ou le financement des formateurs, mais des charges de personnel connexes au niveau de l'administration. Est déterminant en la matière le fait qu'un grand nombre de collaborateurs doive être formé pendant plusieurs jours et ne peut alors pas accomplir ses tâches régulières ou ne peut les exécuter que de manière restreinte. En l'espèce, les partenaires de l'étude tablent sur des charges de formation et de conversion d'environ quatre à cinq jours par personne, pour autant que les fonctions actuellement couvertes par l'environnement Microsoft soient intégralement remplacées par de nouveaux outils.

Ce poste de coûts peut être calculé de manière simple, méthodique et transparente. Il découle essentiellement du nombre de journées de formation par personne, du coût total du personnel par jour de travail et du nombre de collaborateurs concernés. La principale incertitude résulte donc moins de la logique de calcul proprement dite que de l'élaboration d'hypothèses plausibles quant à l'ampleur et à la durée de la formation requise. Ce constat ne s'applique cependant pas à l'identique aux projets de migration touchant principalement la partie serveur (*backend*). Dans ce cas précis, le besoin de formation direct des utilisateurs finaux est souvent faible, tandis que les dépendances techniques avec les systèmes périphériques, les interfaces et les structures d'identification et d'accès ainsi que les charges supplémentaires d'intégration, de test et d'exploitation peuvent être considérables.

Dans la pratique, ces charges sont fréquemment sous-estimées, car elles ne sont pas aussi visibles que les coûts classiques d'un projet, d'une licence ou d'une acquisition. Pour évaluer un changement de manière réaliste, il est donc indispensable de présenter explicitement le temps de formation induit du personnel comme un poste de coûts autonome, sans oublier les charges logistiques (par ex. locaux nécessaires).

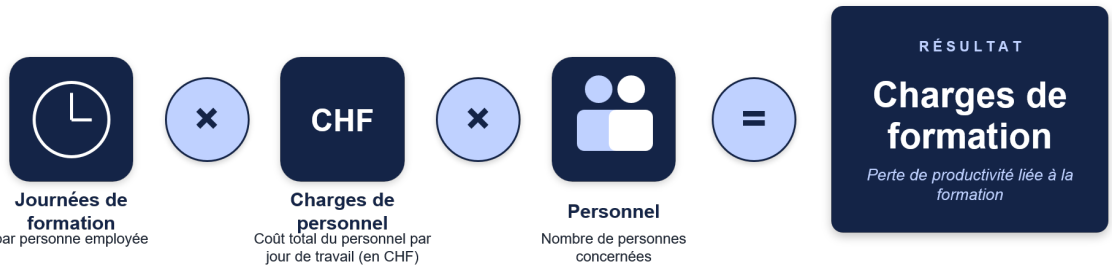


Figure 3 : Charges de formation — faciles à calculer méthodiquement

En plus des charges de formation directement quantifiables, il faut tabler sur des coûts implicites, dont le calcul n'est pas aussi simple. À l'issue des formations, il convient de s'attendre à une période de moindre productivité jusqu'à ce que le rythme de travail habituel soit de nouveau atteint, période durant laquelle les procédures usuelles doivent être réapprises et les routines, rétablies. Cet effet concerne non seulement l'administration proprement dite, mais également la collaboration avec les utilisateurs d'applications spécialisées et les services externes qui s'étaient familiarisés avec les outils et méthodes de travail précédents. Ces pertes de productivité sont généralement peu prises en compte dans le débat actuel, car elles ne sont pas non plus aussi visibles que les coûts classiques d'un projet, d'une licence ou d'une acquisition, même si elles s'étendent au-delà du simple temps de formation sur le plan économique.

Le temps de formation du personnel constitue la principale charge directement quantifiable d'un changement. Elle ne découle pas en premier lieu des frais pour l'élaboration des cours et le financement des formateurs, mais du temps consacré à la formation du personnel, durant lequel celui-ci ne peut pas accomplir ses tâches ordinaires. Un tel changement engendre également des coûts indirects de transformation et de formation, par exemple sous la forme de pertes de productivité dues, notamment, aux ruptures de média, aux questions de compatibilité ou à la perte temporaire des routines établies.

2.3 Différence déterminante : la gamme de fonctions et le degré d'intégration

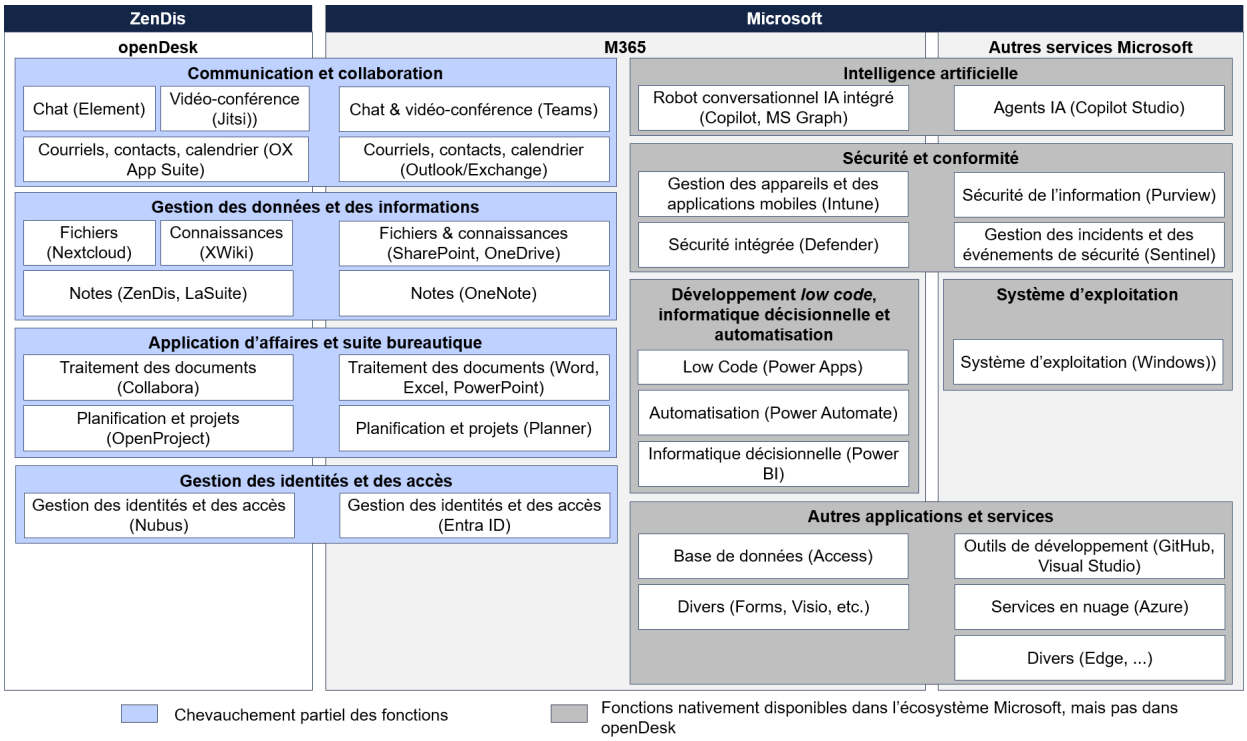


Figure 4 : Vue d'ensemble des fonctions d'un bout à l'autre du cadre technique

Structurée selon les groupes de fonctions du cadre et de la méthodologie technique exposés au point 3.2, la comparaison ci-après se réfère aux fonctions et au niveau d'intégration actuellement disponibles des solutions considérées. Elle illustre donc la performance technique observable, sans pour autant exclure que les fonctions absentes d'un écosystème ouvert puissent être complétées, acquises conjointement ou intégrées à des composants supplémentaires à l'avenir.

Dans ce contexte, openDesk couvre les fonctions bureautiques essentielles, tandis que M365 propose actuellement une palette de fonctions sensiblement plus vaste et un niveau d'intégration natif plus élevé. openDesk offre des solutions de base pour la communication et la collaboration, la bureautique, la gestion des fichiers et de l'information ainsi que pour la gestion des identités et des accès. L'étendue de ces fonctions suffit en principe dans les cas typiques de bureautique numérique. Il convient cependant de préciser que même dans les domaines où openDesk fournit des solutions de base, celles-ci n'ont pas toujours la portée et le degré de maturité des applications M365 établies. Par exemple, en ce qui concerne le tableur, le module Collabora d'openDesk ne peut actuellement pas remplacer entièrement Microsoft Excel. L'interopérabilité n'est par essence pas évaluée ici. À son stade actuel de développement, openDesk souffre par ailleurs de lacunes dans des domaines où M365 offre une véritable valeur ajoutée, notamment en matière de sécurité et de conformité, d'informatique décisionnelle, de

technologie *low code*, d'automatisation, de gestion des appareils et des applications mobiles et des fonctions IA intégrées en continu.

Toutefois, la principale différence ne réside pas tant dans l'étendue des différentes fonctions que dans le degré d'intégration choisi. M365 propose une plateforme très intégrée sur laquelle des services tels que Teams, Outlook, SharePoint, Entra ID, Purview, Defender ou Power Platform utilisent des identités, des autorisations, des interfaces et des modèles de données communs. Tout ceci est complété par un écosystème largement établi comprenant de nombreuses connexions avec des fabricants tiers, tandis qu'openDesk poursuit une approche modulaire basée sur plusieurs composants à code source ouvert. Cette approche offre en principe une marge de manœuvre, puisque les fonctions manquantes peuvent être ajoutées grâce à des modules supplémentaires, un développement commun ou une acquisition ciblée. L'ouverture technique et stratégique du modèle constitue donc une différence notable par rapport à la logique de plateforme de Microsoft, qui est davantage axée sur un fabricant.

Pour la présente classification, il est néanmoins essentiel que l'analyse ne place pas sur un plan d'égalité une éventuelle future possibilité d'extension et les fonctionnalités de la plateforme qui sont déjà disponibles dans l'environnement de production. Même si les fonctions peuvent être développées ou complétées dans un environnement dont le code source est ouvert, cela s'accompagne généralement d'exigences supplémentaires en matière d'architecture, de financement, d'acquisition, de pilotage, d'intégration et d'exploitation, notamment pour les fonctionnalités qui vont au-delà des fonctions principales et doivent être considérées comme étendues. Eu égard à la méthodologie technique considérée ici, la disponibilité native et standardisée actuelle des fonctions et intégrations et les coûts de mise en œuvre raisonnables sont donc déterminants.

Comme indiqué à la figure 4, les atouts d'openDesk proviennent surtout de la couverture des principales fonctions bureautiques et collaboratives, tandis que M365 propose dans plusieurs groupes de fonctions des prestations plus complètes et une intégration plus poussée au sein de la plateforme. Cela vaut notamment dans les organisations qui sont déjà fortement axées sur les services, interfaces et mécanismes de sécurité spécifiques à Microsoft. Dans le même temps, il convient de tenir compte du fait que le marché des logiciels à code source ouvert est encore relativement volatil et que des prestataires comme ZenDiS ne peuvent pas garantir des structures un tant soit peu comparables à celles de Microsoft concernant le groupe et le nombre de fournisseurs, le personnel dans des domaines spécialisés, le financement, etc. Cela n'exclut pas un développement ou une extension ciblée de la gamme de prestations, mais implique un degré de maturité, des conditions de mise à l'échelle et des modèles de responsabilité différents.

OpenDesk propose un socle pour les fonctions bureautiques numériques de base, qui peut être complété par des composants ouverts dans une perspective un peu plus lointaine. De plus, une approche modulaire ouverte peut contribuer à réduire les dépendances technologiques vis-à-vis de certains fabricants et à accroître la liberté de conception sur le plan stratégique. Dans le

marché actuel et la gamme de produits disponibles, M365 répond cependant à une palette d'exigences plus vaste et convainc en particulier lorsque des fonctions très intégrées immédiatement disponibles et un écosystème largement établi revêtent une grande importance.

> openDesk propose des solutions pour les fonctions bureautiques de base et peut contribuer, dans une perspective un peu plus lointaine, à réduire les dépendances vis-à-vis des fabricants grâce à son approche modulaire ouverte. Dans le marché actuel et la gamme de produits disponibles, des lacunes fonctionnelles et intégratives importantes demeurent cependant par rapport à M365, qui dispose actuellement d'une palette de fonctions plus étendue, d'un degré d'intégration sensiblement plus élevé et d'un écosystème mieux établi.

2.4 Les données comme principal élément de la souveraineté numérique

Autre enseignement majeur de cette étude, les données ont une importance particulière pour la souveraineté numérique. Cette dernière ne se mesure toutefois pas à l'aune des seules données, mais résulte de l'interaction de plusieurs éléments : sur le plan technique, du contrôle exercé sur les infrastructures, des interfaces disponibles ou manquantes et de l'interopérabilité ; sur le plan économique, des dépendances propriétaires, des effets d'enfermement propriétaire et de la liberté de décider des technologies ainsi que, sur le plan organisationnel, de l'auditabilité des solutions utilisées, de l'impact sur les processus de travail et la gouvernance et des compétences organisationnelles et personnelles existantes et à développer. Dans cette interaction, le pouvoir de disposer des données est particulièrement important : il est essentiel qu'une collectivité publique conserve le contrôle de ses données tant au niveau de l'infrastructure que lors du traitement par son propre personnel, indépendamment de l'application utilisée pour ce traitement.

Ce contrôle se concrétise à travers les objectifs de protection de la sécurité de l'information : disponibilité, intégrité et confidentialité[1]. Une collectivité publique conserve sa capacité d'agir lorsqu'elle peut les piloter de manière raisonnable et réaliser des changements si nécessaire. La garantie de ce contrôle dépend de facteurs indépendants de l'application : par exemple, le lieu de stockage, le droit applicable et la question de l'accès aux données. Les réglementations étrangères qui permettent un accès facilité des autorités aux données stockées à l'étranger témoignent de l'importance de cette question en matière de souveraineté.

[1] Voir rapport du Conseil fédéral en réponse au postulat 22.4411 Z'graggen « Souveraineté numérique de la Suisse », approuvé le 26 novembre 2025, URL: https://www.admin.ch/fr/newnsb/2VPWG78YrVs4eAVeiklQx, téléchargement au 14 août 2026.

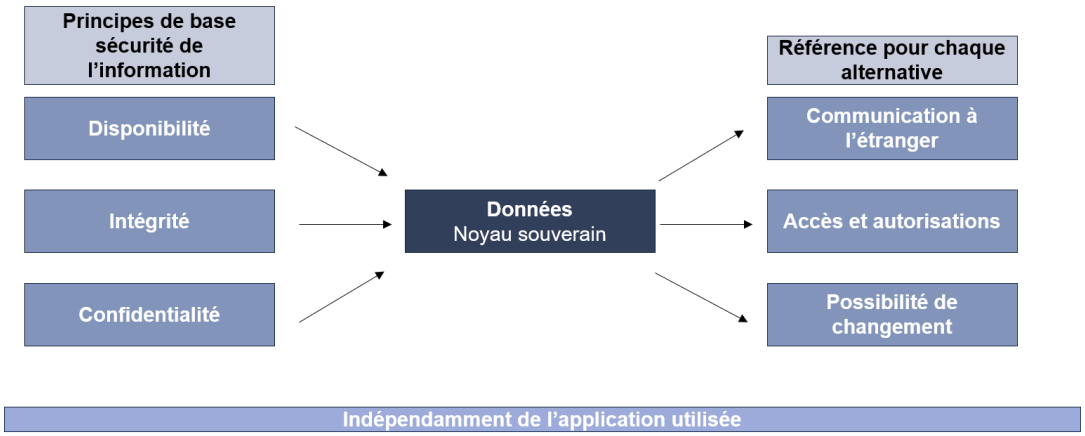


Figure 5 : Le contrôle des données comme référence

Il convient donc également d'évaluer si une solution alternative garantit ce contrôle : accès selon le droit suisse, lieu de stockage vérifiable et possibilité, pour l'exploitant, de changer de fournisseurs grâce à des formats ouverts et à des interfaces standardisées. La souveraineté ne se résume pas au contrôle des données. La disponibilité, la modularité et la sécurité des systèmes utilisés représentent des conditions autonomes. Lorsqu'elles ne sont pas remplies, il n'y a aucune souveraineté, même en cas de contrôle intégral des données.

Les lacunes fonctionnelles d'une solution alternative demeurent pertinentes, mais moins que le contrôle des données. Lorsque des données sont classifiées, gérées dans des formats ouverts et enregistrées dans des lieux vérifiables, la couche d'applications peut être complétée, remplacée ou combinée à un coût sensiblement réduit, pendant que les données, en tant qu'élément souverain, survivent aux changements d'outils et de prestataires.

Les données, et non les applications, déterminent la souveraineté numérique. Leur contrôle, leur disponibilité, leur intégrité et leur confidentialité sont des critères d'évaluation déterminants pour toute solution alternative. Ceux-ci priment l'étendue des fonctions d'une application.

L'exigence relative au contrôle des données n'est pas la même dans tous les domaines : le caractère critique d'un processus et le besoin de protection des données déterminent le niveau de souveraineté approprié. Les processus et données particulièrement sensibles ou souverains sont soumis à des exigences plus strictes que les processus de soutien, dont le besoin de protection est moindre.

2.5 Les quatre aspects de la souveraineté numérique

Les quatre aspects décrits ci-dessous ne définissent pas la souveraineté numérique, mais permettent d'évaluer les conséquences d'un changement de niveau de souveraineté au sein d'une administration. L'un des enseignements de la présente étude est que ces conséquences ne sont pas évaluables sur la base d'un seul indicateur. Elles se révèlent entièrement que lorsque les quatre aspects (technologique, organisationnel, réglementaire et financier) sont pris en compte en commun. Ceux-ci ne sont pas indépendants les uns des autres. Au contraire, ils se subordonnent mutuellement : une mesure apportant un avantage sous un angle précis modifie souvent le contexte sous les autres angles.

Les évaluations des unités examinées et des partenaires de validation rendent cette interaction tangible. Un bénéfice réglementaire en matière de souveraineté des données a des effets organisationnels sur le développement du savoir-faire et les modèles opérationnels, se reflète sur le plan technologique à travers l'architecture et la prévention d'un enfermement propriétaire et peut être quantifié sur le plan financier à l'aide des charges de transformation et d'exploitation. Aucune de ces perspectives ne peut être abordée isolément sans répercussions sur les autres.

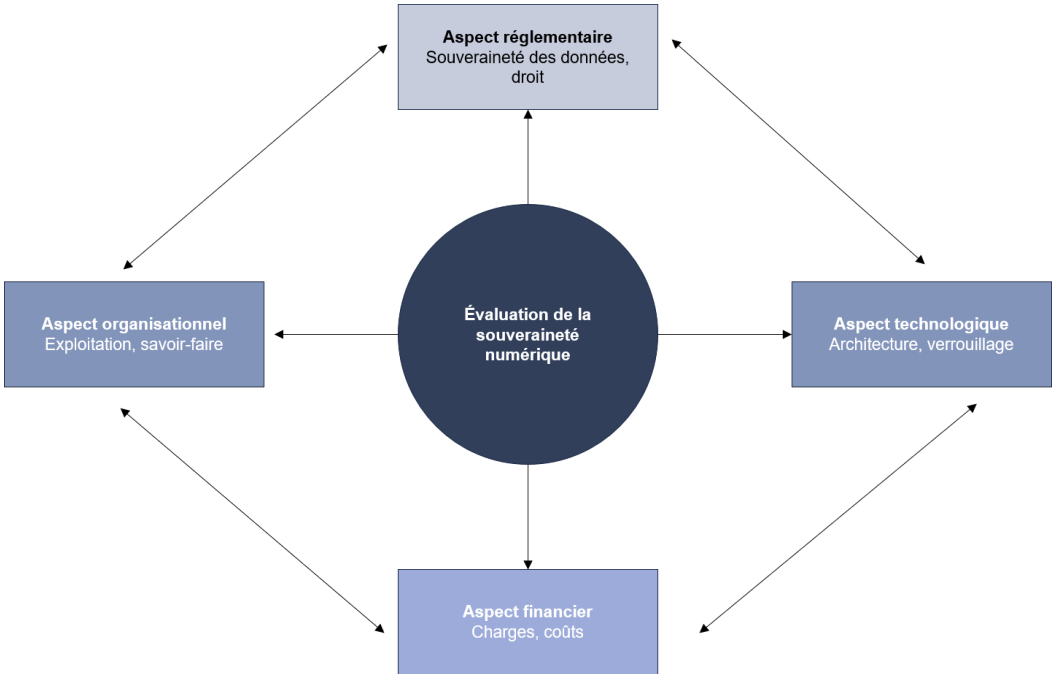


Figure 6 : Les quatre aspects de la souveraineté numérique

La figure 6 présente ces quatre aspects comme des éléments équivalents. Ils agissent conjointement sur la situation globale, tout en s'influençant mutuellement. Seule leur prise en compte commune fournit une vue d'ensemble du niveau de souveraineté dans un cas précis.

Cette interaction a une conséquence méthodologique : une évaluation limitée à un seul aspect, par exemple aux coûts ou à la situation réglementaire, comporterait des angles morts et risquerait d'engendrer des décisions erronées.

> Seule la prise en compte commune des quatre aspects (technologique, organisationnel, réglementaire et financier) fournit une vue d'ensemble permettant de décider de manière viable de la suite de la procédure.

2.6 La souveraineté numérique : un éventail d'options combinables

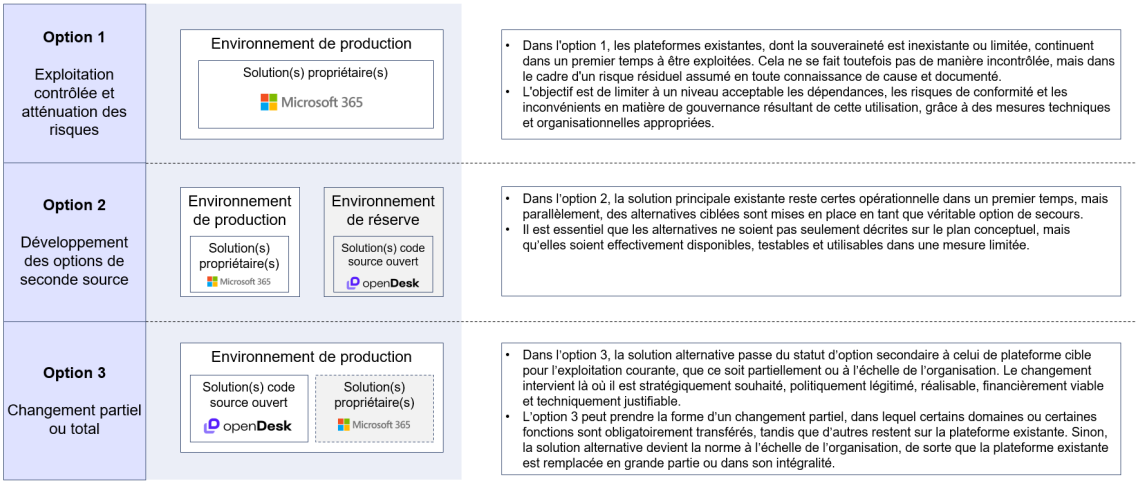


Figure 7 : Options pour la souveraineté numérique pour un poste de travail électronique

La souveraineté numérique n'est pas à comprendre comme un état que l'on atteint pleinement ou que l'on manque, mais comme le résultat d'options choisies de manière ciblée, à différents niveaux d'ambition. Dans le cadre de cette étude, trois options ont été définies ; elles se distinguent par le degré d'indépendance atteint, mais ne sont pas hiérarchisées les unes par rapport aux autres. Pour les administrations, il n'est en général ni réaliste ni judicieux de résilier d'un seul coup les dépendances numériques existantes. On distingue donc entre la poursuite contrôlée des solutions existantes, le développement ciblé d'alternatives et le passage effectif à un environnement cible alternatif, comme le montre la figure 7. Ce qui est déterminant à chaque fois, c'est de savoir quelle option est appropriée pour le domaine fonctionnel concerné.

Option 1 – Exploitation contrôlée et atténuation des risques. Cette option met l'accent sur la poursuite contrôlée des solutions existantes. Elle peut rester l'option retenue de manière durable et ne constitue pas une étape préliminaire obligatoire vers les options 2 et 3. Les plateformes existantes sont utilisées dans le cadre de cette option, mais sur la base d'un risque résiduel sciemment documenté et accepté. Des mesures techniques et organisationnelles restreignent les dépendances subsistantes, par exemple vis-à-vis des différents fabricants, des interfaces propriétaires ou des prestataires de services en nuage ayant de vastes droits d'accès à

l'étranger. Elles englobent notamment des configurations restrictives, une classification claire des données, des directives concernant l'utilisation des contenus sensibles, des garanties contractuelles, des mesures portant sur les connexions et le monitoring ainsi qu'une exclusion réfléchie des cas d'application particulièrement critiques. Dans le cas du poste de travail numérique, cela implique, par exemple, qu'une administration continue d'utiliser M365 comme environnement de travail standard, mais essaie de réduire les risques connexes de souveraineté et de conformité grâce à la configuration, à la gouvernance et aux règles d'utilisation. Dans le cadre de cette option, il ne s'agit pas encore de mettre en place une véritable alternative opérationnelle, mais plutôt de faire en sorte que l'exploitation existante de M365 soit maîtrisable et responsable.

Option 2 – Mise en place d'options de seconde source. Dans le cadre de cette option, une solution alternative est mise en place en tant qu'environnement de réserve ou de secours, en complément de la poursuite contrôlée de l'exploitation existante. Cette option est particulièrement pertinente lorsqu'une administration entend se prémunir contre l'indisponibilité prochaine d'une plateforme propriétaire ou une réduction de sa disponibilité, ou encore contre un changement significatif de la situation en matière de risques, qui résulterait, par exemple, de la forte accentuation d'une menace concernant la confidentialité ou l'intégrité. Cette option ne vise pas encore à changer à court terme l'exploitation ordinaire, mais à créer une capacité d'action au vu des conditions-cadres changeantes. L'environnement alternatif est donc mis en place de manière à pouvoir être activé et déployé en cas de besoin, ou étendu à certains cas d'application critiques. Si l'on prend l'exemple du poste de travail numérique, cela peut impliquer la préparation technique et organisationnelle d'un environnement alternatif comme openDesk en plus de M365, afin qu'il soit disponible comme environnement de réserve en cas de crise ou d'escalade. Cela englobe, par exemple, la mise à disposition des principales fonctions de base telles que la communication, le traitement et l'archivage des documents et la collaboration, pour permettre au moins le maintien des capacités de travail essentielles.

Option 3 – Changement partiel ou complet. Cette option se distingue fondamentalement des précédentes par le fait que la solution alternative n'est plus conservée en parallèle ou testée dans des sous-domaines, mais devient elle-même le principal environnement cible pour l'exploitation ordinaire. La transition intervient dans le cadre d'un changement partiel ou complet lorsqu'elle est justifiée sur le plan stratégique, soutenue sur le plan politique et supportable sur le plan économique. Un changement partiel peut se limiter à certains groupes d'utilisateurs, certains besoins de protection ou à certaines fonctions ou unités d'organisation, tandis qu'un changement complet concerne toute l'administration. Pour le poste de travail numérique, cela signifie qu'une solution comme openDesk ne sera plus exploitée uniquement en complément de M365, mais qu'elle deviendra le poste de travail standard. Les nouveaux utilisateurs, espaces collaboratifs et processus de travail seront alors, par principe, mis en place dans la solution alternative. L'organisation opérationnelle, l'assistance technique, les formations, la gouvernance et les processus standard seront axés sur la nouvelle plateforme. Dans ce scénario, M365 sera utilisé pour les transitions, les exceptions ou les applications restantes, ou sera entièrement remplacé. La différence essentielle par rapport à l'option 2 ne tient donc pas uniquement à

l'ampleur de l'utilisation, mais également au rôle systémique de l'environnement : dans l'option 2, la solution utilisée est une alternative opérationnelle ; dans l'option 3, elle est l'environnement primaire.

> La souveraineté numérique n'est pas un état que l'on atteint pleinement ou que l'on manque, mais le résultat d'options choisies de manière ciblée, à différents niveaux d'ambition. Chaque administration prend cette décision de manière autonome, ou en collaboration avec d'autres collectivités, dans le cadre de ses objectifs politiques et stratégiques, pour le domaine fonctionnel concerné.

[Remarque concernant la traduction : la partie « Analyse » qui suit n'est disponible qu'en allemand.]

3 Analyse

3.1 Kontext

3.1.1 Ausgangslage

Die Arbeitsgruppe «Cloud Governance und Workplace» der DVS hat im Juni 2025 die Second Source-Studie publiziert. Sie untersuchte Chancen und Herausforderungen der Abhängigkeit der öffentlichen Verwaltung von proprietären Cloud-Lösungen wie M365.

Die Studie kommt zu drei zentralen Befunden: Erstens bietet der Markt im Bereich Büroautomation potenzielle und teils praxiserprobte Alternativen zu M365. Initiativen von Anbietern wie VNCLagoon, Infomaniak, EGroupware oder ZenDiS sowie Pilotprojekte in der Schweiz und in Deutschland zeigen die vorhandene Innovationsdynamik. Reifegrad, Funktionsumfang und Skalierbarkeit variieren jedoch deutlich, insbesondere im grossflächigen Verwaltungsbetrieb.

Zweitens ist IT-Resilienz zunehmend im Kontext der Reduktion strategischer Abhängigkeiten und von Vendor-Lock-in zu betrachten. Eine tiefe Integration von Fachanwendungen mit der proprietären Plattform eines Anbieters (z. B. Authentifizierung über Entra ID, Workflow- und Automatisierungsfunktionen) bindet die Verwaltung strategisch. Ein späterer Anbieterwechsel erfordert eine aufwändige Neuintegration bestehender Systeme und Schnittstellen. Ansätze wie Parallelbetrieb oder selektiver Einsatz alternativer Lösungen, etwa bei Video-/Audiokonferenzen oder E-Mail, erhöhen die Resilienz jedoch nicht in jeder Hinsicht. Im Rahmen des IT Service Continuity Managements sind Recovery Time Objective (RTO) und Recovery Point Objective (RPO) massgeblich. Diese können durch den Einsatz von Alternativen allenfalls ungünstig beeinflusst werden. Ein spürbarer Gewinn an Service Continuity ergibt sich primär im Szenario einer politisch motivierten Dienstverweigerung (Kill-Switch), in dem eine vom Hauptanbieter unabhängige Ausweichlösung die Handlungsfähigkeit sichert. Solche Ansätze sind, sind aber mit funktionalen Einschränkungen, zusätzlichem Betriebsaufwand und wirtschaftlichen Trade-offs verbunden.

Drittens setzt ein strategischer Umstieg auf Alternativen eine langfristig angelegte, politisch abgestimmte und institutionenübergreifend koordinierte Vorgehensweise voraus. Erfolgsentscheidend sind eine realistische Transformationsplanung, nachhaltige Finanzierungsmodelle, föderale Zusammenarbeit, die konsequente Nutzung offener Standards, sowie gezielter Kompetenzaufbau innerhalb der Verwaltung. Alternativ kann der Betrieb an einen gemeinschaftlich getragenen, zentralen Dienstleister ausgelagert werden.

Vor diesem Hintergrund und angesichts des weiterhin intensiv geführten politischen Diskurses rund um die Einführung von M365 in Verwaltungseinheiten hat eine Gruppe kantonaler IT-Verantwortlicher eine systematische Marktanalyse alternativer Produkte und eine Auslegeordnung möglicher Konsequenzen eines Wechsels angeregt. Die Geschäftsstelle der DVS hat deshalb die vorliegende Anschlussstudie in Auftrag gegeben. Die systematische Marktanalyse wurde hierbei bereits in der Second Source Studie abgedeckt.

3.1.2 Ziele

Die vorliegende Anschlussstudie analysiert die Abhängigkeiten öffentlicher Verwaltungen in der Schweiz von M365 und zeigt die Konsequenzen eines Wechsels zu Alternativlösungen auf. Im Zentrum stehen die technischen, organisatorischen, regulatorischen und finanziellen Auswirkungen eines solchen Umstiegs. Die Erkenntnisse bieten Entscheidungsträgern in Verwaltung und Politik eine faktenbasierte Grundlage für zukunftsgerichtete Entscheidungen zur Nutzung von M365 und dessen Alternativen.

Ausgangslage und Auswirkungen eines Umstiegs auf eine konkrete alternative Produktsuite werden in zwei Untersuchungseinheiten unterschiedlicher Grösse und Ausgangslage detailliert betrachtet. Dieses Vorgehen erlaubt realitätsnahe Aussagen anhand dieser konkreten Beispiele und liefert übertragbare Erkenntnisse für andere Verwaltungen und Organisationen. Die Ergebnisse der Studie werden anhand weiterer Verwaltungseinheiten validiert.
Diese Validierungspartner beantworteten einen standardisierten Fragebogen, mit dem geprüft wurde, ob sich die gefundenen Muster bestätigen oder organisationsspezifisch sind.

3.1.3 Adressaten

Die Studie richtet sich primär an Entscheidungsträgerinnen und Entscheidungsträger sowie IT-Verantwortliche in Verwaltungseinheiten auf Bundes-, Kantons-, Stadt- und Gemeindeebene, die für die strategische Ausrichtung, Planung und Steuerung von Cloud-basierten Kollaborations- und Produktivitätslösungen verantwortlich sind, gleichzeitig, aber auch weitere Aspekte des Microsoft-Ökosystems im Auge behalten müssen.

Angesprochen sind ebenso Fachpersonen in den Bereichen Beschaffung, Digitalisierung und Datenschutz, für die Anbieterunabhängigkeit und digitale Handlungsfähigkeit von besonderer Relevanz sind.

Adressiert werden zudem politische Vertretungen, Fachstellen sowie weitere Institutionen mit vergleichbaren Herausforderungen im digitalen Sektor. Die Erkenntnisse dienen als Orientierungs- und Entscheidungsgrundlage für die Weiterentwicklung bestehender Lösungen sowie für künftige Beschaffungs- und Transformationsvorhaben.

3.1.4 Fokus und Abgrenzung

Die Studie untersucht die Abhängigkeiten von Schweizer Verwaltungseinheiten von M365 als Software-as-a-Service (SaaS)-Lösung und die Konsequenzen eines Wechsels auf eine Alternative. Im Fokus stehen die Produkte des M365-Portfolios, insbesondere Office-Anwendungen, Exchange Online, SharePoint, Teams und OneDrive, wie in Abbildung 8: Fokus der Studie dargestellt. Zudem werden relevante Integrationen in das M365-Ökosystem betrachtet, beispielsweise in den Bereichen Identitäts- und Zugriffsmanagement (Entra ID) und Sicherheit und Compliance (Purview, Sentinel, Intune).

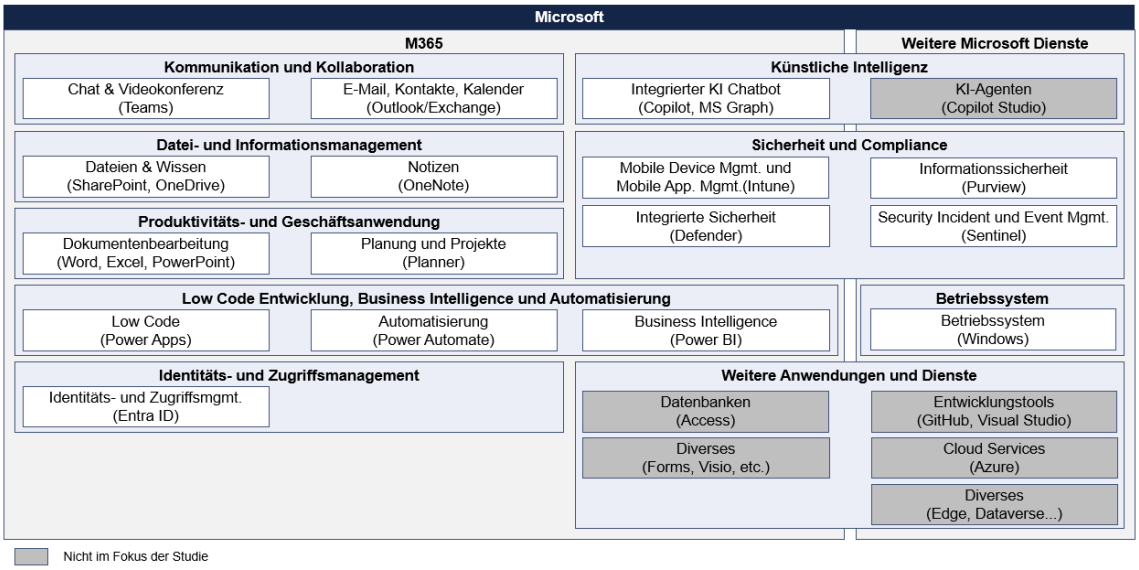


Abbildung 8: Fokus der Studie

Nicht Bestandteil der Untersuchung sind Abhängigkeiten zu weiteren Microsoft-Produkten ausserhalb des M365-Portfolios (z. B. Dynamics, Visual Studio). Ebenso unberücksichtigt bleiben Angebote aus den Bereichen Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS) der Microsoft Azure Cloud.

Mit dieser Abgrenzung bildet die Studie die gesamthafte Cloud-Sicherheits- und Souveränitätslage bewusst nicht vollständig ab. Für Fragen wie Datenstandort, Schlüsselhoheit oder Lawful Access ist die Gesamtarchitektur massgeblich und nicht allein das M365-Portfolio; eine abschliessende Beurteilung dieser Aspekte setzt eine Betrachtung voraus, die auch Azure-Dienste und weitere Cloud-Komponenten einschliesst. Der gewählte Fokus hält die Untersuchung demgegenüber überschaubar und reduziert spekulative Annahmen. Er begrenzt zugleich die Reichweite strategischer Aussagen darüber, wie sich Abhängigkeiten entwickeln könnten, etwa durch KI-Funktionen oder veränderte Lizenzmodelle.

Analysiert werden der aktuelle und absehbare Einsatz von M365-Anwendungen und -Diensten in den zwei Untersuchungseinheiten sowie die Konsequenzen eines Wechsels auf eine konkrete Alternativlösung. Künftige Produktentwicklungen und Neuerungen der Hersteller, sowohl im M365-Ökosystem als auch bei Alternativlösungen, werden nicht berücksichtigt.

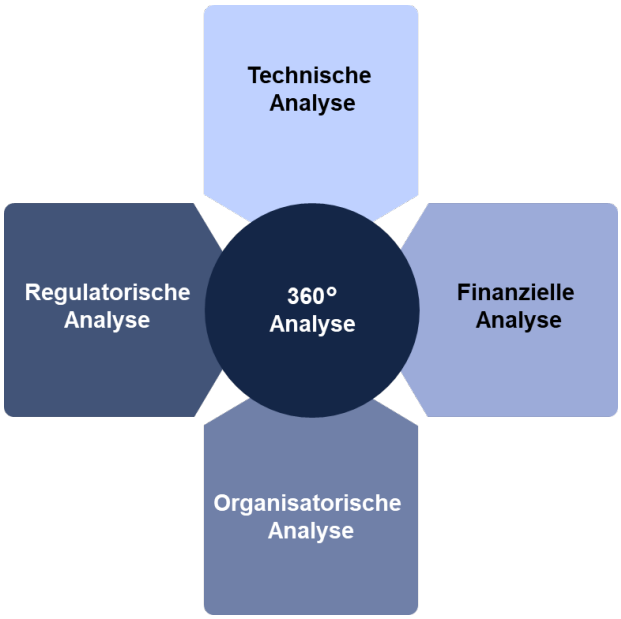
Die Studie konzentriert sich auf die Office-Suite, die von Angestellten der Kernverwaltung genutzt wird, also auf die Kernfunktionen moderner Bürokommunikation und Zusammenarbeit (insbesondere E-Mail, Kalender, Dateiablage, Kollaboration, Audio-/Videokonferenzen). Fachspezifische Anwendungen und Branchensoftware werden nur hinsichtlich ihrer Integrationsfähigkeit betrachtet, nicht einzeln evaluiert.

3.2 Vorgehen & Methodik

3.2.1 Übergreifende Methodik

Zur umfassenden und nachvollziehbaren Untersuchung potenzieller Alternativlösungen zu M365 wurde ein methodisches Vorgehen angewendet, das die relevanten Fragestellungen aus vier Blickwinkeln beleuchtet: technisch, organisatorisch, regulatorisch und finanziell.

Die Frage der digitalen Souveränität wird dabei nicht als eigenständige Dimension behandelt, sondern als querschnittlicher Aspekt, der sich in den technischen, organisatorischen, regulatorischen und finanziellen Analysen widerspiegelt. Dieses multidimensionale Analysemodell deckt die wesentlichen Aspekte eines möglichen Wechsels in Verwaltungseinheiten ab.



Zur Sicherstellung der Praxisrelevanz und Übertragbarkeit der Ergebnisse auf andere Verwaltungseinheiten wurden zwei repräsentative Untersuchungseinheiten ausgewählt. In diesen Einheiten wurden strukturierte Gespräche mit relevanten Stakeholdern geführt. Deren Perspektiven, Anforderungen und Erfahrungen wurden gezielt erhoben und in die Analyse eingebracht.
Zusätzlich wurden Ist-Daten der Untersuchungseinheiten herangezogen, um darauf aufbauend mögliche Soll-Szenarien und deren Auswirkungen in technischer, organisatorischer, regulatorischer uns finanzieller Hinsicht exemplarisch zu analysieren. Der Fokus lag entsprechend auf den Anwendungsszenarien in mittleren bis grossen öffentlich-rechtlichen Verwaltungen.

3.2.2 Technische Methodik

Die technische Analyse untersucht die Bereiche Funktionsumfang, Daten, Hosting, und Integrationen im Kontext von M365 und M365-Alternativen. Im Fokus steht, welche Funktionen in der jeweiligen Untersuchungseinheit genutzt werden und wie weit diese durch die betrachteten Alternativlösungen abgedeckt werden können. Ziel ist es, den Grad der Abhängigkeit von M365 in den konkreten Funktionsbereichen nachvollziehbar zu machen.

Zur Analyse von Nutzung und Bedeutung einzelner M365-Funktionen wird ein strukturiertes Analysemodell verwendet:

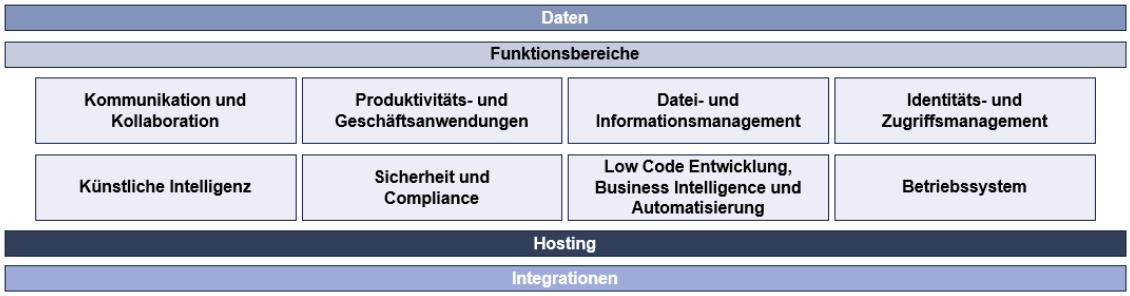


Abbildung 9: Technisches Analysemodell

Das Modell basiert auf den folgenden Hauptkomponenten:

Kategorie	Beschreibung
Daten	Art, Umfang und Sensitivität der in M365-Anwendungen gespeicherten und verarbeiteten Daten
Funktionsbereiche	Anwendungsfelder und Funktionalitäten, die M365 abdeckt
Hosting	Technische Bereitstellung (Cloud, On-Premise, Hybrid) einzelner Anwendungen und Dienste
Integrationen	Anwendungen, Dienste und Systeme mit Integrationen in M365

Tabelle 1: Hauptkomponenten des technischen Analysemodells

Das dargestellte Analysemodell bildet die Grundlage, um das M365-Portfolio hinsichtlich seiner Funktionen und Einsatzmöglichkeiten strukturiert zu bewerten. Das M365 Portfolio enthält diverse Desktop- und Webanwendungen, welche auf verschiedenen Geräten verfügbar sind und ein breites Funktionsspektrum abdecken. Die abgedeckten Funktionsbereiche lassen sich in folgende Kategorien einordnen:

Funktionsbereich	Beschreibung
Kommunikation und Kollaboration	Funktionen für die Kommunikation und Kommunikation, z. B. für die Zusammenarbeit im Team, Telefonie und Schriftverkehr. Beispielhafte M365 Anwendungen und Dienste: Teams, Outlook, Exchange, etc.

Produktivitäts- und Geschäftsanwendungen	Funktionen in den Bereichen Produktivitäts- und Geschäftsanwendungen, z. B. für die tägliche Büroarbeit, wie das Erstellen und Bearbeiten von Dokumenten, die Textverarbeitung, Tabellenkalkulationen. Beispielhafte M365 Anwendungen und Dienste: Word, PowerPoint, Excel, etc.
Datei- und Informationsmanagement	Funktionen in den Bereichen Datei- und Informationsmanagement, z. B. für das Speichern und Verwalten von Dateien und Informationen. Beispielhafte M365 Anwendungen und Dienste: SharePoint, OneDrive, etc.
Identitäts- und Zugriffsmanagement	Funktionen in den Bereichen Identitäts- und Zugriffsmanagement, z. B. für das Erstellen und Verwalten von Identitäten und die Verwaltung von Zugriffen. Beispielhafte M365 Anwendungen und Dienste: Active Directory, Entra ID, etc.
Künstliche Intelligenz	KI-Funktionen, z. B. KI-Assistenten, KI-Chats, KI-Agenten und weitere Beispielhafte M365 Anwendungen und Dienste: Copilot, etc.
Sicherheit und Compliance	Sicherheits- und Compliance relevante Funktionen, z. B. für den Schutz vor Cyberbedrohungen, den Schutz von Daten, die sichere Verwaltung von Geräten. Beispielhafte Anwendungen und Dienste im M365 Ökosystem: Defender, Intune, Purview etc.
Low Code Entwicklung, Business Intelligence und Automatisierung	Funktionen in den Bereichen Low Code Entwicklung, Business Intelligence und Automatisierung, z. B. für das Visualisieren von Daten, das Automatisieren von Prozessen, das Entwickeln von Low-Code Anwendungen. Beispielhafte M365 Anwendungen und Dienste: Power BI, Power Automate, Power Apps, etc.
Betriebssystem	Das Betriebssystem Windows mit den dazugehörigen Funktionen.

Tabelle 2: Funktionsbereiche M365

Das Modell erlaubt eine differenzierte Bewertung der Bedeutung einzelner Funktionen für die Organisation und schafft die Grundlage für einen systematischen Vergleich zwischen M365 und Alternativlösungen.

3.2.3 Organisatorische Methodik

Um die Auswirkungen eines Wechsels von M365 zu einer Alternative zu bewerten, werden folgende vier organisatorische Dimensionen systematisch untersucht:

- Strategie, Sourcing und Vendor-Management: Bewertung der Veränderungen in der Sourcing-Strategie, der Steuerung von -Vendor-Beziehungen und der strategischen Abhängigkeiten.

- Service-Design, Architektur und Governance: Untersuchung der Fähigkeit bestehender Governance-Strukturen, komplexere Architekturentscheidungen und Release-Koordination zu bewältigen.
- Service-Operations, Engineering und Support: Analyse der operativen Auswirkungen auf Support-Prozesse, der notwendigen Skill-Transformation und der Komplexität bei Fehlerdiagnosen.
- Change-Management und User Adoption: Bewertung des kulturellen Wandels von "Feature-Maximierung" zu "Digitaler Souveränität", des erhöhten Schulungsbedarfs durch neue Benutzeroberflächen und der stärkeren Einbindung des Business in die Anforderungsdefinition.

Diese vier Dimensionen ermöglichen eine Quantifizierung der organisatorischen Transformation und identifizieren und welche neuen Fähigkeiten wie Linux-Expertise oder Community-Management aufgebaut werden müssen.

3.2.4 Regulatorische Methodik

Die regulatorische Analyse erfolgt primär auf Basis einer Desk-Analyse und dem Studium der einschlägigen gesetzlichen, vertraglichen und verwaltungsinternen Grundlagen.

Im Zentrum stehen dabei folgende Fragestellungen:

- Einsatz von (Cloud-)Technologien generell: Darstellung der regulatorischen Mindestanforderungen für die Nutzung von Cloud-Technologien durch die öffentliche Hand. Analysiert werden der anwendbare Rechtsrahmen und das Cloud-Stufenmodell der Bundesverwaltung. Ergänzend werden systembedingte Rechtsrisiken identifiziert, die beim Einsatz von Public-Cloud-Diensten verbleiben und durch vertragliche Massnahmen allein nicht vollständig adressiert werden können.
- Einsatz von M365 im Kontext der Rahmenvereinbarung DVS: Prüfung des Mandats der DVS-Rahmenvereinbarung für die Interessenvertretung gegenüber IKT-Anbietern sowie der Grenzen dieses Mandats im Hinblick auf die regulatorische Verantwortung der einzelnen Gemeinwesen.
- Datenrecht & Migration: Untersuchung der wesentlichen Aspekte zu Datenschutz, Privacy und Informationssicherheit, insbesondere der Anforderungen an den Umgang mit sensiblen Daten. Ergänzend werden Fragen der Datenmigration adressiert, namentlich Data Retention und Deletion, Aufbewahrungspflichten, Vertraulichkeit sowie die Einhaltung gesetzlicher Vorgaben zur Datenaufbewahrung und -löschung bei Systemwechseln.

Ergänzend zur Auswertung der rechtlichen und vertraglichen Grundlagen werden die regulatorischen Anforderungen der Untersuchungseinheiten und insbesondere von Blaulichtorganisationen einbezogen, um Sonderregelungen in sicherheitsrelevanten Bereichen zu erfassen.

3.2.5 Finanzielle Methodik

Die finanzielle Analyse zielt darauf ab, die tatsächlichen Gesamtkosten (Total Cost of Ownership, TCO) für den Betrieb von M365 im Vergleich zu potenziellen Alternativlösungen transparent zu machen. Da reine Lizenzpreisvergleiche oft wesentliche Aufwandspositionen vernachlässigen („Lizenz-Illusion“), stützt sich diese Studie auf ein umfassendes Kostenmodell.

Die Kosten werden dabei nach dem international etablierten Technology Business Management (TBM) Framework strukturiert. Dies ermöglicht eine standardisierte Zuordnung zu Kostenarten (Cost Pools) und Funktionen (IT-Towers), was eine objektive Vergleichbarkeit unterschiedlicher Betriebsmodelle sicherstellt, unabhängig von spezifischen Organisationsstrukturen.

Das Modell unterteilt die finanziellen Auswirkungen in vier Hauptdimensionen, um sowohl direkte als auch indirekte Kostenwirkungen zu erfassen.

Laufende Kosten	
Hardware & Software	Jährliche Kosten für Abonnements (M365) bzw. Enterprise-Support-Verträge für Open-Source-Alternativen. Berücksichtigt werden zudem Kosten für Infrastruktur (Server, Storage, RZ-Fläche) und den notwendigen Security-Stack (z. B. MDM, Endpoint Protection), sofern die Alternativlösung dies erfordert.
Wartung & Betrieb	Personalaufwand für Engineering (Architektur, Integration), Patch-Management und Support (Service Desk) für die Endanwender.
Einmalige Kosten	
Risiko & Seiteneffekte	Kalkulatorische Kosten für potenzielle Produktivitätsverluste.
Migration & Change	Projektbezogene Kosten für die technische Datenmigration, das Refactoring von Fachanwendungen und Makros (VBA) sowie Aufwände für Schulung und Change Management zur Befähigung der Mitarbeitenden.

Tabelle 3: Hauptdimensionen finanzielles Analysemodell

Für die Bewertung der finanziellen Dimension gelten folgende Grundsätze:

- Vollständigkeit: Es werden nicht nur Lizenzkosten, sondern auch Infrastruktur, Betrieb, Security und Support einbezogen.
- CapEx–OpEx-Neutralität: Investitionen in eigene Hardware (CapEx) werden über eine jährliche Abschreibung vergleichbar mit laufenden Cloud-Service-Kosten (OpEx) gemacht.
- Transparenz versteckter Kosten: Interner Personalaufwand für Engineering und Betrieb wird explizit ausgewiesen und nicht als „implizit vorhanden“ vorausgesetzt.
- Indirekte Effekte: Auswirkungen auf die Arbeitsproduktivität durch geänderte Benutzeroberflächen oder Kompatibilitätsprobleme werden als steuerungsrelevante Kostenfaktoren sichtbar gemacht.

Die finanziellen Analysen in dieser Studie basieren auf einer Kombination aus vorliegenden Kostendaten der Untersuchungseinheiten, Expertenabschätzungen und plausibilisierten Annahmen. Aufgrund der Heterogenität der Ausgangslagen (z. B. unterschiedliche

Lizenzstaffelungen, individuelle Rabatte, bereits bestehende Betriebsverträge) sowie der dynamischen Preismodelle sowohl bei proprietären Anbietern als auch im OSS-Dienstleistungsmarkt sind die angegebenen Werte als indikative Grössenordnungen zu verstehen, nicht als präzise, eins-zu-eins übertragbare Budgetzahlen.

Ziel ist es, die wesentlichen Kostenblöcke und Relationen sichtbar zu machen und strategische Grössenordnungen zu quantifizieren – nicht, eine detaillierte Wirtschaftlichkeitsrechnung für einzelne Verwaltungseinheiten zu ersetzen.

3.3 Auswahl der Alternativ-Lösung zu M365

3.3.1 Auswahl der Lösung openDesk

Für eine belastbare Bewertung der Auswirkungen eines Plattformwechsels wird eine konkrete Alternativlösung vertieft untersucht. Erst dadurch lassen sich die technischen, organisatorischen, regulatorischen und finanziellen Konsequenzen realitätsnah analysieren und die wesentlichen Fragestellungen identifizieren, die sich Organisationen in einem solchen Transformationsprojekt stellen.

Auf eine erneute vollständige Marktanalyse wurde bewusst verzichtet: Die Second-Source-Studie der Digitalen Verwaltung Schweiz hat den Markt systematisch betrachtet und vier Anbieter identifiziert, VNClagoon, openDesk, kSuite und EGroupware, auf Basis der Kriterien vollständige Gesamtlösung, Open-Source-Basis und Firmensitz in der Schweiz oder EU. Die vorliegende Studie baut auf diesen Erkenntnissen auf und konzentriert sich auf die vertiefte Analyse der praktischen Umsetzbarkeit.

Im Rahmen der Studie wurde festgestellt, dass keine der vier Alternativen eine eindeutig überlegene Lösung darstellt. Alle weisen spezifische Stärken und Schwächen auf. Die Arbeitsgruppe entschied sich für openDesk für die vertiefte Untersuchung in der vorliegenden Studie und basierte dies auf einer Kombination objektiver Kriterien und subjektiver Überlegungen.
Für die zukünftige Bewertung solcher Alternativen ist zu beobachten, wie sich das Anbieter- und Dienstleistungsökosystem rund um openDesk und vergleichbare Lösungen weiterentwickelt.

Wichtiger Hinweis: Die Wahl für openDesk erfolgt ausschliesslich zu illustrativen Zwecken als exemplarisches Beispiel einer OSS-basierten M365-Alternative.

Im Zentrum dieser Studie stehen nicht die Auswahlkriterien einer Alternative selbst, sondern die Fragestellungen und die Konsequenzen eines Plattformwechsels.

Diese Auswahl stellt keine Empfehlung zugunsten von openDesk dar. Die Erkenntnisse und Methodik sind auf Alternativen übertragbar. Konkrete Entscheidungen müssen auf

Basis umfassender, individueller Evaluationen unter Berücksichtigung der spezifischen Anforderungen der jeweiligen Organisation getroffen werden.

3.3.2 Beschreibung der Lösung openDesk

Als Quelle diente die Vorgänger-Studie, die zur Redaktionszeit Verfügung stehenden Informationen aus den Webseiten der Produkthersteller. Ergänzende, vertiefte Informationen über openDesk stammen zudem aus einer bilateralen Interaktion mit ZenDIS geführt im April 2026.

3.3.2.1 Produkt- und Architekturüberblick

openDesk ist im deutschen Markt im Oktober 2024 offiziell lanciert worden und baut auf den Erfahrungen der Vorgängerplattform dPhoenixSuite auf. openDesk ist als Produkt vergleichsweise jung. Gleichzeitig ist zu berücksichtigen, dass sich im Umfeld der Lösung und ihrer Kernkomponenten bereits ein wachsendes Ökosystem von Implementierungs- und Betriebspartnern entwickelt hat.

Das Produkt hat das Ziel, eine digitale Arbeitsplatzlösung auf Open Source Basis zur Verfügung zu stellen, die die Bedürfnisse und Ansprüche der Öffentlichen Verwaltung im Hinblick auf Souveränität und Funktionalität bedient.

Die openDesk Lösung bündelt verschiedene Open-Source-Applikationen wie E-Mail, Kalender, Textverarbeitung, Dateiverwaltung und Chat an einem Ort mit einer einheitlichen Benutzeroberfläche und Single-Sign-On.

Aus Kundensicht präsentiert sich openDesk wie eine klassische SaaS-Lösung: Der Dienst wird betriebsfertig bezogen, typischerweise nutzungsbasiert abgerechnet. Strukturell unterscheidet sich das Modell jedoch wesentlich von klassischen SaaS-Angeboten, da Produktverantwortung und Betrieb zwischen verschiedenen Anbietern aufgeteilt sind. Anders als bei herkömmlichen SaaS-Lösungen, wo der Produkthersteller auch den Betrieb übernimmt, betreibt hier ein separater Hosting-Partner ein Produkt, das er nicht selbst entwickelt hat.

3.3.2.2 Funktionsumfang nach Funktionsbereichen

Im Folgenden geben wir einen Überblick über die derzeit vorhandenen Funktionen von openDesk entlang der Funktionsbereiche des verwendeten technischen Modells:

- Kommunikation und Kollaboration: Als Chat-Lösung ist Element im Einsatz, welches das Austauschen von Informationen in Gruppen- und Einzelchats ermöglicht. Die OX App Suite von Open Xchange stellt eine integrierte E-Mail-Lösung mit den Komponenten OX Mail, OX Kalender und OX Kontakte bereit. Für Video- und Audiokonferenzen steht Nordeck in openDesk zur Verfügung.

- Produktivitäts- und Geschäftsanwendungen: Collabora Online erweitert openDesk um eine Office-Suite, die die Erstellung, Bearbeitung und gemeinsame Nutzung von Dokumenten, Tabellen und Präsentationen unterstützt. Die Anwendung CryptPad ermöglicht die Erstellung und gemeinsame Bearbeitung von Diagrammen.
- Datei- und Informationsmanagement: openDesk stellt mit Nextcloud eine Cloud-Plattform bereit, welche die Synchronisation und den Zugriff auf Dateien über Desktop-, Web- und mobile Endgeräte ermöglicht. Benutzer können Dokumente online bearbeiten, teilen und kommentieren. Als Wissensmanagement-Komponente ist XWiki angebunden: Verwaltungswissen kann strukturiert dokumentiert, geteilt und gezielt durchsucht werden. Die integrierte Anwendung CryptPad ermöglicht die Erstellung und gemeinsame Bearbeitung von Diagrammen.
- Identitäts- und Zugriffsmanagement: Nubus von Univention bietet ein zentrales Identity- und Access-Management zur Integration verschiedener Anwendungen. Es erlaubt sowohl die Einrichtung und Verwaltung einer eigenen Benutzerverwaltung als auch die Anbindung an bestehende Systeme wie Keycloak oder Active Directory.
- Künstliche Intelligenz: Ein direktes Pendant zu Microsoft Copilot ist nicht enthalten. openDesk unterstützt KI-Funktionen auf Ebene der enthaltenen Komponenten, die jeweiligen Hersteller bringen eigene KI-Funktionen mit.
- Sicherheit und Compliance: Verglichen mit Microsoft Purview sind Funktionen (Sensitivity Labelling, Retention Policies, DLP) nicht nativ in openDesk enthalten. Für Sensitivity/Retention Labelling und DLP sind Drittanbieterlösungen erforderlich, die individuell integriert werden müssen.
  Mobile Device/Applikationsmanagement (MDM/MAM) wird nicht nativ angeboten, die Verwaltung erfolgt über die jeweiligen App-Stores.

- Sicherheit: OpenDesk hat verschiedene Sicherheitsfunktionen, darunter beispielsweise:
  - Ende-zu-Ende-Verschlüsselung (Matrix/Chat)
  - OpenPGP-Verschlüsselung (E-Mail)
  - Virenscanner für Datei-Uploads
  - MFA sowie Rollen-/Berechtigungsmanagement
- Business Intelligence, Low Code, und Automatisierung: Ein direktes Pendant zur Microsoft Power Platform ist nicht enthalten. Für Workflow-Automatisierung, Dashboards und Low-Code-Anwendungen sind separate Drittanbieterlösungen erforderlich. Die Suite unterstützt OpenProject (Projektmanagement mit begrenzten Automatisierungsmöglichkeiten) und XWiki (strukturierte Datenverwaltung/Low-Code Möglichkeiten).
- Betriebssystem: openDesk ist primär web-basiert und im Browser auf allen Endgeräten nutzbar. Nicht alle Komponenten sind als vollwertige Desktop-Clients oder Mobile Apps verfügbar. Eine eigenständige openDesk-App sowie gebrandete Apps für die einzelnen Anwendungsbereiche sind in Planung. Es gibt folgende Client Anwendungen und Mobile Apps.
  - Desktop-Clients:
    - Nextcloud Desktop (Windows, macOS, Linux)
    - Element Desktop (Windows, macOS, Linux)

  - Collabora Desktop (Windows, macOS, Linux)
  - OX AppSuite: über IMAP/CalDAV/CardDAV in Standard-Desktop-Mail-Clients einbindbar
- Mobile App (iOS & Android):
  - Nextcloud Mobile
  - Element Mobile
  - Collabora Mobile
  - OX Mail Mobile (E-Mail, Kalender, Kontakte)
  - OpenProject Mobile (eingeschränkter Funktionsumfang)
  - Jitsi Mobile

openDesk bietet einen grundlegenden Funktionsumfang in den Bereichen Kommunikation und Kollaboration, Produktivitäts- und Geschäftsanwendungen, Datei- und Informationsmanagement, und Identitäts- und Zugriffsmanagement. Damit sind wesentliche Office Funktionalitäten grundsätzlich abgedeckt. Jedoch fehlen Funktionen in den Bereichen Sicherheit und Compliance und Business Intelligence, Low Code, und Automatisierung.

Gleichzeitig ist zu berücksichtigen, dass einzelne Funktionen, die in M365 nativ integriert verfügbar sind, in openDesk derzeit nicht oder nur über zusätzliche Drittanbieterlösungen abbildbar sind. Dies betrifft insbesondere die Bereiche Künstliche Intelligenz, Sicherheit und Compliance, Business Intelligence, Low Code und Automatisierung. Wie stark diese funktionalen Lücken ins Gewicht fallen, hängt von den konkreten Geschäftsanforderungen der jeweiligen Organisation ab. Für Standardanwendungsfälle der Bürokommunikation und Zusammenarbeit kann der vorhandene Funktionsumfang grundsätzlich geeignet sein. Bestehen jedoch weitergehende Anforderungen, etwa im Hinblick auf integrierte Arbeitsweisen, automatisierte Fachverfahren, regulatorische Vorgaben, zentrale Steuerung mobiler Endgeräte, oder den Einsatz KI-gestützter Assistenzfunktionen, kommen grundsätzlich drei Umgangsweisen in Betracht: die bewusste Akzeptanz funktionaler Einschränkungen, sofern die betroffenen Fähigkeiten nicht geschäftskritisch sind, die Ergänzung durch Drittanbieterlösungen sowie die Kompensation durch organisatorische oder prozessuale Massnahmen. Vor einer Einführung ist daher zu prüfen, inwieweit die jeweiligen Anforderungen der Organisation durch openDesk selbst oder durch ergänzende Komponenten angemessen adressiert werden können.

3.3.2.3 Produktverantwortung und Ökosystem

Die zentrale Produktverantwortung liegt bei ZenDiS (Zentrum für Digitale Souveränität der Öffentlichen Verwaltung). Das ZenDiS hatte die damalige Bundesregierung im Jahr 2022 gegründet. Bis heute ist der Bund Alleingesellschafter dieser GmbH.[2]

ZenDiS führt die verschiedenen Open-Source-Komponenten zu einer integrierten Suite zusammen, übernimmt die Lizenzierung und steuert die strategische Weiterentwicklung. Diese Rolle ist vergleichbar mit der eines Produktherstellers in klassischen Enterprise-Lösungen. Eine

[2] Deutscher Bundestag, Drucksache 21/5502 vom 22.04.2026 (zitiert: BT-Drs. 21/5502)

Anschubfinanzierung des Bundes ist bis 2026 gesichert. Der weitergehende Finanzierungsplan ist aktuell noch nicht bekannt.

openDesk befindet sich als Produkt in einer dynamischen Aufbauphase. Seit dem offiziellen Launch im Herbst 2024 hat sich in Deutschland ein wachsendes Netzwerk von Dienstleistern und Implementierungspartnern formiert. Deutschland verfügt über ein reiferes openDesk-Ökosystem mit etablierten Anbietern wie B1 Systems als Generalunternehmer sowie GECKO, DACHS IT, Univention, Nextcloud, OpenProject und Open-Xchange. Die Zahl der Personen mit praktischer openDesk-Erfahrung wird auf einige Hundert bis wenige Tausend geschätzt. Eine Grössenordnung im Zehntausenderbereich ist nicht realistisch.

Der Schweizer Markt für openDesk-Dienstleistungen befindet sich in der Aufbauphase. Zum Zeitpunkt der Erstellung der Studie sind den Autoren drei Schweizer Firmen mit operativem openDesk-Angebot bekannt.[3] Es ist davon auszugehen, dass weitere existieren oder demnächst dazustossen. Es ist auch davon auszugehen, dass in ein, zwei Jahren eine dann wieder Konsolidierung der Anbieter stattfinden wird.

Öffentlich zugängliche Zahlen zur Personalstärke mit openDesk-Expertise liegen nicht vor. Eine qualifizierte Schätzung bewegt sich im Bereich von 5–20 Personen pro Anbieter. In Summe ergibt sich, inklusive vereinzelter Freelancer und unternehmensinterner Kompetenzträger ausserhalb der drei genannten Firmen, eine Grössenordnung von rund 30–80 Personen mit praktischer openDesk-Hands-on-Erfahrung in der Schweiz.

Ergänzend besteht in der Schweiz ein breiteres konzeptionelles und strategisches Umfeld im Themenfeld digitale Souveränität, zu dem unter anderem das BFH Institut Public Sector Transformation, verschiedene kantonale IT-Organisationen sowie Akteure aus dem SDS-Netzwerk zählen. Mit der Lancierung des Zentrums SDS (Souveräne Digitale Schweiz) wurde gemäss den veröffentlichten Informationen ein weiterer Rahmen für die Vernetzung und Koordination entsprechender Aktivitäten geschaffen. Den publizierten Angaben zufolge erfolgt die operative Umsetzung mit 23 Partnern in vier Workstreams.[4]

Für die vorliegende Studie ist dabei insbesondere relevant, dass innerhalb dieses breiten angelegten Umfelds auch Aktivitäten mit Bezug zu openDesk stattfinden. Gleichzeitig ist festzuhalten, dass sich das Zentrum SDS nicht auf openDesk beschränkt, sondern ein weiter gefasstes Spektrum an Themen und Initiativen im Bereich digitaler Souveränität adressiert.

Vor diesem Hintergrund ist davon auszugehen, dass sich mit einem Marktausbau in der Schweiz ebenfalls in absehbarer Zeit ein entsprechendes Kompetenz-Ökosystem entwickeln wird,

[3] Adfinis & steppingstone, Bedag, Exigo, Vgl.Netzwerk SDS – openDesk-Seite mit Liste der Schweizer Betreiber. URL: https://netzwerksds.ch/openDesk/, abgerufen am 14. August 2026.
[4] Vgl. Netzwerk SDS, Lancierung Zentrum SDS, URL: https://netzwerksds.ch/lancierung-zentrum-sds/, abgerufen am 14. August 2026.

insbesondere dann, wenn öffentliche Verwaltungen Nachfrage bündeln und sich aktiv am Aufbau der Community beteiligen.

Gegenüber langjährig etablierten Plattform-Ökosystemen ist das openDesk-bezogene Anbieter- und Kompetenzumfeld derzeit noch im Aufbau und entsprechend weniger breit ausdifferenziert. Für die vorliegende Studie ist jedoch nicht in erster Linie ein quantitativer Vergleich mit global etablierten Anbieterlandschaften ausschlaggebend, sondern die Beobachtung, dass sich in der Schweiz erste institutionelle, fachliche und marktseitige Strukturen abzeichnen, aus denen sich mittelfristig ein tragfähigeres Ökosystem entwickeln könnte.

3.3.2.4 Betriebs- und Lizenzmodell

openDesk kann sowohl On-Premise als auch als SaaS betrieben werden. Für die On-Premise Version ist man frei in der Wahl des Hosters. Für die SaaS-Lösung bezieht ZenDiS die Leistungen von einem Hoster in Deutschland.

Lösung	**Lizenz / Monat**	**Hosting**	**Total pro User / Monat**
openDesk (SaaS, Deutschland)	Euro 18.00	Inkludiert	CHF 16.60
openDesk (Enterprise)	Euro 15.00	Nicht inkludiert	CHF 13.80

Tabelle 4: Lizenzkosten openDesk

3.3.2.5 Hosting- und Partnermodell der Enterprise Variante

Für den produktiven Betrieb der Enterprise-Version ist zusätzlich ein Hosting-Partner erforderlich, der die technische Bereitstellung und den laufenden Betrieb der Plattform übernimmt. In dieser Studie wurde die BEDAG Informatik AG befragt und als exemplarischer Hosting-Partner gewählt, da sie über die notwendige Expertise im Betrieb Kubernetes-basierter Plattformen, langjähriger Erfahrung im Betrieb von Open Source Lösungen verfügt und bereits Erfahrungen mit openDesk vorweisen kann.

Wichtiger Hinweis: Die Nennung der BEDAG Informatik AG als Hosting-Partner erfolgt ausschliesslich zu illustrativen Zwecken als exemplarisches Beispiel eines Dienstleisters für openDesk-Hosting.

Im Zentrum dieser Studie stehen nicht die spezifischen Auswahlkriterien eines Hosting-Partners, sondern die organisatorischen Auswirkungen und Betriebsmodelle beim Übergang von M365 zu einer Alternativlösung.

Diese Auswahl stellt keine Empfehlung zugunsten der BEDAG Informatik AG dar. Andere qualifizierte Schweizer oder europäische Hosting-Partner könnten gleichwertige oder passendere Leistungen erbringen. Die dargestellten organisatorischen Erkenntnisse und

die entwickelte Methodik zur Bewertung von Betriebsmodellen sind grundsätzlich auf andere Hosting-Partner übertragbar.

Die folgende Tabelle zeigt die Aufgaben- und Verantwortungsverteilung zwischen den verschiedenen Partnern im openDesk-Ökosystem auf. Diese Struktur verdeutlicht, wie sich die Rolle des Kunden von einem reinen Service-Konsumenten zu einem aktiven Service-Orchestrator wandelt, der verschiedene Anbieter koordinieren und steuern muss.

Partner	**Aufgaben und Verantwortung**
ZenDiS GmbH (Produktverantwortung)	Kernaufgaben: Produktstrategie und Roadmap-Entwicklung für openDesk Koordination der Open-Source-Community und Komponentenhersteller Enterprise-Support-Verträge und Lizenzierung Qualitätssicherung und Release-Management Strategische Partnerschaften mit Komponentenherstellern Governance: Produktentscheidungen werden durch ZenDiS Produktmanagement getroffen Kundenanforderungen können Roadmap beeinflussen Formales Governance-Modell mit Gremien/Boards in Entwicklung
BEDAG Informatik AG (Service Provider)	Operative Verantwortung: 2nd-Level-Support: Direkter Ansprechpartner für die Betriebs- und Support-Organisation der öffentlichen Organisation Infrastruktur-Management: Kubernetes-Cluster, Storage, Networking Monitoring & Alerting: 24/7-Überwachung der Systemverfügbarkeit Backup & Recovery: Automatisierte Datensicherung und Disaster Recovery Security Operations: Patch-Management, Vulnerability-Scanning Capacity Management: Ressourcenplanung und -optimierung SLA-Verpflichtungen: Definierte Response-Zeiten für verschiedene Incident-Kategorien Regelmässige Service-Reviews und Reporting
Komponentenhersteller (3rd-Level-Support)	Verschiedene spezialisierte Hersteller (Nextcloud GmbH, New Vector Ltd., Collabora Productivity Ltd., Open-Xchange AG) sind für die Weiterentwicklung und den spezialisierten Support ihrer jeweiligen Open-Source-Komponenten verantwortlich. Sie stellen Bugfixes, Sicherheitsupdates und neue Features bereit, die über ZenDiS in die openDesk-Suite integriert werden. Der Kunde hat keinen direkten Kontakt zu diesen Herstellern. Die Kommunikation erfolgt über die Eskalationswege via BEDAG und ZenDiS.

Tabelle 5: Aufgaben- und Verantwortungsverteilung Partner im openDesk-Ökosystem

Die konkrete Ausgestaltung der Verantwortlichkeiten und Leistungsumfänge hängt massgeblich von den individuellen Vertragsverhandlungen und den kundenspezifischen Vereinbarungen mit den jeweiligen Partnern ab. Das hier beschriebene Szenario, basiert auf den Interviews mit den ZenDiS und BEDAG geführt im April 2026.

Wichtiger Hinweis: Die nachfolgend dargestellten Vertragsaspekte befinden sich noch vollständig in der Entwicklungsphase. Es existieren weder finale Angebote noch verbindliche Leistungsbeschreibungen. Die Auflistung dient ausschliesslich der Veranschaulichung möglicher Vertragsbestandteile und stellt keine Zusage oder Verpflichtung der genannten Partner dar.

Mögliche ZenDiS-Vertragsaspekte könnten beispielsweise umfassen:
- Potenzielle SLA-Vereinbarungen über eine Standard-Verfügbarkeit hinaus
- Verschiedene Support-Level-Optionen
- Mögliche Zusatzleistungen wie Migration, Schulung und Customizing
- Unterschiedliche Abnahmemengen und Preismodelle

Denkbare BEDAG-Vertragsbestandteile könnten beinhalten:
- Verschiedene Hosting-Konfigurationen und Ressourcenoptionen
- Backup- und Disaster-Recovery-Konzepte
- Compliance-Anforderungen und Audit-Verfahren
- Integrationsmöglichkeiten in bestehende IT-Infrastrukturen
- Unterschiedliche Support-Level und Eskalationsverfahren

Diese beispielhaften Vertragsaspekte sind als reine Orientierungshilfe zu verstehen und geben einen ersten Eindruck möglicher Gestaltungsoptionen. Die tatsächlichen Vertragskonditionen, Leistungsumfänge und organisatorischen Auswirkungen können erheblich von den hier dargestellten Beispielen abweichen und sind zum Zeitpunkt dieser Studie noch nicht definiert.

Beim Betrieb von openDesk Enterprise besteht ein Dreiecksverhältnis zwischen ZenDiS (Produktverantwortung), einem Hosting-Partner und den Komponentenherstellern. Die Rolle der Verwaltung verändert sich dadurch von der Nutzung eines integrierten Dienstes hin zur Koordination mehrerer Vertragspartner mit jeweils eigenen SLAs und Eskalationswegen.

3.4 Normative Ausgangslage

Der regulatorische Rahmen beim Einsatz von Cloud-Diensten lässt sich in drei Schichten gliedern, die sich nach Verbindlichkeit und Charakter unterscheiden.

Bindendes Recht bildet die erste Schicht. Massgeblich sind das jeweilige kantonale Datenschutzrecht, sektorspezifisches Recht für besonders regulierte Bereiche, beispielsweise die polizeiliche und justizielle Datenbearbeitung, kantonale Cybersicherheitsvorgaben sowie das Informationsschutzrecht mit den darin verankerten Klassifizierungspflichten. Hinzu treten das öffentliche Beschaffungsrecht und allgemeine Bestimmungen des Bundesrechts mit horizontaler Wirkung, etwa das Amtsgeheimnis.

Soft Law und Aufsichtspraxis bilden die zweite Schicht. Die Resolution der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) zur Auslagerung von Datenbearbeitungen in die Cloud adressieren explizit die Nutzung US-amerikanischer Hyperscaler durch Schweizer Behörden.[5]

Verwaltungsinterne Vorgaben, ISDS-Konzepte, IT-Reglemente, Klassifizierungsweisungen, bilden die dritte Schicht. Sie sind im jeweiligen Anwendungsbereich verbindlich, können das übergeordnete Recht aber weder ersetzen noch dispensieren.

Datenschutzecht

Das Datenschutzrecht der Kantone ist heterogen ausgestaltet. Jede Verwaltungseinheit untersteht primär dem Datenschutzrecht ihres Kantons. Über die kantonalen Unterschiede hinweg lassen sich folgende Anforderungen als typisch bezeichnen: das Erfordernis einer hinreichenden gesetzlichen Grundlage für jede Bearbeitung, Datenminimierung und Zweckbindung, Aufbewahrungs- und Löschpflichten, verschärfte Anforderungen für besonders schützenswerte Personendaten sowie eine vertragliche Regelung beim Beizug externer Bearbeiter.
Die Bekanntgabe von Personendaten ins Ausland ist regelmässig nur unter zusätzlichen Voraussetzungen zulässig, insbesondere bei angemessenem Schutz im Empfängerstaat oder bei rechtsgenüglichen Garantien. Die konkreten Anforderungen, namentlich an Standardvertragsklauseln und allfällige ergänzende Schutzmassnahmen, ergeben sich aus dem im Einzelfall anwendbaren Recht und der Praxis der zuständigen kantonalen Aufsichtsbehörde.
Eine eigenständige Pflicht zur Datenschutz-Folgeabschätzung für risikoreiche Bearbeitungen ist in mehreren kantonalen Gesetzen verankert. Im Kontext einer Plattformeinführung oder -migration ist die im Einzelfall anwendbare Regelung zu prüfen.

Sektorspezifisches Recht für Blaulichtorganisationen

Für die polizeiliche und justizielle Datenbearbeitung tritt sektorspezifisches Recht als lex specialis hinzu. Eine für die allgemeine Verwaltung datenschutzrechtlich vertretbare M365-Konfiguration präjudiziert die Zulässigkeit für den Blaulichtbereich nicht. Diese ist separat nach dem sektorspezifischen Recht zu beurteilen. Praktisch bedeutet dies, dass bestimmte

[5] Privatim, Resolution zur Auslagerung von Datenbearbeitung in die Cloud, URL: https://www.privatim.ch/wp-content/uploads/2025/11/20251124_privatim_Resolution-Hyperscaler_DE.pdf, abgerufen am 14. August 2026.

Datenkategorien, etwa Daten aus Vollzugsprozessen des Bundes oder besonders sensitive polizeiliche Informationen, auch dann von der M365-Standardumgebung auszunehmen sein können, wenn diese für die übrige Verwaltung freigegeben ist. Zudem bestehen erhöhte Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit der Informationen. Dies unterscheidet sie strukturell von anderen Verwaltungseinheiten im Kontext einer M365-Alternativenprüfung.

Cybersicherheit
Kantonale Cybersicherheitsvorgaben stützen sich regelmässig auf international rezipierte Standards und stellen Anforderungen an technische und organisatorische Massnahmen, die dem «Stand der Technik» entsprechen müssen. Die Auslegung dieses unbestimmten Rechtsbegriffs obliegt der jeweils zuständigen Aufsichtsstelle. Für Cloud-Arbeitsplatzplattformen sind insbesondere die Themen Identitäts- und Zugriffsmanagement, Verschlüsselung in Transit und at Rest sowie Schlüsselverwaltung relevant.

KI-Regulierung
Die Regulierung künstlicher Intelligenz wird in den Kantonen schrittweise eingeführt und ist zum Zeitpunkt der Erhebung in unterschiedlichem Stand und wird derzeit als Sicherheitsanforderung verstanden.

Beschaffungsrecht
Das öffentliche Beschaffungsrecht stellt strukturelle Anforderungen an die Auswahl von IT-Plattformen. Bei Hyperscaler-Plattformen ist der Anbietermarkt faktisch konzentriert, was den Wettbewerb in einer regulären Ausschreibung einschränkt. Sicherheitspolitisch exponierte Anbieter müssen darüber hinaus mit Akzeptanzrisiken im politischen Umfeld rechnen.

Systembedingte Rechtsrisiken
Neben vertraglichen und organisatorischen Anforderungen ergeben sich gewisse Risiken bereits aus der Architektur von Public-Cloud-Diensten sowie der internationalen Aufstellung ihrer Anbieter. Diese können durch vertragliche Massnahmen zwar adressiert und teilweise mitigiert, in der Regel jedoch nicht vollständig ausgeschlossen werden.

- Zugriffe durch ausländische Behörden:
  Ein wesentliches Thema sind extraterritoriale Zugriffs- und Überwachungsbefugnisse ausländischer Staaten. Bei US-Anbietern sind insbesondere zwei Regelwerke relevant: Der CLOUD Act verpflichtet Anbieter mit US-Bezug unter bestimmten Voraussetzungen zur Herausgabe von Daten, die sich in ihrem Einflussbereich befinden, unabhängig davon, wo diese gespeichert sind. Ergänzend erlaubt Section 702 FISA gezielte Überwachungsmassnahmen gegenüber Nicht-US-Personen, wobei auch Cloud-Anbieter zur Mitwirkung herangezogen werden können.
  Ein vertraglich vereinbarter Speicherort in der Schweiz reduziert dieses Risiko nicht vollständig, da die Anwendbarkeit des US-Rechts primär an den Anbieter anknüpft. Daraus ergibt sich ein Spannungsfeld zu den schweizerischen Rechtshilfeverfahren, die grundsätzlich eine Einbindung nationaler Behörden vorsehen. Vergleichbare Fragestellungen

können sich auch bei Anbietern aus anderen Jurisdiktionen mit weitreichenden behördlichen Zugriffsbefugnissen ergeben.
- Eingeschränkte Kontrolle und Auditierbarkeit: Nach den anwendbaren datenschutzrechtlichen Vorgaben bleibt der Verantwortliche verpflichtet, sich zu vergewissern, dass der Auftragsbearbeiter angemessene Datensicherheitsmassnahmen gewährleistet. In vielen Fällen ist die direkte Kontrolle von Cloud-Diensten durch den Verantwortlichen eingeschränkt und Auditmöglichkeiten beschränken sich häufig auf standardisierte Berichte oder Zertifizierungen unabhängiger Dritter.
  In der Praxis ergibt sich daraus eine gewisse Diskrepanz zwischen der rechtlichen Verantwortung, die beim Auftraggeber verbleibt, und den tatsächlichen Einflussmöglichkeiten auf die technische Umsetzung beim Anbieter.

Datenrecht und Migration
Ein potentieller Plattformwechsel von M365 zu einer Alternativlösung begründet eigenständige regulatorische Pflichten, die über jene des laufenden Betriebs hinausgehen. Die Migrationsphase konstituiert neue Bearbeitungsverhältnisse, aktiviert spezifische gesetzliche Anforderungen und exponiert die Verwaltungseinheit gegenüber Risiken, die im regulären Betrieb in dieser Form nicht bestehen:
- Bearbeitungsverhältnisse mit Migrationsdienstleistern: Die Datenübertragung aktiviert neue Auftragsbearbeitungsverhältnisse, die nach dem anwendbaren kantonalen Datenschutzrecht vertraglich abzubilden sind. Soweit externe Dienstleister Verwaltungsdaten im Klartext verarbeiten, sind sie funktional in den Geheimhaltungsverbund einzubeziehen.
- Datenschutz-Folgeabschätzung beziehungsweise Vorabkontrolle: Migrationsprojekte stellen aufgrund Datenmenge, Drittbeteiligung und Einsatz neuer Technologien typischerweise risikoreiche Bearbeitungen dar und sind nach den Vorgaben des im Einzelfall anwendbaren kantonalen Datenschutzrechts vorgängig zu beurteilen.
- Aufbewahrungs- und Löschpflichten: Gesetzliche Aufbewahrungspflichten, Archivrecht, Geschäftsunterlagen, sektorspezifische Fristen, bestehen unabhängig vom System fort. Gleichzeitig sind nicht mehr benötigte Daten auf der Quellplattform nach Zweckwegfall zu löschen. Da eine punktgenaue Löschung in Backups und Zwischenspeichern eines Hyperscalers technisch nur eingeschränkt möglich ist, sind Aufbewahrungs-, Rückgabe- und Löschfristen vertraglich vor Migrationsbeginn zu definieren und deren Einhaltung nachzuweisen.
- Datenportabilität und Informationssicherheit während der Transition: Die technische Fähigkeit, Daten vollständig, strukturiert und in einem weiterverwendbaren Format aus M365 zu exportieren, ist Voraussetzung für jeden Plattformwechsel; Umfang, Format und Vorhaltedauer beim bisherigen Anbieter sind vertraglich vor Migrationsbeginn zu klären. Während der Migration existieren Daten temporär in zwei Systemen, Zugriffsrechte werden umgebaut, neue Schnittstellen sind nicht vollständig gehärtet, technische und organisatorische Massnahmen sind explizit auch für diese Phase zu definieren und zu dokumentieren.

Praktisch bedeutet dies: Der eigentliche regulatorische Aufwand der Migration liegt nicht ausschliesslich in der Einhaltung einzelner Normen als in der vertraglichen Absicherung gegenüber sämtlichen beteiligten Parteien bisheriger Anbieter, Migrations- und Integrationsdienstleister, neuer Plattformanbieter und gegebenenfalls neuer Hosting-Provider, in der Dokumentation der Pflichterfüllung sowie in der Aufrechterhaltung des Schutzniveaus während eines technisch heiklen Übergangs. Diese Pflichten sind kostenrelevant und in der Wirtschaftlichkeitsbetrachtung einer Alternativenprüfung zu berücksichtigen.

Einsatz von M365 im Kontext der Rahmenvereinbarung DVS
Die öffentlich-rechtliche Rahmenvereinbarung über die Digitale Verwaltung Schweiz (BBl 2021 3030) weist der DVS unter anderem die Aufgabe zu, die beteiligten Gemeinwesen im Bereich der Digitalisierung und der IKT zu unterstützen, namentlich durch «Interessensvertretung gegenüber IKT-Anbietern, insbesondere hinsichtlich gemeinsamer Rahmenverträge und Konditionserklärungen der beteiligten Gemeinwesen» (Art. 4.2 Abs. 1 lit. e). Die DVS hat damit das Mandat, die Interessen der beteiligten Gemeinwesen gegenüber Anbietern wie beispielsweise Microsoft zentral zu vertreten, namentlich bei der Aushandlung gemeinsamer Rahmenverträge.

Gleichzeitig stellt die Rahmenvereinbarung klar, dass die DVS Empfehlungen abgibt, aber keine verbindlichen Regelungen aufstellt (Art. 2 Abs. 3), und dass die Vereinbarung nicht in die Zuständigkeiten des Bundes, der Kantone und der Gemeinden eingreift (Art. 1 Abs. 2). Die DVS erbringt zudem keine eigenen IKT-Leistungen (Art. 4.2 Abs. 2). Die Verantwortung für die Einhaltung der regulatorischen Vorgaben, insbesondere des anwendbaren Datenschutzrechts, der Informationssicherheitsvorgaben und des Amtsgeheimnisses, verbleibt damit vollumfänglich bei jedem einzelnen Gemeinwesen. Aus den koordinierten Rahmenverträgen ergeben sich faktische Standards, die rechtlich unverbindlich, aber politisch / ökonomisch wirksam sind. Somit kann die DVS die Vertragsverhandlung mit Anbietern zentralisieren, jedoch nicht die damit einhergehende regulatorische Verantwortung. Jedes Gemeinwesen steht somit in der Verantwortung eigenständig zu prüfen, ob der Einsatz von M365 für seine konkreten Datenkategorien und Geheimhaltungspflichten rechtskonform ist.

Zu den von der DVS getroffenen Massnahmen zählen unteranderem:
- Um den gemeinsamen Beschaffungsbedarf der Gemeinwesen systematisch zu erfassen, wurde durch die eOperations Schweiz AG eine umfassende Umfrage bei allen Kantonen durchgeführt, um den Bedarf an Alternativen zu Office-Produkten zu erfassen und zu quantifizieren.
- Als Ergänzung zu den bestehenden Rahmenverträgen werden weitere Konditionserklärungen als Vertragsbestandteile und -grundlagen für die Beschaffung von Hard- und Software entwickelt. Entsprechende Konditionserklärungen sollen mit Anbietern wie ZenDis, Infomaniak und weiteren initiiert werden, um den Gemeinwesen einen erweiterten Rahmen für ihre Beschaffungen zu bieten.
- Zur strategischen Weiterentwicklung kann das Thema Digitalisierungssouveränität und die Erhöhung der Handlungsfähigkeit der Verwaltung in einer neuen Fachgruppe mit Experten

diskutiert werden. Diese Vertiefungsgruppe kann Teilnehmende aus verschiedenen bestehenden Arbeitsgruppen einbeziehen und auf der bereits bestehenden Vertiefungsgruppe aufbauen.
- Abschliessend ist festzuhalten, dass durch die von der DVS geführten M365-Vertragsverhandlungen bedeutend verbesserte Vertragskonditionen für die beteiligten Gemeinwesen erreicht wurden, namentlich Zusatzrabatte bei verschiedenen Produkten sowie die Unterstellung unter Schweizer Recht statt ausschliesslich ausländischem Recht.

3.5 Ergebnisse der Analyse

3.5.1 Untersuchungseinheiten und Hinweis zur Analyse

Um die Auswirkungen eines Wechsels von M365 zu openDesk konkret zu erfassen, wurden zwei Verwaltungseinheiten als Untersuchungseinheiten beigezogen. Beide Einheiten setzen M365 heute produktiv ein, unterscheiden sich jedoch hinsichtlich Grösse und organisatorischer Ausprägung ihrer IT.
- Die Untersuchungseinheit 1 ist eine kantonale Verwaltung mit rund 6’000 Verwaltungsmitarbeitenden. Die zentrale Informatikorganisation umfasst rund 200 Mitarbeitende, die den Betrieb und die Weiterentwicklung der zentralen IKT-Services verantworten.
- Die Untersuchungseinheit 2 ist eine mittelgrosse Verwaltung mit etwa 1’500 Verwaltungsmitarbeitenden. Die IT-Organisation zählt rund 70 Mitarbeitende und ist für die Bereitstellung der Arbeitsplatz- und Fachanwendungen zuständig.

Die Analysen stützen sich auf strukturierte Gespräche mit den jeweiligen CIOs sowie mitverantwortlichem Team-bzw. Abteilungsmitgliedern aus der M365-Organisation, sowie ausgewählten Vertretern von Blaulichtorganisationen. Es handelt sich dabei um ausgewiesene Fachexpertinnen und -Experten, deren Einschätzungen auf langjähriger Praxiserfahrung beruhen. Die Ergebnisse sind als qualifizierte Expertenmeinungen der jeweiligen Organisation zu verstehen und erheben keinen Anspruch auf Vollständigkeit oder eine umfassende, empirische Marktstudie.
Ergänzend dazu wurden fünf kantonale Verwaltungen in einem reduzierten Umfang als sogenannte „Validierungspartner“ mit einem Fragebogen beigezogen, um die zentralen Erkenntnisse der beiden Untersuchungseinheiten zu spiegeln. Ein Kondensat ist in dieses Kapitel eingeflossen.

Betriebssysteme sowie Low-Code-/Automatisierungsplattformen wurden zwar im Rahmen der Ist-Erhebung adressiert, jedoch bewusst nicht in eine detaillierte Soll-Bewertung einbezogen, um den Umfang der Studie klar zu begrenzen.

3.5.2 Ergebnisse der Analyse Untersuchungseinheit 1

3.5.2.1 Technische Ist-Situation

Übersicht des eingesetzten M365 Funktionsumfangs:

Die Untersuchungseinheit 1 setzt M365 sehr umfassend und zielgerichtet für die tägliche Arbeit der Angestellten der Kernverwaltung ein. Im Mittelpunkt steht die Unterstützung moderner Arbeitsformen, die Steigerung der Produktivität und die Einhaltung hoher Sicherheits- und Compliance-Standards. Die hohe Durchdringung der relevanten Kernfunktionen von M365 zeigt einen fortgeschrittenen Digitalisierungsgrad auf. In einzelnen Gebieten wird zudem die Nutzung weiterer Funktionen angestrebt, wie zum Beispiel im Bereich Datenklassifikation mit systemgestützten Tagging-Mechanismen und Data Loss Prevention (DLP). Lediglich im Bereich Künstliche Intelligenz ist die Nutzung der entsprechenden M365-Services aktuell gezielt limitiert. Anstelle des Microsoft Copilot greift die Untersuchungseinheit 1 auf eine eigens betriebene Lösung zurück.

Die folgende Tabelle bewertet den Funktionsumfang des eingesetzten M365 Produkte in zentralen Themenbereichen anhand einer fünfstufigen Skala. Die Skala dient der Einordnung, wie umfassend und fortgeschritten die jeweiligen M365-Dienste bereits organisatorisch genutzt werden

Stufe	Beschreibung
1	Nicht/nur sehr rudimentär genutzt
2	Einzelne Anwendungsfälle
3	Gelegentlicher Einsatz
4	Umfassender Einsatz, teilweise erweiterte Nutzung und Integration
5	Sehr umfassender und tief integrierter Einsatz im Regelbetrieb

Tabelle 6: Bewertungsstufen Nutzung von M365 Produkte

Die nachfolgende Analyse konzentriert sich auf die wichtigsten Dienste und Anwendungen von M365, die in der Verwaltung eine zentrale Rolle spielen. Im Fokus stehen hierbei insbesondere Dienste und Anwendungen wie Exchange Online, SharePoint Online oder Microsoft Teams. Weniger zentrale Services, wie etwa Loop oder Clipchamp, bleiben im Rahmen dieser Betrachtung unberücksichtigt. Die nachfolgende Tabelle bietet einen kompakten Überblick über die aktuell im Einsatz befindlichen, zentralen M365-Komponenten und ordnet sie den jeweiligen Funktionsbereichen zu.

Funktionsbereich	Einstufung	Eingesetzte Dienste und Anwendungen
Kommunikation und Kollaboration	5	Teams Exchange Online Outlook
Produktivitäts- und Geschäftsanwendungen	5	Excel Word PowerPoint Access

Datei- und Informationsmanagement	5	SharePoint Online SharePoint On-premise OneDrive
Sicherheit und Compliance	5	Defender for Endpoint Defender for Office 365 Defender for Server Sentinel Purview Intune
Künstliche Intelligenz	1	Microsoft Copilot wird nicht eingesetzt
Betriebssystem	5	Windows 11 (64 Bit)
Identitäts- und Zugriffsmanagement	5	Entra ID Entra PIM Active Directory Windows Hello for Business Microsoft Authenticator
Analytics und Automatisierung	4	Power BI Power Apps Power Automate

Tabelle 7: Analyse Nutzung M365 Untersuchungseinheit 1

Kommunikation und Kollaboration:

- Exchange und Outlook: In der Untersuchungseinheit 1 wird Exchange Online für die Endbenutzer-Mailboxen verwendet. Jeder Mitarbeitende verfügt über eine eigene Mailbox, und für Fachabteilungen stehen Gruppenmailboxen zur Verfügung. Die Mitarbeitenden nutzen überwiegend den Outlook-Desktop-Client für den E-Mail-Zugriff.
- Teams: Teams ist als Standardlösung im Einsatz zum Telefonieren und Chatten, sowohl innerhalb der Verwaltung als auch in das öffentliche Telefonnetz (Public Switched Telephone Network, PSTN). Die Zusammenarbeit mit Office-Dokumenten findet überwiegend über den klassischen Fileservice statt. Teams und SharePoint werden primär für Projekte und ad-hoc Kollaboration genutzt. Zudem ist Teams Rooms im Einsatz, bei denen spezielle Hardware für hybride Meetings zur Verfügung steht. Es werden auch Teams Premium Lizenzen mit zusätzlichen Möglichkeiten, insbesondere bei der Verschlüsselung, eingesetzt. Es können Addins und Apps aus dem M365 “Marktplätzen” bezogen werden, diese unterliegen jedoch einer zentralen Prüfung und Freigabe.

Produktivitäts- und Geschäftsanwendungen:

- Excel, Word, und PowerPoint: Die Angestellten der Kernverwaltung nutzen sowohl die Desktop-Version als auch die Web-Version der Standardanwendungen Excel, Word und PowerPoint im Rahmen von Office 365 für die Erstellung textbasierter Unterlagen. Vereinzelt sind auch legacy Geschäftsapplikationen auf Basis von Access im Einsatz.

Datei- und Informationsmanagement:

- OneDrive: 2025 wurde der bisherige Home-Laufwerk-Speicher durch OneDrive ersetzt. Jeder Angestellte der Kernverwaltung verfügt über ein eigenes OneDrive-Profil mit einem Terabyte Speicher.

- SharePoint: SharePoint Online wird primär für Dateiablagen in Teams genutzt. Ausserdem sind vereinzelt eigenständige SharePoint Seiten im Einsatz. SharePoint wird auch als Datenquelle für die Power Plattform verwendet. Es gibt kleinere Fachanwendungen, welche mit SharePoint on Premises betrieben werden. SharePoint wird nicht für das Intranet und Wiki eingesetzt.

Sicherheit und Compliance:
- Defender: Defender ist sowohl im Server- als auch im Client-Bereich als Antivirenschutz im Einsatz. Zusätzlich wird Defender für Office 365 verwendet, um auch den E-Mail-Verkehr abzusichern. Durch den Einsatz von Defender als XDR-Lösung werden Bedrohungen über Identitäten, Anwendungen und weitere Ressourcen hinweg automatisiert erkannt, untersucht und abgewehrt.
- Sentinel: Microsoft Sentinel wird als Security Information and Event Management (SIEM) Lösung eingesetzt und dient als zentrales Log-Management System für das Security Operations Center (SOC).
- Purview: Microsoft Purview wird für die Umsetzung von Retention Policies für alle Daten eingesetzt. Über das E-Discovery wird eingesetzt, um gelöschte Daten unter dem Retention Hold zu suchen und wiederherzustellen. Diese Funktion wird unter anderem für die gezielte Wiederherstellung von Daten genutzt. Es befindet sich derzeit ein Projekt in der Umsetzung mit dem Ziel Sensitivity Labels zur Klassifizierung und zum Schutz von Daten mit Microsoft Purview einzuführen.
- Intune: Microsoft Intune wird als cloudbasierte Enterprise-Mobility-Management-Lösung eingesetzt zur Verwaltung und Sicherung von Organisationsdaten auf mobilen Endgeräten. Die Untersuchungseinheit 1 registriert, konfiguriert und verwaltet neue Geräte mittels Mobile Device Management (MDM). Beispielsweise stellt eine Blaulichtorganisation für ihre Mitarbeitenden ca. 1400 mobile Geräte zur Verfügung, welche mittels MDM verwaltet werden. Auf privaten Smartphones, die für den Zugriff auf Unternehmensressourcen genutzt werden, werden M365-Anwendungen mittels Mobile Application Management (MAM) verwaltet und damit Organisationsdaten auf App-Ebene geschützt. Die Organisationsdaten in diesen Apps sind verschlüsselt abgelegt und zusätzlich durch eine PIN geschützt. Es wird gesteuert, welche Daten die jeweiligen Apps verlassen dürfen und welche nicht. So ist es beispielsweise nicht möglich, Dokumente aus einer geschützten App mit einer nicht freigegebenen Drittanbieter-Anwendung zu öffnen, und auch das Kopieren und Einfügen von Inhalten ist in seinem Umfang eingeschränkt. Zusätzlich kann im Bedarfsfall ein Remote Wipe der Unternehmensdaten durchgeführt werden, ohne dass private Daten auf dem Gerät davon betroffen sind.

Künstliche Intelligenz:
- Copilot: Der KI-Dienst Copilot ist auf Tenant-Ebene deaktiviert. Die Untersuchungseinheit 1 nutzt einen eigenen KI-Chatbot. Dieser ist verfügbar für alle nicht geheimen Daten und läuft als Standalone-Lösung, ohne Integration in Office-Anwendungen.

Betriebssystem:

- Windows: Windows 11 wird in der 64-Bit-Version eingesetzt. Die Office-Anwendungen sind jedoch in der 32-Bit-Version installiert. Zudem ist auf den Systemen die BitLocker-Verschlüsselung aktiviert, um die Daten vor unbefugtem Zugriff zu schützen.

Identitäts- und Zugriffsmanagement:
- Active Directory und Entra ID: Für die zentrale Verwaltung von Benutzern und Rechten wird sowohl Active Directory (on-premise) als auch Entra ID (Cloud) eingesetzt.
- Windows Hello: Zur Anmeldung an Windows-Geräten wird Windows Hello for Business Anmeldemethode eingesetzt. Dabei kommen Methoden wie Gesichtserkennung, Fingerabdruck oder PIN zum Einsatz. Es werden zudem Passkeys (FIDO2) eingesetzt.
- Authenticator: Zur Multifaktor-Authentifizierung kommt die Microsoft Authenticator App zum Einsatz. Benutzer bestätigen ihre Anmeldungen per App auf dem Smartphone, per Push-Benachrichtigung, Zahleneingabe oder biometrischem Faktor.
- Entra ID PIM: Für die Verwaltung von privilegierten Konten (z. B. Administratoren) wird Entra PIM verwendet. Hierüber können erhöhte Rechte für definierte Zeiträume angefordert und zugeteilt werden.

Analytics und Automatisierung:

- Power BI: Power BI wird über alle Verwaltungseinheiten eingesetzt in verschiedensten Themengebieten. Historisch gesehen wurde Power BI Reportserver als SQL-Server Reportserver (SSRS) on-premises genutzt, während mittlerweile zunehmend auch der Power BI Reportserver in der Cloud eingesetzt wird. Derzeit existieren über 1000 Einzelreports, von denen etwa 10 Prozent in der Cloud und 90 Prozent on-premises betrieben werden.
- Power Apps: Einerseits gibt es eine Umgebung für persönliche Produktivität. Andererseits gibt es für business-relevante Anwendungsfälle Managed-Umgebungen, die von der zentralen IT betreut werden über festgelegte DLP-Richtlinien verfügen. Die Untersuchungseinheit 1 setzt auf PowerApps entwickelte Anwendungen für ein breites Spektrum ein. Beispielsweise in der Pikettverwaltung, Störungsmeldungen, Erfassung Nebenbeschäftigungen und Budgetkontrolle. Einige Use Cases werden aus Business Continuity Management Gründen nicht mit der Power Platform umgesetzt. Beispielsweise sind Notrufzentralen ausgenommen, da hier besonders hohe Kritikalität besteht. Es sind schätzungsweise 50 Business relevante Power Apps im Einsatz, welche durch ganze Teams genutzt werden. Rechnet man auch Power Apps ein, welche nur einzelne Nutzer für ihre persönliche Produktivität einsetzen, dann sind es ca. 260 Apps.
- PowerAutomate: PowerAutomate wird in der Untersuchungseinheit 1 für einfache bis komplexe Automatisierungs- und/oder Digitalisierungsanwendungsfälle eingesetzt. Es sind derzeit ca. 100 Power Automate Workflows im Einsatz, welche dezentral in den Fachbereichen erstellt und gewartet werden.

Die Untersuchungseinheit 1 nutzt M365 umfassend und integriert nahezu alle zentralen Dienste wie Teams, Outlook, SharePoint und Sicherheitslösungen im Arbeitsalltag. Die Nutzung von KI-Funktionen wie Microsoft Copilot ist jedoch gezielt eingeschränkt, stattdessen setzt die Untersuchungseinheit 1 auf eine eigene on-premise Lösung.

Übersicht der Integrationen in M365:
Untersuchungseinheit 1 verfolgt einen konsequenten Digitalisierungsansatz und bindet in diesem Rahmen eine Vielzahl von Fachanwendungen und Tools in die M365 Umgebung ein. Aktuell bestehen über 50 Applikationen mit verschiedenen Integrationsszenarien aus beinahe allen Verwaltungseinheiten. Insbesondere in den Bereichen Kommunikation, Kollaboration, Sicherheit und Identitätsmanagement sind tiefe und in Teilen bidirektionale Anbindungen implementiert, die einen standardisierten und effizienten Informationsfluss zwischen den Systemen gewährleisten. Eine Ausnahme bilden die Blaulichtorganisationen wie die Polizei und Rettungsdienste, deren Systeme aufgrund von besonders restriktiven Anforderungen bislang wenige Anbindungen an die M365-Plattform aufweisen.

Um den Integrationsgrad der einzelnen Funktionsbereiche systematisch darzustellen, verwenden wir folgende Skala:

Stufe	Beschreibung
1	Keine Integrationen
2	Vereinzelte Integrationen
3	Umfassende Integrationen

Tabelle 8: Bewertungsskala Integrationsgrad der einzelnen Funktionsbereiche

Die folgende Tabelle zeigt, für welche Funktionsbereiche in welchem Umfang Integrationen vorliegen:

Funktionsbereich	Einstufung	Beispielhafte Integrationen
Kommunikation und Kollaboration	3	IncaMail (Verschlüsselungsservice der Schweizerischen Post) Hoxhunt für Phishing-Simulation Luware Nimbus Competella Kurmi Intranet SEPPmail
Produktivitäts- und Geschäftsanwendungen	2	Vorlagenverwaltung
Datei- und Informationsmanagement	3	Gever-System Sharepoint File-Service
Sicherheit und Compliance	3	Sentinel Purview Defender for Endpoint Defender for M365
Künstliche Intelligenz	1	Keine
Betriebssystem	3	Matrix 42 (Service Management) Lenovo Cloud Deploy und Device Orchestrator
Identitäts- und Zugriffsmanagement	3	Citrix KeyCloak Ivanti SAP Cloud Identity
Analytics und Automatisierung	2	Power Platform Konnektoren

Tabelle 9: Analyse Integrationstiefe Funktionsbereiche Untersuchungseinheit 1

Im Rahmen der folgenden Ausführungen wird jeweils auf die zentralsten und betrieblich signifikanten Integrationen eingegangen.

Kommunikation und Kollaboration:
Im Bereich Kommunikation und Kollaboration sind verschiedene M365-Integrationen im Einsatz. Beispielsweise sind verschiedene Fachapplikationen an M365 angebunden, um automatisierte Alerts via Mail zu versenden. Für verschlüsselte E-Mails wird IncaMail in Outlook verwendet.

Zudem wird Hoxhunt in Outlook eingesetzt, um Mitarbeitende durch Phishing-Simulationen zu sensibilisieren.

Im Bereich Telefonie sind Lösungen wie Luware Nimbus und Competella in Teams integriert. Beispielsweise werden Telefonzentralen über Competella betrieben, wobei Teams für die Telefonie und den Prozess dahinter verwendet wird. Die Session Border Controller werden in eigenen Rechenzentren betrieben, sind notwendig für externe PSTN-Anrufe und sind mit Teams-Telefonie verbunden. Das Intranet zeigt den aktuellen Präsenzstatus der Teams-User, sodass ersichtlich ist, ob jemand beschäftigt oder offline ist.

Produktivitäts- und Geschäftsanwendungen:
Im Bereich Produktivitäts- und Geschäftsanwendungen ist besonders das Vorlagenmanagement Tool Office at Work als M365 Integration relevant. Mit Office at Work sind zahlreiche Template-Vorlagen für Word, Excel, PowerPoint und auch für E-Mail-Signaturen zentral verfüg- und steuerbar, die sowohl in der Desktop- als auch in der Web-Version genutzt werden.

Datei- und Informationsmanagement:
Im Bereich Datei- und Informationsmanagement sind verschiedene Integrationen vorhanden. Beispielhaft wird die Sharepoint-basierte Anwendung als zentrale Ablage für Projekt-Dokumente eingesetzt.

Sicherheit und Compliance:
Im Bereich Sicherheit und Compliance stellen Sentinel und Microsoft Purview zentrale Integrationsknotenpunkte dar.

Das SIEM-System Microsoft Sentinel ist tief in die gesamte M365- und Azure-Infrastruktur eingebettet und ermöglicht eine ganzheitliche Überwachung und analysebasierte Auswertung der Security-Events. Insbesondere ist Sentinel über Schnittstellen direkt mit Defender-Produkten (Defender for Endpoint, Defender for Office 365) und verschiedenen Audit- und Logquellen aus der Microsoft-Cloud sowie Hybridkomponenten integriert. Das Security Operations Center (SOC) nutzt Sentinel.
Microsoft Purview ist für die Durchsetzung von Retention-Policies und insbesondere für Auditing und E-Discovery zentral integriert. Es besteht eine Schnittstelle zur M365- und Azure-Umgebung, sodass beispielsweise Aktivitäten in Exchange Online, SharePoint Online und Teams zentral protokolliert und in Verdachts- oder Missbrauchsfällen ausgewertet werden können.

Künstliche Intelligenz:
Im Bereich Künstliche Intelligenz ist die Nutzung der entsprechenden M365-Services aktuell gezielt limitiert. Anstelle des Microsoft Copilot greift die Untersuchungseinheit 1 auf eine eigens betriebene Lösung zurück. Daher gibt es in diesem Bereich keine relevanten Integrationen.

Betriebssystem:
Im Bereich Betriebssystem und Clients sind verschiedene Integrationen in M365 vorhanden. Das Service-Management-Tool Matrix42 dient als zentrales ITSM-System. Darin werden unter anderem die ITIL-Prozesse Incident Management, Problem Management und Change Management (per Ticket) abgewickelt. Matrix42 umfasst zudem verschiedene weitere Funktionsbereiche, wie z. B. Configuration Management (CMDB), Softwarepaketverwaltung, Vertragsmanagement sowie Servicebeschreibungen. Für Lenovo Geräte kommen zwei zentrale Tools zum Einsatz: Cloud Deploy und Device Orchestrator. Ohne diese Tools können keine neuen Geräte bereitgestellt werden. Die Automatisierung erfolgt durch die Anbindung von Skripten auf Clients und Konfigurationen, die über die Graph API und PowerShell implementiert werden.

Identitäts- und Zugriffsmanagement:
Im Bereich Identitäts- und Zugriffsmanagement fungiert Entra ID als zentraler Cloud-Identity-Provider. Die lokale Active Directory wird bidirektional mit Entra ID synchronisiert, sodass Identitäten, Gruppen und Berechtigungen konsistent sowohl On-Premises als auch in der Cloud verfügbar sind.
Eine Vielzahl weiterer Lösungen ist direkt oder indirekt an das M365-IAM angebunden:

- Die Anmeldung bei Citrix-Diensten erfolgt über Entra ID. Der Zugriff auf Citrix-Umgebungen ist zusätzlich mit Multi-Faktor-Authentifizierung abgesichert.
- Keycloak fungiert als On-Premises-Broker für bestimmte Fachanwendungen. Authentifizierungsanfragen werden von Keycloak übernommen und an Entra ID zur eigentlichen Identitätsprüfung weitergeleitet. Keycloak wird insbesondere für das Smart Service Portal als zentrale IAM-Komponente genutzt.
- SAP Cloud Identity ist ebenfalls mit Entra ID gekoppelt und dient als Identitätsprovider für verschiedene SAP-Anwendungen.
- Auf den Endgeräten sorgt Ivanti für die Bereitstellung einer Always-On-VPN-Lösung, bei der die Benutzerauthentifizierung zentral über Entra ID erfolgt. In Kombination mit Windows Hello for Business, das als Multi-Faktor-Authentifizierung (Biometrie, PIN oder FIDO-Security-Key) genutzt wird, ist für die Benutzer nach der Anmeldung am Gerät ein Single Sign-On zu M365-Diensten gegeben.
- Für bestimmte Geschäftsanwendungen wird der Oracle Identity Manager (OIM) als Identity-Governance- bzw. Provisioning-System eingesetzt. OIM konsolidiert dazu relevante Identitäts- und Berechtigungsdaten aus angebundenen Quellsystemen und stellt diese für die weiterführende Nutzung in nachgelagerten Zielsystemen bereit; hierzu gehört auch die Bereitstellung ausgewählter Identitätsdaten für Entra ID, das die zentrale Authentifizierung übernimmt.

Analytics und Automatisierung:
Im Bereich Analytics und Automatisierung sind zahlreiche Power BI Reports im produktiven Einsatz, die teilweise auf unterschiedliche Datenquellen zugreifen, sowohl cloudbasiert als auch on-premises. Die Datenintegration erfolgt dabei häufig über die Power Platform Konnektoren. Ergänzend werden PowerApps und Power Automate Flows genutzt, um Workflows zu

automatisieren und einen bidirektionalen Datenaustausch zwischen M365 und Fachapplikationen zu ermöglichen.

Daten:
Derzeit werden beim Untersuchungseinheit 1 Daten der Datenkategorien öffentlich bis vertraulich (inklusive Personendaten) in M365 bearbeitet für definierte Anwendungsfälle. Für Migrationen von Geschäftsprozessen und neuen Anwendungsfälle in M365 muss eine zusätzliche individuelle Prüfung vorab erfolgen. Es werden derzeit keine geheimen Daten in M365 bearbeitet.
Das aktuell genutzte Datenvolumen auf Exchange Online beträgt ca. 25 Terabyte, auf SharePoint Online ca. 15 Terabyte, und auf OneDrive for Business ca. 56 Terabyte. Aufgrund der vorhandenen Lizenz kann die Untersuchungseinheit 1 bis zu 80 Terabyte auf SharePoint Online speichern.

Zudem sind verschiedene für die Verwendung in M365 vorgesehene Makros, Vorlagen, und zugeschnittene Low-Code Entwicklungen im Einsatz. Makros werden verwaltungsweit hauptsächlich für Listen- und Datenmutationen sowie zur Datenübernahme aus Fachapplikationen in Office-Dokumente genutzt.
Makros werden wo immer möglich durch alternative Lösungen (z. B. Power BI, Office Scripts) ersetzt. Nicht ersetzbare Makros werden geprüft und zentral mittels Zertifikat signiert, um Veränderungen zu verhindern. Es dürfen nur signierte VBA-Skripte ausgeführt werden.

Es sind über 100 zentrale Vorlagen für wiederkehrende Geschäfte und Briefverkehr, beispielsweise Projektedokumente oder Präsentationen im Einsatz. Die Untersuchungseinheit 1 nutzt das Vorlagenmanagementsystem Office at Work.

Zudem sind diverse Microsoft Power Platform Low Code Entwicklungen im Einsatz, darunter Power BI Dashboards, Microsoft Power Apps Anwendungen, und Power Automate Flows.

Die Untersuchungseinheit 1 hat mehr als 50 Fachanwendungen und Tools über verschiedene Integrationsszenarien tief in die M365-Umgebung eingebunden. Besonders in den Bereichen Kommunikation, Kollaboration, Sicherheit, Datei- und Identitätsmanagement bestehen weitreichende, oft bidirektionale Anbindungen, die effiziente und standardisierte Prozesse ermöglichen. Eine Ausnahme bilden die Blaulichtorganisationen, deren Systeme aus Datenschutzgründen bislang nicht in M365 integriert sind.

3.5.2.2 Organisatorische Ist-Situation

Die organisatorische Analyse der Untersuchungseinheit 1 verdeutlicht eine IT-Landschaft, die über die letzten Jahre konsequent auf den Betrieb und die Nutzung des Microsoft Ökosystems und M365 optimiert wurde. Seit dem produktiven Regelbetrieb von M365 im Jahr 2022 hat die

organisatorische Integration einen hohen Reifegrad erreicht. Dies manifestiert sich in folgenden Kernbereichen:

- Spezialisierte Rollenprofile: Die Untersuchungseinheit 1 verfügt über eingespielte Teams mit tiefem Expertenwissen in den Bereichen Workplace- und Application-Services. Die internen Kompetenzen sind passgenau auf die Cloud-Governance und die Administrationswerkzeuge von Microsoft ausgerichtet.
- Getätigte Investitionen: Der heutige Betrieb fusst auf massiven Investitionen in spezifisches Microsoft-Know-how. Die Fachkräfte sind hochgradig spezialisiert, was eine hohe Servicequalität ermöglicht, die Organisation aber personell eng an die technologische Roadmap des Herstellers bindet.
- Zentralisierte Governance: Die strategische Steuerung sowie Architektur- und Change-Entscheidungen erfolgen über eine fest installierte Koordinationsstelle. Dies stellt sicher, dass Neuerungen im M365-Tenant kontrolliert und kantonsweit harmonisiert eingeführt werden.
- Skalierbarer Support: Der User-Support ist hochgradig befähigt, Anwenderanfragen effizient zu bearbeiten. Da die Applikationen aufgrund ihrer Marktverbreitung auch im privaten Umfeld bekannt sind, profitiert die Organisation von einer hohen intuitiven Akzeptanz und einem geringen Schulungsbedarf bei Basisfunktionen.
- Kontinuierlicher Engineering-Aufwand: Auch das M365-Ökosystem erfordert laufende Anpassungen bei Konfiguration und Funktionalität und ist nicht wartungsfrei und erfordert somit stetige Aufwände interner Engineers. Da komplexe Störungen und die Ursachenanalyse beim Backend in Kooperation mit dem Hersteller zu lösen sind, ist die Organisation auf den Herstellersupport angewiesen.

Die Untersuchung zeigt ferner ein stabiles Bild:

- Strategie & Sourcing: Durch die Konzentration auf einen Hauptlieferanten ist der Sourcing-Aufwand strukturell optimiert. Die Prozesse für Lizenzierung und Provisionierung sind weitgehend automatisiert, was die internen Management-Ressourcen schont und eine hohe Planbarkeit schafft.
- Design & Governance: Die Untersuchungseinheit 1 profitiert von der «Quasi-Standardisierung» des Produktes, was eigene Architektur und Integrationsaufwände minimieren.
- Operations & Engineering: Die personelle Ausstattung im Betrieb gilt als solide. Der Fokus liegt primär auf der Konfiguration und dem Monitoring der Cloud-Dienste. Die Verantwortung für das Backend-Engineering liegt beim Provider, was die interne Organisation von hardwarenahen Betriebsaufgaben entlastet.
- Change & User Adoption: M365 wird als moderner Arbeitsplatz wahrgenommen. Die Einführung neuer Features erfolgt agil über die vom Hersteller vorgegebenen Release-Zyklen. Die Herausforderung besteht hierbei weniger in der technischen Bereitstellung als vielmehr in der kontinuierlichen Begleitung der Nutzer bei der Anwendung neuer Kollaborationsformen.

Der Untersuchungseinheit 1 ist bewusst, dass die aktuelle Ausrichtung auf M365 zu einer signifikanten Abhängigkeit führt. Man nutzt zwar die Vorteile der herstellergetriebenen Standardisierung zur Reduktion des interkantonalen Koordinationsaufwands, erkennt jedoch den damit verbundenen strategischen Lock-in bei Prozessen und aufgebauten Kompetenzen und Profilen explizit an.

Zusammenfassend ist die heutige Organisation der Untersuchungseinheit 1 auf Effizienz und die Nutzung von Synergien innerhalb der Microsoft-Welt ausgerichtet. Die Prozesse sind schlank, die Verantwortlichkeiten klar definiert und die Belegschaft ist mit den Werkzeugen vertraut.

3.5.2.3 Regulatorische Ist-Situation

Die regulatorische Analyse der Untersuchungseinheit 1 im spezifischen Kontext einer Blaulichtorganisation zeigt ein insgesamt gefestigtes, risikobasiertes Steuerungsmodell im Umgang mit M365. Die Nutzung der Plattform wird aus Sicht der Organisation als bewusst eingegangenes und gesteuertes Risiko verstanden, das durch institutionelle, technische und organisatorische Massnahmen auf ein, als tragfähig beurteiltes Niveau reduziert wird. Gleichzeitig werden strukturelle Grenzen dieses Ansatzes erkannt, die weder technisch noch vertraglich vollständig aufgelöst werden können.

Dies manifestiert sich in folgenden Kernbereichen:

- Risikobasierter Steuerungsansatz: Die Nutzung von M365 erfolgt auf Grundlage eines institutionell verankerten Konzepts für Informationssicherheit und Datenschutz (ISDS). Dieses verknüpft regulatorische Anforderungen systematisch mit technischen und organisatorischen Massnahmen (TOMs). M365 wird dabei nicht als per se konforme Lösung verstanden, sondern als Plattform, deren Einsatz unter Berücksichtigung eines definierten Restrisikos erfolgt.
- Spezifische Nutzungseinschränkungen: Bestimmte Datenkategorien, insbesondere primär klassifizierte Informationen gem. ISG/ISV des Bundes, unterliegen besonderen Vorgaben. Nach Einschätzung des Interviewpartners schliessen diese derzeit eine Bearbeitung über Standarddienste von M365 aus. Die eingesetzten Behelfslösungen (insbesondere E2E-Verschlüsselung mittels eGov-Zertifikat) werden dabei als funktional eingeschränkt beurteilt.
- Eingeschränkte Datenhoheit: Ein zentrales Thema stellt aus Sicht der Organisation die fehlende Kontrolle über die Verschlüsselungsschlüssel dar. Da diese beim Anbieter liegen, ergibt sich eine technologiebedingte, faktische Einschränkung der Datenhoheit. Das damit verbundene Restrisiko wird im Rahmen des ISDS-Konzepts systematisch beurteilt und als akzeptable eingeordnet, gleichzeitig wird der Einsatz einer eigenen Schlüsselkontrolle aktiv geprüft.
- Datenklassifikation im Aufbau: Die Umsetzung der Datenklassifikation auf der Basis der verabschiedeten einschlägigen organisatorischen Vorgaben befindet sich nach Angaben des Interviewpartners noch in der Umsetzung. Dies erschwert aktuell eine durchgehend

differenzierte und konsistente Anwendung von Schutzmassnahmen über alle Datenkategorien hinweg.
- Begrenzte wahrgenommene Handlungsalternativen: Funktional gleichwertige Alternativen zu M365 werden aus Sicht des Interviewpartners derzeit nicht gesehen. Insbesondere wird die integrierte Sicherheitsarchitektur von M365 als Vorteil hervorgehoben, da sie mit vergleichsweise geringem personellem Aufwand ein Schutzniveau ermöglicht, das mit separaten Einzellösungen nicht in gleichem Mass erreichbar wäre.

Die Untersuchung zeigt ferner folgendes Bild:
- Rechtsrahmen & Aufsicht: Die primäre rechtliche Grundlage bildet die anwendbare kantonale Datenschutzgesetzgebung. Die Aufsicht durch die zuständige Datenschutzbehörde erfolgt nach Einschätzung des Interviewpartners aktiv, insbesondere im Hinblick auf die Überprüfung der technischen und organisatorischen Massnahmen. Generelle Einschränkungen hinsichtlich der Nutzung von Cloud-Diensten bestehen dabei nicht, sofern die gesetzlichen Anforderungen eingehalten werden.
- Bundesrechtliche Spezialanforderungen: In Bereichen mit Bundesbezug bestehen zusätzliche regulatorische Vorgaben, die von den allgemeinen kantonalen Regelungen abweichen können. Diese führen in der operativen Umsetzung zu Abgrenzungsfragen und punktuellen Einschränkungen bei der Nutzung von Cloud-Diensten.
- Externe Orientierungshilfen: Fachliche Leitlinien, z. B. von privatim, sind der Organisation bekannt und werden berücksichtigt. Ihre Anwendung erfolgt jedoch im Sinne eines risikobasierten und praxisorientierten Ansatzes.
- Beschaffungsrechtlicher Rahmen: Die Anbieterwahl erfolgt im Rahmen der Vorgaben des öffentlichen Beschaffungsrechts. Nach Einschätzung des Interviewpartners beeinflussen dabei auch politische und sicherheitspolitische Akzeptanzüberlegungen den faktisch verfügbaren Anbietermarkt.
- Governance & Kontrollinstanzen: Die regulatorische Steuerung ist institutionell verankert (Informationssicherheit und Datenschutz) und wird aktiv umgesetzt. Ergänzend ist der Aufbau weiterer Koordinationsfunktionen (z. B. Cyber-Koordination) vorgesehen. Die Einbindung übergeordneter politischer Instanzen unterstreicht die erhöhte Sensibilität sicherheitsrelevanter IT-Entscheide im Kontext von Blaulichtorganisationen.
- Schutzzielorientierte Risikoexposition:
  - Verfügbarkeit: Wird als vorrangiges Schutzziel eingestuft, da Systemausfälle unmittelbare Auswirkungen die Erbringung kritischer kantonaler Aufgaben haben können. Entsprechend bestehen erhöhte Anforderungen an Resilienz, Notfallfähigkeit und Backup-Konzepte, wobei insbesondere die Datensicherung ausserhalb der Cloud als laufender Entwicklungspunkt genannt wird.
  - Vertraulichkeit: Die Schlüsselkontrolle durch externe Anbieter wird als technologieimmanentes Faktum eingeordnet. Ein potenzieller unberechtigter Zugriff durch den Anbieter oder auf dessen Veranlassung kann nicht vollständig ausgeschlossen werden, ist aber durch vertragliche Absicherungen hinreichend und glaubhaft abgesichert.

- Drittlandzugriffe: Extraterritoriale Zugriffsbefugnisse werden als systemisches Risiko verstanden, welches durch die konsequente Anwendung technischer und organisatorischer Massnahmen (TOM) auf ein akzeptables Mass reduziert werden kann.
- Vendor Lock-in: Die Abhängigkeit vom Anbieter wird als erheblich eingeschätzt und betrifft sowohl funktionale als auch sicherheitsrelevante Komponenten. Gleichzeitig wird anerkannt, dass die enge Integration Effizienz- und Sicherheitsvorteile mit sich bringt.
- Bewertung von Handlungsoptionen: Allfällige Alternativen zu M365 werden anhand klar definierter Kriterien beurteilt. Im Vordergrund stehen funktionale Gleichwertigkeit, Integrationsfähigkeit in bestehende Sicherheitsarchitekturen, Anforderungen an Krisenbetrieb und Resilienz sowie die rechtliche Einordnung der Hosting-Lokation.

Zusammenfassend erfolgt die Nutzung von M365 in der Untersuchungseinheit 1 in einem Spannungsfeld zwischen regulatorischen Anforderungen, operativer Leistungsfähigkeit und strategischer Abhängigkeit. Die identifizierten Restrisiken, insbesondere im Hinblick auf Datenhoheit und potenzielle Drittlandzugriffe, werden im Rahmen des bestehenden ISDS-Ansatzes aktiv adressiert, können jedoch systembedingt nicht vollständig eliminiert werden.

3.5.2.4 Finanzielle Ist-Situation

Untersuchungseinheit 1 verfügt über eine umfassende Kostentransparenz, die weit über reine Lizenzgebühren hinausgeht. Die vorliegenden Daten verdeutlichen dabei jene finanziellen Schwerpunkte, die direkt dem M365-Ökosystem zuzuordnen sind und bei einer allfälligen Migration auf ein Alternativprodukt unmittelbar zur Disposition stünden.

Zum Schutz der Vertraulichkeit wir die Nennung von absoluten Finanzzahlen vermieden. Der Fokus liegt stattdessen auf aggregierte Ergebnisse und Tendenzen, diese machen die wirtschaftlichen Zusammenhänge ebenso deutlich.

Position	Anteil der Kosten
Lizenzkosten	64 %
Engineering-Kosten	23 %
Externes Spezialwissen	7 %
Backup-Lösung	6 %

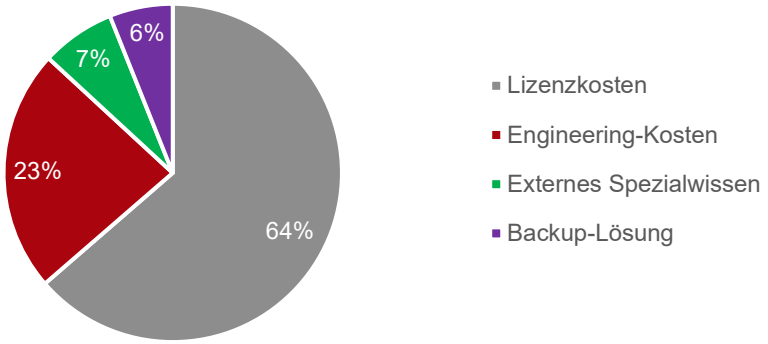


Abbildung 10: Kostenverteilung jener Kosten der Untersuchungseinheit 1, die einen direkten Bezug zu M365 haben

- Dominanz der direkten Lizenzkosten: Die Basis bilden die M365-Abonnements (insb. E5-Komponenten), deren jährliches Gesamtvolumen sich für eine Organisation dieser Grösse in einem niedrigen einstelligen Millionenbereich bewegt. Pro intern, angestellter Person (d.h. ohne Externe) entspricht dies einer monatlichen Kosten in der Grössenordnung von 50 CHF.
- Signifikanter interner Betriebsaufwand: Hinter den Lizenzkosten steht ein erheblicher personeller Aufwand durch verschiedene Engineering Teams. Diese verantworten u.a. die Konfiguration des Identitätsmanagements (Entra ID), die Absicherung der Endgeräte (Intune), die automatisierte Softwareverteilung und Paketierung sowie die Bereitstellung von Email- und Kollaborationslösungen (UCC).
- Daten- und Sicherheitsinvestitionen: Mit einem verwalteten Datenvolumen von insgesamt rund 96 Terabyte (verteilt auf Exchange, SharePoint und OneDrive) entstehen signifikante Aufwände für Speicher-Governance und die regulatorisch geforderte Archivierung.
- Ergänzende Expertise und Outtasking: Über den Eigenbetrieb hinaus nutzt Untersuchungseinheit 1 ein Budget im mittleren sechsstelligen Bereich für spezialisiertes „Expert-on-Call“-Wissen. Während knapp 40 % dieser Mittel die spezifische M365-Betriebsunterstützung absichern, fliessen die verbleibenden Aufwendungen primär in das Outtasking der Telefonie-Infrastruktur.

Die heutige Standardisierung auf Microsoft wirkt wie ein „unsichtbares“ Investitionsgut. Wissensaufbau und -management ist über die Jahre historisch erbracht, eingespielte Arbeitsabläufe basieren auf Microsoft.
Ein allfälliger Wechsel weg von diesem Produkt würde beträchtliche, bislang nicht monetarisierte Change-Management-Kosten nach sich ziehen (Schulung, Prozessanpassungen, Produktivitätsverluste).

3.5.2.5 Technische Soll-Analyse

Die technische Soll-Analyse der Untersuchungseinheit 1 zeigt mögliche technische Auswirkungen eines Wechsels von M365 zu openDesk auf. Die Analyse basiert auf Experteneinschätzungen, wobei subjektive Bewertungen unvermeidbar sind. Die Ergebnisse sind daher als Expertenmeinung zu potenziellen technischen Veränderungen zu verstehen.

Daten

Die Migration von M365 auf openDesk bringt aus datentechnischer Sicht Herausforderungen mit sich. In der untersuchten Organisation liegt ein beträchtlicher Anteil der bestehenden Daten und Dokumente in proprietären Office-Formaten (z. B. .docx, .xlsx, .pptx). Zudem sind diverse Excel-Makros und VBA-Skripte im Einsatz. Herausforderungen bei der Datenmigration werden insbesondere in folgenden Bereichen erwartet:

- SharePoint-Metadaten und Workflows: Die Migration von SharePoint-Inhalten, insbesondere von Metadaten und Workflows, stellt eine relevante Hürde dar. Metadatenstrukturen und Workflow-Definitionen sind spezifisch auf SharePoint abgestimmt und lassen sich nicht direkt auf openDesk übertragen. Daher sind eine Analyse, Anpassung und ggf. der Neuaufbau dieser Strukturen im Zielsystem erforderlich.
- Dateiberechtigungen und Verknüpfungen: Bestehende Dateiberechtigungen sind häufig komplex und über mehrere Ebenen hinweg angelegt, oftmals mit spezifischen Metadaten verknüpft. Die Migration erfordert individuelle Anpassungen. Ein vollständiger Neuaufbau der Berechtigungskonstrukte kann erforderlich werden, um die Zugriffssicherheit und Nachvollziehbarkeit im Zielsystem zu gewährleisten.
- Datenbanken (MS Access): Die Organisation nutzt weiterhin lokale MS-Access-Datenbanken. Da openDesk hierfür keine direkte Alternative bietet, müssen entweder die Anwendungen durch Drittanbieter-Lösungen ersetzt oder auf eine andere Plattform migriert werden, was zusätzliche Anpassungs- und Entwicklungsaufwände nach sich zieht.

.

Die Migration der Daten von M365 auf openDesk erfordert insbesondere bei SharePoint Metadaten, Berechtigungsstrukturen, und Datenbanken einen potenziell erhöhten Anpassungs- und Umstellungsaufwand.

Funktionsumfang

Im Falle einer Migration von M365 auf openDesk werden folgende funktionale Einschränkungen als besonders relevant erachtet:

- Security und Compliance: Sicherheits- und Compliance-relevante Funktionalitäten wie Microsoft Sentinel, Purview, PIM/Conditional Access und Defender sind im Open-Source-Bereich nur mit eingeschränkter Funktionalität oder durch Kombination mehrerer Dritttools abbildbar. Die Erreichung eines vergleichbaren Security- und Compliance-Standard ist mit erheblichem zusätzlichem Implementierungs- und Betriebsaufwand verbunden.
- Business Intelligence: Da die Untersuchungseinheit 1 die Datenanalyse und Visualisierungsfunktionen von M365 umfangreich einsetzt und openDesk diese Funktionalität

nicht abdeckt, würde eine Umstellung auf openDesk eine Drittanbieter Lösung erforderlich machen. Aufgrund der hohen Anzahl eingesetzter Dashboards und der engen Verzahnung mit Geschäftsprozessen wird von erheblichem Aufwand für eine Umstellung ausgegangen.
- Externe Kommunikation und Zusammenarbeit: Beim Austausch von Dokumenten und Dateiablagen mit externen Partnern (z. B. Bund, Justiz, Behörden) ist mit Anpassungsbedarf zu rechnen hinsichtlich Zugriffs- und Authentifizierungsmechanismen, Rechteverwaltung und Kompatibilität.

Insgesamt bietet openDesk grundlegende relevante Funktionen für die digitale Kollaboration. Um jedoch den gleichen funktionalen und nicht-funktionalen Standard wie bei M365 bezüglich Sicherheit und Compliance Funktionen und Business Itelligence Funktionen zu gewährleisten, werden zusätzliche Drittanbieter Produkte und möglicherweise angepass-te Lösungen benötigt.

Integrationen
Eine Migration von M365 auf openDesk würde umfangreiche Anpassungen erfordern, da die untersuchte Organisation eine Vielzahl angebundener Fachapplikationen und Schnittstellen betreibt

- Microsoft Graph API als zentrale Schnittstelle: Über 50 Fachanwendungen sind über die Graph API angebunden. Ein unmittelbarer Ersatz für die Graph API in openDesk ist nicht vorhanden. Individuelle Adapterlösungen und umfangreiche Anpassungen wären erforderlich, um eine vergleichbare Integrationstiefe zu erreichen.
- Identity & Access Management: Eine Umstellung auf openDesk würde bedeuten, dass Authentifizierungsmechanismen (2FA, etc.) und Berechtigungen neu aufgebaut, bestehende Workflows angepasst und Schnittstellen, insbesondere zu externen Behörden oder Institutionen, neu konzipiert werden müssen.
- Mobile Device Management und Endgeräte: openDesk enthält kein natives MDM (Mobile Device Management) oder MAM (Mobile Application Management). MDM/MAM-Funktionalitäten müssen durch eine Drittanbieterlösung abgedeckt werden, wobei offen ist ob relevante Funktionalitäten im gleichen Umfang vorhanden sind (bspw. Revokationen, etc.). Zudem müssten relevante Sicherheitskonzepte für den Export und Zugriff auf Daten von privaten Geräten komplett überarbeitet werden.

Eine Migration auf openDesk erfordert umfangreiche Anpassungen an bestehenden Schnittstellen, Authentifizierungs- und Sicherheitskonzepten. Aufwand und Komplexität sind dabei insbesondere durch den Wechsel von Microsoft-spezifischen Standards auf Open-Source-Komponenten bestimmt.

3.5.2.6 Organisatorische Soll-Analyse

Die organisatorische Soll-Analyse für Untersuchungseinheit 1 zeigt die strukturellen Veränderungen auf, die ein Wechsel von M365 zu openDesk mit sich bringen würde. Die Analyse basiert auf systematischen Bewertungen der Experten. Es ist anzumerken, dass subjektive Einschätzungen der befragten Experten in die Bewertungen einfliessen. Die Ergebnisse sind daher als Experteneinschätzung zu verstehen, die wichtige Erkenntnisse über potenzielle organisatorische Veränderungen liefert.

Die wesentlichen Punkte sind:

- Transformation der IT-Rolle: Da openDesk nicht die umfassende Integration von M365 bietet, müssen ergänzende Produkte (z. B. Security-Layer) separat beschafft und integriert werden. Dies bedeutet die Orchestrierung mehrerer Anbieter zu einer funktionsfähigen Gesamtlösung. Die Rolle der IT-Organisation verändert sich somit. Während heute eine effiziente Konsumentenrolle gegenüber Microsoft eingenommen wird, erfordert openDesk verstärkt die Rolle eines Service-Integrators.
- Kompetenzaufbau Wissenstransfer: Die Organisation steht vor der Herausforderung, neue Fähigkeiten aufzubauen. OpenDesk-Expertise und Open-Source-Kompetenzen sind heute praktisch nicht vorhanden und müssten entwickelt werden. Gleichzeitig würde das über Jahre aufgebaute Microsoft-spezifische Wissen an strategischem Wert verlieren. Die Experten bewerten den aktuellen Wissensstand bei M365 als "institutionalisiert", während bei openDesk das "Wissen primär bei externen Beratern liegt" und "interner Kompetenzaufbau zwingend" ist, da sonst zusätzliche Risiken und Abhängigkeiten entstehen.
- Multi-Vendor-Management und Verantwortungsabgrenzung: Die heutigen schlanken Governance-Prozesse müssten durch komplexere Multi-Vendor-Strukturen ersetzt werden. Statt einer zentralen Ansprechstelle entstehen verschiedene Verantwortlichkeiten: Hosting-Vertrag, ZenDiS-Vertrag sowie separate Verträge für fehlende Komponenten. Das openDesk-Modell verfügt zwar über eine definierte Verantwortungsstruktur, ist jedoch "noch nicht in dem Masse etabliert und standardisiert, wie es bei Microsoft der Fall ist".
- Einflussmöglichkeit auf die Produktentwicklung: OpenDesk ermöglicht durch seine Open-Source-Basis aktivere Mitgestaltung über Community und User-Groups, während bei M365 die Roadmap vollständig von Microsoft diktiert wird. OpenDesk bündelt zudem Änderungen in planbare, monatliche Releases mit definierten Wartungsfenstern, was mehr Kontrolle bietet.
- Betriebsmodell-Anpassungen: Die Integration erfordert nur moderate Anpassungen des IT-Betriebsmodells. Während grundlegende Rollen bestehen bleiben können, entstehen neue Vernetzungen und Abhängigkeiten. Der Ersatz von Microsoft Purview durch alternative Data-Loss-Prevention-Lösungen erfordert beispielsweise völlig neue Betriebsprozesse.
- Release-Management und Produktentwicklung: Während M365 durch Microsofts massive Investitionen in Qualitätssicherung weitgehend automatisierte Updates ermöglicht, erfordert openDesk höheren internen Aufwand. Die Experten erwarten mehr Testing, da Microsoft "deutlich grössere Investitionen in die Qualitätssicherung fliessen lassen kann". Zu berücksichtigen ist zudem die Möglichkeit des Forking: Die Open-Source-Basis erlaubt es zwar, von der offiziellen Entwicklungslinie abzuweichen und eigene Anpassungen

vorzunehmen, doch ist deren Tragweite nicht zu unterschätzen. Eine eigenständige Fortführung abgezweigter Versionen bindet interne Ressourcen dauerhaft, erschwert die Übernahme künftiger Releases und kann neue Abhängigkeiten schaffen.

- Standardisierung und interkantonale Zusammenarbeit: Kritisch ist die Standardisierungsfrage: Ohne koordinierte Einführung besteht "hohes Risiko der Fragmentierung". Etablierte Funktionen wie die Federation von Berechtigungen zwischen Kantonen wären "nicht mehr so einfach umsetzbar". Bei M365 sorgt der Vendor automatisch für einheitliche Standards zwischen den Kantonen. Positiv ist jedoch, dass openDesk durch seine offene Architektur grundsätzlich bessere Möglichkeiten für standardisierte, interoperable Lösungen bietet - allerdings erfordert dies eine koordinierte Herangehensweise und entsprechende Governance-Strukturen.
- Compliance und Souveränität: OpenDesk bietet bessere Compliance-Möglichkeiten durch die Möglichkeit eines sehr individuellen Schweizer Hostings und Open-Source-Basis, was volle Souveränität "out of the box" ermöglichen kann. Die befragten Experten ergänzen jedoch: "Es ist aktuell unklar, welche Standards ein neuer Hoster tatsächlich erfüllen würde" und "Egal wo es gehostet wird, hat man ein Risiko."
- Exit-Strategien und Vendor Lock-in: Trotz theoretisch besserer Exit-Optionen durch Open-Source-Basis entstehen neue Abhängigkeiten. Die Experten betonen, dass "ein Wechsel von openDesk zu einer anderen Lösung ebenfalls mit erheblichem Aufwand verbunden wäre" - man befände sich lediglich in einem anderen Lock-in. Positiv ist jedoch die grundsätzlich höhere Flexibilität durch die modulare Architektur und offenen Standards, die es ermöglicht, einzelne Komponenten auszutauschen, auch wenn ein kompletter Systemwechsel weiterhin aufwändig bliebe. Allerdings ist auch bereits der theoretisch mögliche Tausch von Komponenten in wenig realistisch (Forking; Release-Management, Abhängigkeiten, Testing) und im Lichte eines Suite-Ansatzes wenig attraktiv.
- Unveränderte Aspekte: Bestimmte organisatorische Bereiche würden sich kaum verändern: Die grundlegenden Service-Management-Strukturen, Projektmanagement-Prozesse und die schlussendliche Grösse des Engineering-Teams bleiben nach Experteneinschätzung weitgehend konstant, nachdem der Parallelbetrieb abgeschlossen ist. Auch die Anforderungen an Backup und Disaster Recovery sowie die grundsätzlichen Sicherheitsanforderungen unterscheiden sich nicht wesentlich zwischen den Plattformen.
- Strategische Bereitschaft: Die IT-Organisation signalisiert grundsätzliche Bereitschaft für einen Wechsel: "Der Support wäre durchaus vorhanden, wenn es eine echte 1:1-Alternative gäbe, die nicht so viel Impact hätte." Die Experten betonen, dass die IT die Umsetzung selbstverständlich angehen würden, "wenn sie den entsprechenden politischen Auftrag und das notwendige Budget und Personal erhielte."

Während openDesk Vorteile bei Einflussmöglichkeiten und theoretischer Souveränität bietet, erfordert es erhebliche Investitionen in neue Kompetenzen und komplexere Governance-Strukturen. Die Organisation ist grundsätzlich bereit für diese

Transformation, sofern die politischen, personellen und finanziellen Rahmenbedingungen geschaffen werden.

3.5.2.7 Finanzielle Soll-Analyse

Die finanzielle Soll-Analyse für die Untersuchungseinheit betrachtet die potenziellen Kostenwirkungen eines Wechsels von der heute etablierten M365-Plattform hin zur OSS-basierten Suite openDesk. Eine exakte Bestimmung der Soll-Finanzen ist ohne konkrete Offerten, verbindliche Leistungsdefinitionen und detaillierte Lastenhefte nicht möglich. Die nachfolgenden Angaben beruhen auf einem strukturierten, am in Kapitel 3 beschriebenen Kostenmodell ausgerichteten Vorgehen. Die wesentlichen Kostenblöcke eines möglichen openDesk-Szenarios wurden gemeinsam mit Fachpersonen der Untersuchungseinheit 1 entlang der Kategorien Lizenzen, Hosting, Security, Betrieb, Migration, Anpassungen, Schulung und Adoption durchgearbeitet und plausibilisiert.

Aus Vertraulichkeits- und Darstellungsgründen werden in der Studie nicht sämtliche Rechenannahmen, Einzelpositionen und internen Herleitungen im Detail ausgewiesen. Stattdessen werden aggregierte Ergebnisse, Grössenordnungen und Kostentendenzen dargestellt. Die ausgewiesenen Werte sind daher als indikative, gemeinsam validierte Schätzungen zu verstehen; sie stellen keine verbindliche Kalkulationsgrundlage dar und können je nach Organisation, Zielbild und Vertragsgestaltung erheblich variieren.

Wiederkehrende Kosten

Unter diesen Vorbehalten zeigte eine grobe Kostenanalyse mit den befragten Experten, dass sich die Gesamtkosten pro Jahr einer Alternative wie openDesk tendenziell in einem ähnlichen Rahmen bewegen wie die heutige M365-Lösung.

Lizenzkosten-Einsparung: Der direkte Vergleich der Lizenzkosten zeigt zunächst einen deutlichen Vorteil für die Open-Source-Alternative: Während Microsoft E5 Lizenzen bei ca. CHF 47.50 pro User und Monat liegen (entspricht bei 5'800 Lizenzen rund 3.3 Millionen CHF jährlich), wird die openDesk SaaS-Lösung mit etwa 18 Euro pro User und Jahr kalkuliert (entspricht ca. 1.15 Millionen CHF). Dies würde theoretisch zu jährlichen Einsparungen von über 2 Millionen CHF bei den direkten Lizenzkosten führen.

Unsicherheiten bei der Preisgestaltung: Die aktuellen Lizenzpreise basieren auf Angaben der ZenDiS zu ihrem SaaS-Produkt, gehostet in Deutschland. Die genannten 18 Euro (Stand April 2026) beinhalten sowohl Hosting als auch Lizenzen und gelten für 500+ User bei einer Mindestdauer von 12 Monaten. Würde man sich nur für die Lizenz entscheiden und das Hosting selbst übernehmen, läge der Preis bei 15 Euro pro User und Jahr. Eine einfache Schlussfolgerung, dass die Differenz von 3 Euro (18-15 Euro) den reinen Hosting-Kosten entspricht, wäre nicht zulässig, da keine Einsicht in die Verträge zwischen ZenDiS und deren beauftragten Hostern besteht.

Hosting-Kosten in der Schweiz: Verbindliche Angaben zu openDesk Hosting-Preisen in der Schweiz (und somit für ein openDesk SaaS Schweiz-Lösung) existieren zum Zeitpunkt der Studie (April 2026) nicht. In ersten informellen Marktrückmeldungen wurde deutlich, dass die Hosting-Kosten in der Schweiz voraussichtlich ein Mehrfaches der in Deutschland üblichen Werte betragen dürften. Konkrete Preisindikationen konnten für den spezifischen Umfang von 5'800 Usern der Untersuchungseinheit 1 nicht gemacht werden. Bei grösseren Organisationen wären grundsätzlich günstigere Konditionen zu erwarten als bei kleineren Einheiten. Zum Zeitpunkt der Redaktion dieser Studie laufen die Verhandlungen mit dem ZenDis und diversen Schweizer Dienstleistern. Perspektivisch ist von deutlich tieferen Werten auszugehen.

Diese Einschätzung deckt sich mit der allgemeinen Marktbeobachtung, wonach Hosting-Leistungen in der Schweiz aufgrund höherer Lohn-, Energie- und Infrastrukturkosten teurer ausfallen als in Deutschland. Die rechnerische Differenz von 3 Euro aus dem deutschen ZenDiS-Modell (18 Euro SaaS abzüglich 15 Euro Enterprise-Lizenz) kann daher nicht unmittelbar als Referenzwert für ein Schweizer Hosting herangezogen werden.

Die aktuelle technische Umgebung für den Betrieb von openDesk unterliegt einer gewissen Komplexität mit circa 80 Pods für den Betrieb einer Umgebung. Das deutsche SaaS-Angebot wird auf einer auf grösseres Volumen optimierte Infrastruktur u.a. des Cloud-Providers STACKIT (Schwarz Digits) betrieben. Schweizer Anbieter betreiben demgegenüber, mangels aktueller Mandantenfähigkeit von openDesk, pro Kunde eine separate Instanz. Dieser strukturelle Unterschied ist ein wesentlicher Treiber der erwarteten Mehrkosten in der Schweiz.
Die Möglichkeit das Produkt zukünftig mandantenfähig zu betreiben, wird für Schweizer Hosting-Anbieter einen erheblichen Effizienzeffekt erzeugen und für den Kunden einen extremen Preisvorteil ergeben. Die wichtigste technische Ursache der Schweizer Mehrkosten ist die zum Zeitpunkt der Studie fehlende Multi-Tenancy von openDesk. Ein Schweizer Hoster muss für 30 Mitarbeitende denselben Aufbau betreiben, wie für 300. Mit der geplanten Einführung der Mandantenfähigkeit dürfte sich dieser Kostenfaktor für Schweizer Hoster deutlich reduzieren.[6]

Preisvergleiche hängen stark davon ab, was genau verglichen wird. Die konkrete Ausgestaltung ist stets abhängig von der spezifischen Vertragsgestaltung und deren Verhandlung, wodurch sich erhebliche Abweichungen ergeben können.

Exemplarische Kostenberechnung
Die openDesk-Lizenzpreise basieren auf Angaben von ZenDiS (Stand Mai 2026). Die Vergleichswerte zu Microsoft E5 stammen von Untersuchungspartner 1. Die Hosting-Preise für die Schweiz sind fiktiv und aus dem ZenDiS-Modell abgeleitet. Als Hosting-Standort wird die Schweiz angenommen, da die Untersuchungspartner und ihre Dienstleister dort ansässig sind. Eine Evaluation des Hosting-Standorts war nicht Gegenstand dieser Untersuchung.

[6] Hersel, R. (2026): Serie: openDesk ausprobiert – Teil 7 – Fazit. GNU/Linux.ch, URL: Serie: openDesk ausprobiert - Teil 7 - Fazit - GNU/Linux.ch, abgerufen am 14. August 2026.

Zur Illustration der Grössenordnungen wird nachfolgend mit diesen fiktiven, aus dem ZenDiS-Modell abgeleiteten Hosting-Preisen gerechnet:

- Untergrenze: CHF 5 pro User und Monat (Schweiz), in etwa der rechnerischen Differenz zum deutschen SaaS-Angebot entsprechend
- Obergrenze: rund CHF 14 pro User und Monat (Schweiz), rund entsprechend dem openDesk-Lizenzpreis selbst

Für die nachfolgende Beispielrechnung wird exemplarisch ein Hosting-Preis von CHF 10 pro User und Monat verwendet, ausschliesslich zur Illustration und ohne Anspruch auf Marktrelevanz. Da sich der Markt in einer dynamischen Entwicklungsphase befindet und die Preisgestaltung stark von Volumen, Vertragsdauer und individueller Ausgestaltung abhängt, ersetzt diese Studie keine organisationsspezifische Offertenphase.

Beispielrechnung (5'800 User)

Bei einem fiktiven Hosting-Preis von 10 CHF pro User und Monat ergäbe sich folgendes Kostenbild:

- openDesk-Lizenzen (Enterprise): ca. 960'000 CHF/Jahr (ca. CHF 14 pro User und Monat × 5'800 User)
- Hosting (Schweiz, fiktiv): ca. 696'000 CHF/Jahr (CHF 10 pro User und Monat × 5'800 User)
- Total Lizenz- und Hosting-Kosten: ca. 1.66 Mio. CHF/Jahr
- Theoretische Einsparung gegenüber Microsoft E5: rund 1.65 Mio. CHF/Jahr

Lösung	Lizenz (CHF)	Hosting (CHF)	Total (CHF)
Microsoft E5	47.50	Inkludiert	47.50
openDesk (Enterprise)	14	(exkl.)	14
openDesk (Enterprise, inkl. Hosting)[7]	14	10.00	23.80
openDesk (SaaS)	16.60	Inkludiert	16.60

Tabelle 10: Kosten für Lösung pro User im Monat im Vergleich

Neue Kostenpositionen: Der theoretischen Lizenz-Einsparung stehen neue Kostenpositionen gegenüber, die einen wesentlichen Teil der Einsparung wieder aufheben. Sie entstehen, weil openDesk nicht die integrierten Funktionen von M365 mitbringt und entsprechende Funktionalitäten durch separate Lösungen abgedeckt werden müssen. Die im Rahmen dieser Studie quantifizierten neuen Kostenblöcke umfassen:

- Security-Stack (ca. 1.25 Mio. CHF/Jahr): Mobile Device Management (MDM), Endpoint Protection, Data Loss Prevention sowie Identity- und Access-Management-Komponenten als Ersatz für die integrierten Microsoft-Sicherheitsfunktionen
- Mobile Arbeitsplätze (ca. 148'000 CHF/Jahr): Investitionen in VPN-Infrastruktur und sichere Zugriffslösungen, da openDesk nicht die nativen HTTPS-Zugriffsmöglichkeiten von M365 bietet

Die beiden Positionen summieren sich auf rund 1.4 Mio. CHF/Jahr und stehen einer Lizenzeinsparung von rund 1.6 Mio. CHF/Jahr gegenüber. Rechnerisch verbleibt daraus ein rechnerischer Nettoeffekt in der Grössenordnung von wenigen hunderttausend CHF pro Jahr, der angesichts der Schätzunsicherheiten sowohl der Lizenz- wie der Security-Stack-Kosten als innerhalb der Bandbreite der Schätzgenauigkeit liegend einzuordnen ist. Durch die nachfolgend genannten, nicht quantifizierten Kostenblöcke wird dieser Wert voraussichtlich weiter reduziert oder vollständig aufgehoben.

- Ersatz für die Power Platform: Low-Code-, Automatisierungs- und Workflow-Funktionalitäten (Power Automate, Power Apps) sind in openDesk nicht in vergleichbarer Form vorhanden.

[7] Hosting-Preis (CHF 10) exemplarisch gemäss Beispielrechnung, ohne Anspruch auf Marktrelevanz.

- Ersatz für Microsoft Graph API und ergänzende Integrationsdienste: Die heute über die Graph API und weitere Microsoft-spezifische Schnittstellen realisierten Integrationen müssten in einer openDesk-Umgebung über offene Standards und individuelle Adapter neu aufgebaut werden.

Die beiden zuletzt genannten Kostenpositionen wurden im Rahmen dieser Studie bewusst nicht monetär quantifiziert, da eine belastbare Bezifferung eine detaillierte Analyse des heutigen Nutzungsumfangs sowie eine konkrete Zielarchitektur voraussetzt. Sie sind jedoch als weitere, potenziell relevante Kostenblöcke bei einer Gesamtbewertung explizit zu berücksichtigen. Diese zusätzlichen Kostenpositionen entstehen, weil integrierte Funktionalitäten von M365 im Alternativszenario durch mehrere separate Lösungen ersetzt bzw. ergänzt werden müssen. Dies erhöht den Aufwand für Integration, Abstimmung und Betrieb und kann damit zu höheren laufenden Kosten führen, auch wenn ein solcher Ansatz gleichzeitig grössere Flexibilität bei der Ausgestaltung einzelner Komponenten ermöglichen kann.

Unveränderte Kostenpositionen: Bestimmte Kostenpositionen bleiben nach Experteneinschätzung weitgehend unverändert: Das Engineering-Team wird langfristig voraussichtlich in ähnlicher Grösse bestehen bleiben, da der Wegfall von Microsoft-spezifischen Aufgaben durch neue Integrations- und Betriebsarbeiten kompensiert wird. Zu berücksichtigen ist dabei, dass sich die Rollenprofile und Kompetenzanforderungen verändern. Die Auswirkungen dieser veränderten Anforderungen auf die Personalkosten pro Kopf sind im Rahmen dieser finanziellen Analyse nicht abschliessend beurteilbar: Je nach Marktverfügbarkeit der geforderten Profile, Lohnniveau und Weiterbildungsbedarf können sich sowohl höhere als auch tiefere Kosten ergeben. Eine belastbare Einschätzung wäre in einer detaillierten Umsetzungsplanung zu vertiefen.

Ebenso wird der Bedarf an externer Expertise auf einem ähnlichen Niveau erwartet. Bereits heute anfallende Kosten für Backup und Disaster Recovery bleiben in der Grössenordnung von rund 300'000 CHF pro Jahr bestehen, da auch alternative Lösungen entsprechende Datensicherungsanforderungen haben.

Zu berücksichtigen ist zudem, dass ein Wechsel weg von den M365-Kernkomponenten nicht automatisch alle Microsoft-Abhängigkeiten beseitigt: Funktionen, die heute innerhalb der E5-Lizenz mitgenutzt werden (z. B. Teile des Identity- und Endpoint-Managements), müssten bei einer selektiven Ablösung neu bzw. anders lizenziert werden, typischerweise über Standalone-Lizenzen deren Preis-Leistungs-Verhältnis erfahrungsgemäss deutlich ungünstiger ausfällt als im gebündelten E5-Paket, sodass die realisierbare Netto-Einsparung bei einer selektiven Ablösung geringer ausfallen kann als bei einem vollständigen Wechsel.

Drei zentrale Unsicherheitsfaktoren beeinflussen die Gesamtkostenbewertung erheblich:

1. Dynamik der Lizenzpreise: Die Preisgestaltung für openDesk befindet sich noch in einer dynamischen Entwicklungsphase. Sowohl die Lizenz- als auch die Hosting-Komponenten

unterliegen technischen Optimierungen und Skalierungseffekten, die zu erheblichen Preisveränderungen führen können.
2. Hosting-Kosten als Schlüsselkomponente: Die Kosten für Hosting in der Schweiz sind zum Zeitpunkt der Studie nicht verbindlich verfügbar. Diese Komponente hat direkten Einfluss auf die Gesamtwirtschaftlichkeit der Alternative.
3. Ersatzprodukte als Kostentreiber: Die zu beschaffenden Ersatzprodukte für die wegfallenden integrierten M365-Funktionalitäten beeinflussen den jährlichen Preis massgeblich. Je nach gewähltem Sicherheitsniveau und spezifischen Anforderungen können diese Kosten erheblich von den geschätzten Werten abweichen.

Einmalige Kosten
Neben den laufenden Kosten entstehen bei einem Wechsel zu openDesk erhebliche einmalige Transformationskosten, die sich auf mehrere Millionen CHF belaufen. Diese Investitionen sind erforderlich, um die bestehende M365-Umgebung vollständig auf die neue Plattform zu migrieren und die Organisation auf die veränderten Arbeitsabläufe vorzubereiten.

Die wesentlichen einmaligen Kostenblöcke umfassen:

- Anpassungskosten (ca. 5.65 Mio. CHF): Das Umschreiben von Fachanwendungen mit M365-Schnittstellen sowie die Anpassung von Dokumentenformaten stellen den grössten Einzelposten dar. Diese Schätzung basiert auf groben Kalkulationen ohne detaillierte Einzelbewertung - durchschnittlich werden ca. 70'000 CHF pro Applikation angenommen, zusätzlich entstehen Kosten für die Formatanpassung bei grossen Verwaltungsanwendungen. Die tatsächlichen Anpassungskosten sind jedoch ohne genaue Analyse jeder einzelnen Applikation nicht exakt bestimmbar und können je nach Komplexität der Anwendungen erheblich variieren.
  Diese Anpassungs- resp. Migrationskosten sind stark abhängig davon, was genau migriert wird. Wie aus dem technischen Abschnitt erläutert, können bestimmte Komponenten gar nicht migriert werden, andere sind möglicherweise nicht sinnvoll zu übertragen.
- Schulung & Adoption (ca. 18.37 Mio. CHF): Diese Position umfasst die direkten Schulungskosten; also die Kursteilnahme der Verwaltungsmitarbeitenden und den damit verbundenen, kalkulierten Produktionsausfall (5'500 Mitarbeitenden, 5 Tage à 650 CHF). Zusätzlich sind Projektkosten für diese Einarbeitung, Change und Schulung enthalten.
- Externe Beratung und Validierung (ca. 1.85 Mio. CHF): Kosten für Architektur-Zertifizierung, Sicherheitsaudits und Implementierungsunterstützung durch externe Spezialisten.
- Doppelspurigkeiten während der Transformationsphase: Ferner ist zu betrachten, dass während einer geschätzten Einführungszeit von 4-8 Jahren zusätzliche Kosten für notwendige Doppelspurigkeiten personeller (Engineering -und Support-Team) und technischer Natur (Lizenzen, Systeme) entstehen, da sowohl die bestehende M365-Umgebung weiterhin betrieben als auch die neue openDesk-Plattform aufgebaut und stabilisiert werden muss.

  Diese Parallelführung führt zu erhöhten Personalkosten im Engineering-Bereich, da Kompetenzen für beide Plattformen vorgehalten werden müssen. Zusätzlich entstehen

Lizenzkosten für beide Systeme während der Migrationsphase, was die Gesamtkosten der Transformation weiter erhöht. Eine genaue Quantifizierung dieser Doppelspurigkeit ist ohne detaillierte Migrationsplanung nicht möglich. Als Indikation beziffern wir die laufenden Kosten für einen Zeitraum von 6 Jahren.

- Produktivitätsverluste: Zusätzlich und nachträglich zu den direkten Transformationskosten ist mit erheblichen Produktivitätsverlusten zu rechnen, die durch Formatierungsfehler oder Kompatibilitätsprobleme mit externen Marktpartnern entstehen. Diese werden auf etwa 4 Tage Arbeitsausfall pro Mitarbeiter im ersten Jahr und 2 Tage im zweiten Jahr geschätzt, was einem kalkulatorischen Verlust von über 21 Millionen CHF entspricht. Diese indirekten Kosten sind schwer quantifizierbar, stellen aber einen wesentlichen Faktor bei der Gesamtbewertung dar.

Zur Vermeidung von Doppelzählungen werden zwei zeitlich und inhaltlich unterschiedliche Effekte getrennt ausgewiesen: Die Schulungs- und Adoptionskosten beinhalten die Arbeitszeit, in der Mitarbeitende während der Schulungsphase in Kursen gebunden sind und ihren regulären Aufgaben nicht nachgehen können. Die Produktivitätsverluste erfassen demgegenüber den nachgelagerten Effekt nach Abschluss der Schulung: die Phase verminderter Arbeitsgeschwindigkeit, in der eingespielte Routinen neu erlernt, Funktionen gesucht und Kompatibilitätsprobleme behoben werden müssen. Beide Blöcke sind additiv zu verstehen und überschneiden sich nicht.

Gesamte einmalige Kosten: Die Transformations-Projektkosten belaufen sich auf geschätzte 25-30 Millionen CHF. Um diese Summe in Relation zu setzen: Sie entspricht etwa dem 7-9-fachen der jährlichen M365-Lizenz-Kosten von 3.3 Millionen CHF. Diese Investitionen sind unabhängig von den potentiellen, laufenden Kosteneinsparungen zu betrachten und müssten über einen sehr langen Zeitraum amortisiert werden.

Kostenkategorie	Betrag	Bemerkung
Anpassungskosten	5.65 MCHF	Fachanwendungen und Datenmigration
Schulung & Adoption	18.37 MCHF	Schulung und Adoption
Externe Beratung	1.85 MCHF	Architektur, Security und Governance
Direkte Projektkosten	25.87 MCHF	Summe der Projektkosten
Produktivitätsverlust	21.45 MCHF	Nicht kalkuliert in den Projektkosten
Doppelspurigkeit	30.66 MCHF	Parallelbetrieb der alten Lösung; nicht Teil der Projektkosten

Tabelle 11: Übersicht einmalige Kosten bei einem Wechsel der Untersuchungseinheit 1

Die Höhe dieser einmaligen Kosten unterstreicht, dass ein Wechsel zu openDesk primär eine strategische Entscheidung darstellt, die nicht durch kurzfristige Kosteneinsparungen motiviert werden kann.

3.5.3 Ergebnisse der Analyse Untersuchungseinheit 2

3.5.3.1 Technische Ist-Situation

Übersicht des eingesetzten M365 Funktionsumfangs:
Untersuchungseinheit 2 setzt M365 bereits sehr umfassend und zielgerichtet für die tägliche Arbeit der Angestellten der Verwaltung ein. Im Mittelpunkt steht die Unterstützung moderner Arbeitsformen, die Steigerung der Produktivität und die Einhaltung hoher Sicherheits- und Compliance-Standards. Die hohe Durchdringung der relevanten Kernfunktionen von M365 zeigt einen fortgeschrittenen Digitalisierungsgrad auf. Der Bereich Analytics und Automatisierung wird derzeit noch wenig genutzt, es gibt jedoch ein Pilot Projekt für künftige Nutzung von Power BI.

Die folgende Tabelle bewertet den Funktionsumfang der eingesetzten M365-Produkte in zentralen Themenbereichen anhand einer fünfstufigen Skala. Die Skala dient der Einordnung, wie umfassend und fortgeschritten die jeweiligen M365-Dienste bereits organisatorisch genutzt werden:

Stufe	Beschreibung
1	Nicht/nur sehr rudimentär genutzt
2	Einzelne Anwendungsfälle
3	Gelegentlicher Einsatz
4	Umfassender Einsatz, teilweise erweiterte Nutzung und Integration
5	Sehr umfassender und tief integrierter Einsatz im Regelbetrieb

Tabelle 12: Bewertungsstufen Nutzung von M365 Produkte

Die nachfolgende Analyse konzentriert sich auf die wichtigsten Dienste und Anwendungen von M365, die in der Verwaltung eine zentrale Rolle spielen. Im Fokus stehen hierbei insbesondere Dienste und Anwendungen wie Exchange Online, SharePoint Online oder Microsoft Teams. Weniger bedeutende Services, wie etwa Forms oder Clipchamp, bleiben im Rahmen dieser Betrachtung unberücksichtigt. Die nachfolgende Tabelle bietet einen kompakten Überblick über die aktuell im Einsatz befindlichen, zentralen M365-Komponenten und ordnet sie den jeweiligen Funktionsbereichen zu.

Funktionsbereich	Einstufung	Eingesetzte Dienste und Anwendungen
Kommunikation und Kollaboration	4	Teams Exchange Hybrid Outlook
Produktivitäts- und Geschäftsanwendungen	5	Excel Word PowerPoint
Datei- und Informationsmanagement	4	SharePoint Online SharePoint On-premise OneDrive

Sicherheit und Compliance	5	Defender for Endpoint Defender for Office 365 Defender for Server Defender for Identity Defender for Cloud Apps Sentinel Purview Intune (Mobile Device Management und Mobile Application Management)
Künstliche Intelligenz	2	Microsoft Copilot Chat wird eingesetzt Pilotprojekt für Microsoft Copilot
Betriebssystem	5	Windows 11 (64 Bit)
Identitäts- und Zugriffsmanagement	5	Entra ID Entra PIM Active Directory Windows Hello for Business Microsoft Authenticator
Analytics und Automatisierung	2	Pilotprojekt für Power BI

Tabelle 13: Analyse Nutzung M365 Untersuchungseinheit 2

Kommunikation und Kollaboration:

- Outlook: In der Verwaltung wird Exchange Hybrid eingesetzt. Derzeit läuft die Migration auf Exchange Online für die Endbenutzer-Mailboxen. Für den Versand sensitiver Informationen wird die integrierte Lösung SEPPMail eingesetzt. Die Mitarbeitenden nutzen überwiegend den Outlook-Desktop-Client für den E-Mail-Zugriff.
- Teams: Teams ist als Standardlösung im Einsatz zum Telefonieren und Chatten.

Produktivitäts- und Geschäftsanwendungen:

- Excel, Word, und PowerPoint: Die Angestellten der Verwaltung nutzen sowohl die Desktop-Version als auch die Web-Version der Standardanwendungen Excel, Word und PowerPoint im Rahmen von Office 365.

Datei- und Informationsmanagement:

- OneDrive: In der Verwaltung wird OneDrive von den Mitarbeitenden genutzt, wobei jedoch strikte Richtlinien vorgeben, welche Inhalte hochgeladen werden dürfen. Derzeit ist es nicht möglich, Dateien über OneDrive mit externen Personen zu teilen. Im Gegensatz dazu bietet Microsoft Teams eine Möglichkeit für externe Freigaben, allerdings ist hierfür ein interner Freigabeprozess vorgesehen.
- SharePoint: Zurzeit haben Nutzer weiterhin lokale Netzwerklaufwerke, wie etwa das Laufwerk P. Es ist jedoch geplant, diese durch SharePoint-Sites zu ersetzen. Hierzu läuft aktuell ein Projekt. Ein weiteres Ziel des Projekts ist es, die bestehenden lokalen SharePoint-Anwendungen schrittweise auf SharePoint Online zu migrieren. Anwendungen, wie beispielsweise das Gebäudemanagement, sind bereits teilweise in Migration. Das derzeitige Intranet basiert noch nicht auf SharePoint, es wird jedoch geprüft, auch diesen Bereich künftig auf SharePoint umzustellen. Aktuell wird geprüft, ob das Wissensmanagement mit

den Funktionen von SharePoint ausreichend abgebildet werden kann. Hinsichtlich SharePoint-Listen wird erwogen, die Erstellung persönlicher Listen durch Nutzer einzuschränken, um eine bessere Übersicht und Governance zu gewährleisten.

Sicherheit und Compliance:
- Defender: Defender ist sowohl im Server (Windows & Linux) als auch im Client-Bereich als Endpointschutz im Einsatz.
- Sentinel: Microsoft Sentinel wird als Security Information and Event Management (SIEM) Lösung eingesetzt für das Security Operations Center (SOC).
- Purview: Microsoft Purview wird für die Klassifizierung von Dokumenten mit Sensitivity Labels verwendet. Zudem werden DLP-Richtlinien angewendet, die beispielsweise verhindern, dass VERTRAULICHE oder GEHEIM klassifizierte Daten gemäss Informationsschutzverordnung (IschV) in die Cloud geladen oder an externe Empfänger versendet werden. Die Sensitivity Labels sind verpflichtend und das Standardlabel ist auf "Intern (Amtsgeheimnis)" gesetzt. Auch bei der Nutzung von Copilot wird sichergestellt, dass VERTRAULICHE oder GEHEIM klassifizierte Dokumente nicht ausgelesen werden können. Retention Labels werden aktuell noch nicht verwendet, da auf Vorgaben der Ämter gewartet wird.
- Intune: Microsoft Intune kommt insbesondere im Bereich Mobile Application Management (MAM) zum Einsatz. Für die Zukunft ist zudem die Einführung von Mobile Device Management (MDM) geplant.

Künstliche Intelligenz:
- Copilot: Die Nutzer haben Zugang zum Copilot Chat. Aktuell läuft ein Pilotprojekt, um zu prüfen, wie der Copilot zukünftig vollständig eingesetzt werden kann. Der produktive Einsatz erfolgt derzeit, abgesehen von wenigen Einzellizenzen, noch nicht. Copilot ist strategisch als fester Bestandteil vorgesehen und kann bei Bedarf bestellt werden.

Betriebssystem:
- Windows: Windows 11 wird in der 64-Bit-Version eingesetzt. Die Office-Anwendungen sind in der 64-Bit-Version installiert. Zudem ist auf den Systemen die BitLocker-Verschlüsselung aktiviert, um die Daten vor unbefugtem Zugriff zu schützen.

Identitäts- und Zugriffsmanagement:
- Active Directory und Entra ID: Für die zentrale Verwaltung von Benutzern und Rechten wird sowohl Active Directory (on-premise) als auch Entra ID (Cloud) eingesetzt.
- Windows Hello: Zur Anmeldung an Windows-Geräten wird Windows Hello for Business als passwordless Anmeldemethode als Option eingesetzt. Dabei kommen Methoden wie Gesichtserkennung, Fingerabdruck oder PIN zum Einsatz. Authenticator: Zur Multifaktor-Authentifizierung kommt die Microsoft Authenticator App zum Einsatz. Benutzer bestätigen ihre Anmeldungen per App auf dem Smartphone, per Push-Benachrichtigung, Zahleneingabe oder biometrischem Faktor. Es werden zudem für spezielle Zugriffe Passkeys (FIDO2) eingesetzt.

- Entra PIM: Für die Verwaltung von privilegierten Konten (z. B. Administratoren) wird Entra PIM verwendet. Hierüber können erhöhte Rechte für definierte Zeiträume angefordert und zugeteilt werden.

Analytics und Automatisierung:
- PowerBI: In der Verwaltung gibt es aktuell ein Pilotprojekt für PowerBI, das sich ausschliesslich auf PowerBI in der Cloud konzentriert und keine On-Premise-Konnektoren nutzt. Ziel dieses Pilotprojekts ist es, verschiedene Auswertungen und Analysen für das Amt für Informatik zu ermöglichen, insbesondere im Bereich IT-Service-Management (ITSM) und für Finanzthemen wie Budgetierung und Finanzbuchhaltung, die ebenfalls auf dem ITSM-Tool basieren. Auch andere Ämter zeigen Interesse an ähnlichen Auswertungen.

In der Untersuchungseinheit 2 wird M365 umfassend für zentrale Arbeitsbereiche wie Kommunikation, Produktivität, Informationsmanagement sowie Sicherheit und Compliance eingesetzt. Einige Funktionen wie Copilot (KI) und PowerBI werden noch pilotiert.

Übersicht der Integrationen in M365:
Die Untersuchungseinheit 2 bindet eine Vielzahl von Fachanwendungen und Tools in die M365 Umgebung ein. Insbesondere in den Bereichen Sicherheit und Compliance sind tiefe und in Teilen bidirektionale Anbindungen implementiert, die einen standardisierten und effizienten Informationsfluss zwischen den Systemen gewährleisten.

Um den Integrationsgrad der einzelnen Funktionsbereiche systematisch darzustellen, verwenden wir folgende Skala:

Stufe	Beschreibung
1	Keine Integrationen
2	Vereinzelte Integrationen
3	Umfassende Integrationen

Tabelle 14: Bewertungsskala Integrationsgrad der einzelnen Funktionsbereiche

Die folgende Tabelle zeigt, für welche Funktionsbereiche in welchem Umfang Integrationen vorliegen:

Funktionsbereich	Einstufung	Beispielhafte Integrationen
Kommunikation und Kollaboration	2	SEPPMail
Produktivitäts- und Geschäftsanwendungen	2	Vorlagen Manager

Datei- und Informationsmanagement	3	Verschiedene Fachanwendungen
Sicherheit und Compliance	3	Sentinel Purview
Künstliche Intelligenz	3	Copilot Integrationen in M365 Anwendungen und Dienste via Microsoft Graph API
Betriebssystem	1	
Identitäts- und Zugriffsmanagement	3	KeyCloak Fachapplikationen
Analytics und Automatisierung	1	Keine

Tabelle 15: Analyse Integrationstiefe Funktionsbereiche Untersuchungseinheit 2

Im Rahmen der folgenden Ausführungen wird jeweils auf die zentralsten und betrieblich signifikanten Integrationen eingegangen.

Kommunikation und Kollaboration:
Im Bereich Kommunikation und Kollaboration sind verschiedene M365-Integrationen im Einsatz. Beispielsweise sind verschiedene Fachapplikationen an M365 angebunden, um automatisierte Alerts via Mail zu versenden. Für verschlüsselte E-Mails wird SEPPMail für Exchange verwendet.

Produktivitäts- und Geschäftsanwendungen:
Im Bereich Produktivitäts- und Geschäftsanwendungen ist ein in Word integriertes Vorlagenmanagement Tool im Einsatz.

Datei- und Informationsmanagement:
Im Bereich Datei- und Informationsmanagement sind verschiedene Fachanwendungen mit SharePoint integriert. Beispielsweise für das Gebäudemanagement oder die Finanzmarktaufsicht.

Sicherheit und Compliance:
Im Bereich Sicherheit und Compliance stellen Sentinel und Microsoft Purview zentrale Integrationsknotenpunkte dar.

Das SIEM-System Microsoft Sentinel ist tief in die gesamte M365- und Azure-Infrastruktur eingebettet und ermöglicht eine ganzheitliche Überwachung und analysebasierte Auswertung der Security-Events. Insbesondere ist Sentinel über Schnittstellen direkt mit Defender-Produkten (Defender for Endpoint, Defender for Office 365, etc.) und verschiedenen Audit- und Logquellen aus der Microsoft-Cloud sowie Hybridkomponenten integriert. Das Security Operations Center (SOC) nutzt Sentinel.

Microsoft Purview ist für die Durchsetzung von DLP-Policies und Sensitivity Labels integriert.

Künstliche Intelligenz:
Im Bereich Künstliche Intelligenz kann bei Bedarf in der Verwaltung der M365 Copilot bestellt werden, welcher über Microsoft Graph in diverse relevante M365 Anwendungen und Dienste integriert ist.

Betriebssystem:
Im Bereich Betriebssystem sind keine Integrationen vorhanden.

Identitäts- und Zugriffsmanagement:
Im Bereich Identitäts- und Zugriffsmanagement sind die Integrationen von Microsoft Entra ID und Active Directory zentral.

Eine Vielzahl weiterer Lösungen ist direkt oder indirekt an das M365-IAM angebunden.

Keycloak fungiert als On-Premises-Broker für bestimmte Fachanwendungen.
Authentifizierungsanfragen werden von Keycloak übernommen und an Entra ID zur eigentlichen Identitätsprüfung weitergeleitet.

Analytics und Automatisierung:
Power BI, Power Apps, und Power Automate werden derzeit nicht produktiv eingesetzt.

Daten:
Derzeit werden in der Verwaltung Daten der Datenkategorien öffentlich, intern, eingeschränkt und DSGVO (für besondere Kategorien von personenbezogenen Daten) in M365 in der Cloud verarbeitet für definierte Anwendungsfälle. Daten der Kategorien vertraulich und geheim gemäss IschV dürfen nicht in der M365 Cloud verarbeitet werden, nur auf Office 365 Apps auf dem lokalen Arbeitsplatz.

Makros werden derzeit in der gesamten Verwaltung eingesetzt, hauptsächlich für Listen- und Datenmutationen. In der Organisation dürfen nur signierte VBA-Skripte ausgeführt werden.
Es sind mehrere Vorlagen für wie Textdokumente und Präsentationen im Einsatz.

Hosting:
SharePoint, Microsoft Exchange, und die Teams-Telefonie werden hybrid bereitgestellt.

Die Untersuchungseinheit 2 verfügt über weitreichende und teils bidirektionale Integrationen verschiedener Fachanwendungen und Tools in M365, insbesondere in den Bereichen Sicherheit/Compliance, Künstliche Intelligenz und Identitätsmanagement.

3.5.3.2 Organisatorische Ist-Situation

Untersuchungseinheit 2 hat M365 im letzten Jahr eingeführt und zeigt heute eine gut etablierte, Microsoft-optimierte und auf Microsoft angepasste IT-Organisation. Die Analyse ist geprägt von folgenden Punkten:

- Etablierte Partnerstrukturen mit kalkulierbaren Kosten: Untersuchungseinheit 2 arbeitet mit einem Partner, der zwischen Microsoft und der Organisation vermittelt. Schnittstellen und Kosten sind kalkulierbar und klar definiert, was zu einem geringen Steuerungsaufwand führt. Die Organisation profitiert von einem strukturierten «Generalunternehmer-Modell» mit minimaler interner Ressourcenbindung für das operative Vendor-Management.
- Kontinuierliche Transformation durch M365-Anpassung: Die Organisation befindet sich weiterhin in der Transformation, da sie eine Plattform eingeführt hat und sich laufend anpassen muss. Es hängen noch zu viele Aufgaben an wenigen "Kopfmonopolen", aber die Entwicklung geht in Richtung spezialisierter Teams. Das Fachwissen wird schrittweise in der Organisation verankert und institutionalisiert. Microsoft entwickelt die Plattform stetig weiter, was die Organisation immer wieder herausfordert. Die Anpassungsprozesse sind noch nicht abgeschlossen, da die Plattform kontinuierliche organisatorische Veränderungen erfordert.
- Perfekte Standardisierung durch De-facto-Standard: Microsoft gibt den Standard vor und fungiert als De-facto-Standard, wodurch automatisch Interoperabilität gewährleistet ist. Jeder hat Microsoft und jeder kann damit umgehen, was die Standardisierung vereinfacht. Diese automatische Standardisierung eliminiert jeglichen Koordinationsaufwand und ermöglicht volle Synergien mit anderen Parteien.
- Keinerlei Roadmap-Einfluss: Die Organisation hat absolut keinen Einfluss auf die Entwicklungsrichtung von M365 und muss alle vorgegebenen Änderungen der eingesetzten Funktionen und Komponenten übernehmen. Microsoft bestimmt Funktionsumfang, Weiterentwicklungen und Abkündigungen vollständig autonom. Diese Situation wird als "Friss oder stirb"-Verhältnis charakterisiert, bei dem die Roadmap ausschliesslich durch den Anbieter diktiert wird.
- Nahtlose Architektur-Integration: Microsoft sorgt für die perfekte Integration aller Komponenten. Die Gesamtarchitektur und deren Interoperabilität sind durch den Vendor definiert, ohne dass interne Architekten stark gebunden werden. Die Organisation muss keine Schnittstellen selbst bauen oder bei Updates reparieren, da die Interoperabilität systemisch gewährleistet ist.
- Moderate Fachämter-Integration mit variierenden Kompetenzen: Die Fachämter können Anforderungen nennen, wobei die IT diese in entsprechende Konfigurationen übersetzt. Es braucht mehr IT-Kompetenz in den Fachämtern, und die Spannweite reicht von Experten bis zu jenen mit weniger Wissen. Die Zusammenarbeit funktioniert grundsätzlich, erfordert aber strukturierte Prozesse zwischen fachlichen Anforderungen und technischer Umsetzung.
- Etablierte Compliance mit regulatorischen Vorgaben: Die regulatorischen Vorgaben werden durch die Plattform erfüllt, wobei entsprechende organisatorische und technische Massnahmen implementiert wurden. Es gibt ein Nutzungsreglement und DSGVO- resp. DSG-konforme konforme Datenklassifizierungen sowie Pflichtlernpfade. Die Compliance-Prozesse sind in die bestehenden Governance-Strukturen integriert und funktionieren routiniert.

- Hohe Nutzerakzeptanz und starkes Management-Commitment: Eine interne Umfrage bei den M365-Endanwenderinnen und -Endanwendern zeigte überwiegend positive Rückmeldungen zur alltäglichen Nutzung und zum verfügbaren Funktionsumfang; die Nutzerakzeptanz wird daher als hoch eingestuft (Bewertung 4.5 auf einer Skala von 1–5). Zudem: Das Management-Commitment zur M365-Strategie ist stark ausgeprägt im Amt, während es in der Politik etwas tiefer liegt. Die erfolgreiche User Adoption zeigt sich in der produktiven Nutzung der verfügbaren Funktionen.

Untersuchungseinheit 2 zeigt eine Organisation im Übergang, die M365 soeben eingeführt hat und sich noch in der Transformationsphase befindet. Während die technische Integration nahtlos funktioniert und die Standardisierung perfekt ist, befinden sich Kompetenzen und Prozesse noch im Aufbau. Die Organisation hat eine hocheffiziente, aber vollständig Microsoft-abhängige Struktur geschaffen, die einen Wechsel zu einem organisatorischen Grossprojekt mit kompletter Restrukturierung machen würde, besonders herausfordernd, da die M365-Strukturen noch nicht vollständig etabliert sind.

3.5.3.3 Regulatorische Analyse

Die regulatorische Analyse der Untersuchungseinheit 2 zeigt ein formal legitimiertes und institutionell verankertes Modell für den Einsatz von M365 als zentrale Arbeitsplatzinfrastruktur der Verwaltung, einschliesslich der angebundenen Blaulichtorganisationen. Die Nutzung erfolgt auf Grundlage eines expliziten politischen Entscheids, wonach das verbleibende rechtliche Restrisiko, insbesondere im Zusammenhang mit möglichen Behördenzugriff (Lawful access), bewusst in Kauf genommen und als vertretbar eingestuft wurde.

Die Nutzung von M365 ist damit nicht nur technisch und organisatorisch, sondern auch politisch-rechtlich abgestützt und als gesteuertes Risiko institutionalisiert.

Dies manifestiert sich in folgenden Kernbereichen:

- Politisch legitimierter Risikotransfer: Grundlage bildet ein formeller Regierungsbeschluss, mit dem das verbleibende Restrisiko, insbesondere im Hinblick auf extraterritoriale Zugriffsbefugnisse, explizit zur Kenntnis genommen wurde. Die Nutzung von M365 erfolgt damit auf Basis einer bewussten Risikoabwägung auf Regierungsebene.
- Informationsschutzbasierte Nutzungseinschränkungen: Für Daten der Klassifizierungsstufen «vertraulich» und «geheim» gemäss Informationsschutzverordnung (IschV) ist die Nutzung von M365 ausgeschlossen. Ein entsprechendes Klassifikationssystem ist etabliert, dessen konsistente Anwendung im operativen Alltag nach Einschätzung des Interviewpartners jedoch eine laufende Herausforderung darstellt.
- Differenzierte Schlüsselstrategie: Customer Managed Keys wird eingesetzt und verschlüsselt alle gespeicherten Daten (Data@Rest) im Tenant mit unserem Key. Der Schlüssel befindet sich im Azure Key Vault mit einer zugemieteten HSM. Im Verlustfalle kann ein vier Augen Recovery Prozess eingeleitet werden. Double Key Encryption (filebasierte Verschlüsselung)

wird nicht flächendeckend eingesetzt, da es Impacts auf Services mit sich bringt. Damit wird dem Grundsatz der Verhältnismässigkeit Rechnung getragen: Der weitergehende Schutz, den ein ausserhalb der Anbieterumgebung gehaltener Schlüssel bietet, geht mit funktionalen Einschränkungen der Plattform einher, weshalb sein Einsatz auf jene Daten beschränkt wird, deren Schutzbedarf diese Einschränkungen rechtfertigt. Die Schlüsselstrategie ist damit risikobasiert und nach Massgabe des jeweiligen Schutzbedarfs abgestuft ausgestaltet.
- Bewusst eingegangener Vendor Lock-in: Die Abhängigkeit vom Anbieter wurde bereits bei der Einführung antizipiert. Ein Konzept zur Datenextraktion sowie eine Exitstrategie sind vorhanden, wurden jedoch bislang nicht operativ erprobt.
- Aktive politische Einbettung: Die Nutzung von M365 ist Gegenstand eines laufenden politischen Diskurses. Parlamentarische Anfragen werden durch die zuständigen Stellen faktenbasiert beantwortet, was auf eine aktive Bewirtschaftung der regulatorischen und politischen Dimension hinweist.

Die Untersuchung zeigt ferner folgendes Bild:
- Antizipation zukünftiger Regulierung (insbesondere KI): Regulatorische Entwicklungen, insbesondere im Bereich künstlicher Intelligenz, werden bereits berücksichtigt. Entsprechende Governance-Strukturen (z. B. Richtlinien, Schulungen, organisatorische Zuständigkeiten) befinden sich im Aufbau und werden künftig zusätzliche Compliance-Anforderungen mit sich bringen.
- Informationsschutz und Klassifizierung: Die organisationsinterne Informationsschutzsystematik definiert verbindliche Klassifizierungsstufen mit entsprechenden Nutzungseinschränkungen. Die praktische Umsetzung, insbesondere die korrekte Klassifizierung im Arbeitsalltag, wird als wesentlicher Erfolgsfaktor und gleichzeitig als Herausforderung beschrieben.
- Beschaffungsrechtlicher Kontext: Die Beschaffung unterliegt den Vorgaben des öffentlichen Beschaffungsrechts. Nach Einschätzung des Interviewpartners ist der Markt für vergleichbare Plattformlösungen faktisch stark konzentriert, was den effektiven Wettbewerb einschränkt und als strukturelle Rahmenbedingung zu berücksichtigen ist.
- Governance & Kontrollinstanzen: Die Governance-Struktur ist mehrschichtig ausgestaltet und umfasst neben klassischen Rollen (Informationssicherheit, Datenschutz, CISO) zusätzliche spezialisierte Funktionen (insbesondere Cybersicherheit sowie perspektivisch KI-Governance). Ergänzend bestehen politische und parlamentarische Kontrollmechanismen, welche die Nutzung von Cloud-Diensten begleiten.

Schlüsselthemen der regulatorischen Risikoexposition:
- Drittstaatszugriffe: Werden als primäre Risikoachse eingeordnet. Die Bewertung erfolgt anhand der tatsächlichen rechtlichen Zugriffsmöglichkeiten sowie der Durchsetzbarkeit von Datenschutzrechten.
- Verschlüsselung und Schlüsselkontrolle: Customer Managed Key wird flächendeckend angewendet, bedingt aber eine E5 Lizenz. Der Schlüssel befindet sich im Azure Key Vault mit einer zugemieteten HSM. Erweitert wird die Double Key Encryption (filebasierte Verschlüsselung) punktuell eingesetzt.

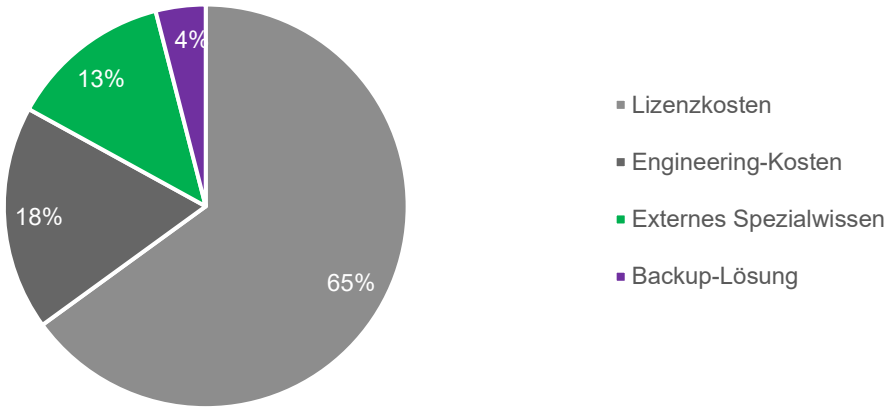
- Metadatenverarbeitung und Transparenz: Die Abhängigkeit von Anbieterinformationen wird als eigenständige regulatorische Herausforderung bewertet.
- Vendor Lock-in: Bestehende Abhängigkeiten werden anerkannt, durch vorhandene Exit-Konzepte jedoch teilweise adressiert, wobei deren praktische Umsetzbarkeit bislang nicht verifiziert ist.
- Bewertung von Handlungsoptionen: Mögliche Alternativen zu M365 werden anhand klar definierter Kriterien beurteilt. Im Zentrum stehen insbesondere die Gewährleistung eines vergleichbaren Schutzniveaus gegenüber staatlichen Zugriffen, funktionale und sicherheitstechnische Gleichwertigkeit, Integrationsfähigkeit in bestehende Systemlandschaften, effektive Datenhoheit (insbesondere Schlüsselkontrolle) sowie Krisenfestigkeit und Exitfähigkeit.

Untersuchungseinheit 2 ist sich bewusst, dass die Nutzung von M365, insbesondere im Zusammenspiel von Verwaltung und Blaulichtorganisationen, in einem Spannungsfeld zwischen rechtlichen Anforderungen, sicherheitstechnischen Erwartungen und operativer Effizienz erfolgt. Die bestehenden Restrisiken, namentlich im Bereich Drittstaatenzugriffe und eingeschränkter Transparenz, werden aktiv adressiert, jedoch im Rahmen des politisch legitimierten Gesamtmodells als vertretbar eingeordnet.

3.5.3.4 Finanzielle Ist-Situation

Die direkt M365 zugewiesenen Kosten der Untersuchungseinheit 2 sind klar lizenzgetrieben. Mit den M365-Abos werden gleichzeitig Infrastruktur, Security-Funktionen und ein grosser Teil des Betriebs „mitgebündelt“, was die Budgetierung vereinfacht und viele Einzelpositionen im Schatten verschwinden lässt. Gleichzeitig zeigt die Analyse aber, dass rund ein Drittel der direkt M365-bezogenen Aufwände aus Zusatzkosten für internes Engineering, Backup/DR und externe Expertise besteht.

Zum Schutz der Vertraulichkeit vermeiden wir die Nennung von absoluten Finanzzahlen. Wir konzentrieren uns stattdessen auf aggregierte Ergebnisse und Tendenzen – diese machen die wirtschaftlichen Zusammenhänge ebenso deutlich und lassen valide Erkenntnisse für die Studie zu.



Position	Anteil der Kosten
Lizenzkosten	65 %
Engineering-Kosten	18 %
Externes Spezialwissen	13 %
Backup-Lösung	4 %

- Dominanz der M365-Lizenzkosten: Den grössten Einzelblock bilden die M365-Abonnements (E5-Pläne für interne Mitarbeitende). Pro intern angestellter Person entspricht dies einer monatlichen Investition im Bereich von einigen Dutzend Franken und stellt damit den zentralen, klar kalkulierbaren OpEx-Posten dar.
- Ergänzende Betriebs- und Backup-Aufwände: Neben den Lizenzen fallen für M365-nahe Backup- und Disaster-Recovery-Leistungen jährliche Kosten von rund 4 % der Lizenz- und Betriebskosten an. Diese decken insbesondere die Sicherung geschäftskritischer Daten und die Einhaltung regulatorischer Anforderungen ab, ohne dass zusätzliche, explizit M365-spezifische Infrastrukturkosten (Server, RZ-Fläche) ausgewiesen werden.
- Interner Engineering- und Integrationsaufwand: Für den Betrieb und die Weiterentwicklung der M365-basierten Workplace-Umgebung sind interne Kapazitäten für Architektur, Identitätsmanagement und Schnittstellenintegration notwendig. Diese Ressourcen stellen sicher, dass M365 in die bestehende Systemlandschaft (z. B. Identity- und Access-Management, Fachapplikationen, Single Sign-On) sauber eingebettet ist. Im Kostenmodell werden diese Personalkosten mit zirka 18 % der direkt M365 zugewiesenen Kosten beziffert.
- Externe Expertise im Betrieb: Für spezialisierte Betriebsunterstützung und M365-Engineering werden jährlich rund 13 % der direkt M365 zugewiesenen Kosten eingesetzt. Diese Mittel

sichern den Zugang zu Expertenwissen für Konfiguration, Sicherheitsoptimierungen und komplexe Betriebsfragen, ohne dass umfangreiche interne Spezialistenkapazitäten aufgebaut werden müssen.
- Konzentration der Kosten im SaaS-Modell: Infrastruktur- und Security-Investitionen, die direkt dem M365-Ökosystem zugerechnet werden könnten, sind heute nicht separat ausgewiesen. Sie werden primär durch die Microsoft-Cloud abgedeckt oder in generischen IT-Budgets geführt.

M365 manifestiert sich bei der Untersuchungseinheit 2 als lizenzgetriebener Service, mit einer wesentlichen Abhängigkeit zu den wiederkehrenden M365-Abonnementgebühren. Mit diesen Lizenzen werden gleichzeitig ein Grossteil der Infrastruktur-, Security- und Betriebsleistungen gebündelt eingekauft, was die Budgetierung vereinfacht, aber die eigentliche Kostenstruktur stark in den Lizenzposten konzentriert.

3.5.3.5 Technische Soll-Analyse

Die technische Soll-Analyse der Untersuchungseinheit 2 zeigt mögliche technische Auswirkungen eines Wechsels von M365 zu openDesk auf. Die Analyse basiert auf Experteneinschätzungen, wobei subjektive Bewertungen unvermeidbar sind. Die Ergebnisse sind daher als Expertenmeinung zu potenziellen technischen Veränderungen zu verstehen.

Daten

Die Migration von M365 auf openDesk bringt aus datentechnischer Sicht Herausforderungen mit sich. In der untersuchten Organisation liegt ein beträchtlicher Anteil der bestehenden Daten und Dokumente in proprietären Office-Formaten (z. B. .docx, .xlsx, .pptx), mit teilweiser Erweiterung um komplexe Makros und VBA-Skripte.

Insbesondere die Konvertierung dieser Bestandsdaten in offene Formate stellt eine zentrale Herausforderung dar. Zwar bietet Collabora im openDesk-Kontext grundsätzlich eine akzeptable Kompatibilität und kann Standarddokumente weitgehend ohne Datenverlust übernehmen, bei Spezialfällen wie Makros, spezifischen Formatierungen oder Formularfunktionen können jedoch Inkompatibilitäten auftreten. Beispielsweise führen VBA-gestützte Excel-Vorlagen zu Funktionsverlust im Zielsystem. Viele Dokumente müssten deshalb einzeln validiert und ggf. manuell nachbearbeitet oder umfunktioniert werden. Der Prüf- und Nachbesserungsaufwand wird als signifkant veranschlagt.

Die Migration von M365 auf openDesk ist datentechnisch herausfordernd, da viele bestehende Dateien in proprietären Formaten vorliegen Besonders bei Makros und speziellen Formatierungen wird von einem erheblichen Prüf- und

Nachbesserungsaufwand ausgegangen, da viele Dokumente individuell angepasst werden müssen.

Funktionsumfang

OpenDesk setzt sich aus diversen Open-Source-Komponenten zusammen. Einzelne Bausteine funktionieren für bestimmte Anwendungsfälle (klassische Textverarbeitung, Präsentationen, Tabellenkalkulation) zufriedenstellend. Dennoch werden die folgenden Einschränkungen festgestellt:

- Makro- und VBA-Unterstützung: Viele Prozess- und Fachabläufe der Organisation basieren auf intensiver Makronutzung, beispielsweise für automatisierte Workflows oder zur Realisierung spezifischer Amtsgeschäfte. Diese Funktionalitäten lassen sich in openDesk potenziell nicht in vollem Umfang abbilden.
- Spezifische Formatierung und Corporate Design: Formatierungs-, Schrift- und Layouttreue zwischen M365-Dateiformaten und openDesk Alternativen ist potenziell nicht überall gewährleistet. Gerade bei Vorlagen und offiziellen Formularen führt dies zu Akzeptanzproblemen.
- Security & Compliance: M365 implementiert zahlreiche, sofort verfügbare Compliance- und Protection-Features (z. B. Data Loss Prevention, Sensitivity- und Retention-Labels, Einbindungsmöglichkeiten in Sentinel). OpenDesk bündelt grundlegende Sicherheitsfunktionen, ein einheitlich hoher Security- und Compliance-Level muss jedoch durch Verheiratung und Integration zahlreicher Einzelkomponenten erst geschaffen werden. Aktuell fehlen bei openDesk noch zentrale Features in Bezug auf Nachvollziehbarkeit und Schutz sensibler Daten fehlen oder erfordern Zusatzaufwand.
- Produktweiterentwicklung: M365 profitiert von grossen, kontinuierlichen Investitionen und schneller Feature-Implementierung durch Microsoft. Im Open-Source-Bereich sind die Innovationsdynamik und langfristige Stabilität aktuell noch weniger gut planbar.

OpenDesk bietet mit seinen Open-Source-Komponenten grundlegende Funktionen für die digitale Kollaboration, erfordert jedoch bei weitergehenden Anforderungen wie erweiterte Security und Compliance Funktionen zusätzlichen Anpassungs- und Integrationsaufwand. Im Vergleich dazu wird die langfristige Produktentwicklung und Feature-Implementierung bei OpenDesk als weniger planbar wahrgenommen.

Integrationen

Ein zentraler Aspekt bei einem möglichen Wechsel von M365 auf openDesk ist die Frage, in welchem Umfang die bestehende Systemlandschaft der Untersuchungseinheit 2 in die neue Zielumgebung integriert werden könnte. Die Organisation verfügt heute über verschiedene angebundene Fachanwendungen und sicherheitsrelevante Systeme, die teilweise tief in die Microsoft-Umgebung eingebettet sind. Besonders betroffen wären Integrationen, die derzeit auf Microsoft-spezifischen Diensten, proprietären Schnittstellen oder eng gekoppelten Plattformmechanismen beruhen, beispielsweise über Exchange, SharePoint, Microsoft Graph, Entra ID, Purview oder Sentinel.

Im Unterschied zu M365 stellt openDesk keine von einem Hersteller stammende Gesamtsuite dar, sondern eine Lösung, die sich aus mehreren Komponenten zusammensetzt. Daraus ergibt sich für die Soll-Situation ein anderes Integrationsparadigma: Während im Microsoft Ökosystem zahlreiche Funktionen und Schnittstellen bereits plattformintern aufeinander abgestimmt sind, müsste die Integration in einer openDesk-basierten Zielarchitektur stärker über offene Standards, APIs, Middleware und individuelle Adapterlösungen realisiert werden.

Grundsätzlich ist davon auszugehen, dass bei einem Wechsel auf openDesk nicht alle bestehenden Integrationen unverändert übernommen werden könnten. Vielmehr wäre für jeden Funktionsbereich zu prüfen, ob
- eine bestehende Integration direkt ersetzbar ist,
- eine funktional gleichwertige Anbindung über Standardschnittstellen realisiert werden kann,
- eine Anpassung der Fachanwendung notwendig wird,
- oder ein bisheriger Integrationsfall ganz neu konzipiert werden müsste.

Vor diesem Hintergrund ist in der Soll-Situation eher von einer partiellen Neuordnung als von einer reinen technischen Migration der Integrationslandschaft auszugehen. Besonders deutlich werden die Auswirkungen eines Wechsels auf openDesk in den nachstehenden Integrationsfeldern:

- Sicherheit und Compliance: Der grösste strukturelle Unterschied zwischen der Ist- und der Soll-Situation ist im Bereich Sicherheit und Compliance zu erwarten. In der heutigen Umgebung übernehmen Microsoft Sentinel und Microsoft Purview zentrale Plattformfunktionen für Security-Monitoring, Auditierung, DLP, Sensitivity Labels und Compliance-nahe Steuerungsmechanismen. Diese Fähigkeiten sind tief in die Microsoft-Plattform integriert und profitieren von einer gemeinsamen Datenbasis, einheitlichen Identitäten und nativen Produktkopplungen. In einer openDesk-basierten Zielarchitektur wäre ein vergleichbarer Integrationsgrad voraussichtlich nicht unmittelbar vorhanden. Stattdessen müsste eine eigenständige Sicherheits- und Compliance-Architektur aufgebaut werden. Dazu könnten beispielsweise gehören:
  - ein separates SIEM für Protokollsammlung und Korrelation
  - eigenständige Logging- und Auditkonzepte für die beteiligten openDesk-Komponenten
  - alternative Lösungen für DLP und Informationsklassifizierung
  - sowie gegebenenfalls zusätzliche Werkzeuge für E-Mail-Sicherheit, Endpoint-Schutz und revisionsnahe Nachvollziehbarkeit

  Aus Integrationssicht würde sich der Schwerpunkt damit von einer tiefen plattforminternen Kopplung hin zu einer übergreifenden Sicherheitsorchestrierung verlagern. Dies erhöht voraussichtlich den Architektur-, Betriebs- und Abstimmungsaufwand. Insbesondere müsste sichergestellt werden, dass Logs, Sicherheitsereignisse, Benutzerkontexte und Klassifizierungsinformationen aus verschiedenen Komponenten konsistent zusammengeführt werden können.
- Künstliche Intelligenz: Im Bereich Künstliche Intelligenz wäre davon auszugehen, dass die in M365 mögliche Integrationstiefe nicht fortgeführt werden könnte. Copilot greift über Microsoft

Graph auf Inhalte, Kontexte, Berechtigungen und Beziehungen innerhalb der Microsoft-Dienste zu. Gerade diese enge Anbindung an E-Mail, Dateien, Besprechungen, Chats und Dokumente ist eine wesentliche Grundlage des Funktionsumfangs von Copilot. In einer openDesk-Zielumgebung wäre eine solche durchgängige, suiteweite KI-Integration in dieser Form nicht gegeben. KI-Funktionen müssten entweder über separate, spezialisierte KI-Dienste angebunden, auf einzelne Komponenten beschränkt, oder über eigene Integrationsschichten mit Such-, Berechtigungs- und Kontextdiensten aufgebaut werden. Dies wäre nicht ausgeschlossen, aber deutlich komplexer als in einer Microsoft-zentrierten Umgebung. Für die Soll-Situation ist daher eher von einem niedrigen Integrationsgrad im KI-Bereich auszugehen, sofern nicht bewusst zusätzliche strategische Investitionen in diesen Bereich erfolgen.

- Datei- und Informationsmanagement: Im Bereich Datei- und Informationsmanagement ist der heutige Integrationsgrad wesentlich durch Anbindungen von Fachanwendungen an SharePoint geprägt. Für eine openDesk-Zielarchitektur wäre daher zentral zu untersuchen, welche Rolle die dort eingesetzten Datei- und Dokumentenablagen übernehmen sollen und ob bestehende Fachanwendungen diese über standardisierte Schnittstellen anbinden können. Soweit heutige Integrationen auf generischen Dateioperationen, WebDAV, REST-APIs oder klar dokumentierten Austauschformaten beruhen, erscheint eine Migration grundsätzlich eher realisierbar. Schwieriger wäre die Situation dort, wo Fachverfahren spezifische SharePoint-Funktionen nutzen, etwa Metadatenmodelle, Berechtigungskonzepte, versionierte Dokumentenworkflows, Listenkonzepte oder individuell entwickelte SharePoint-Connectoren. In solchen Fällen wäre nicht nur die technische Schnittstelle, sondern häufig auch der fachliche Prozess neu zu gestalten.

Ein Umstieg auf openDesk würde die Integrationslandschaft der Untersuchungseinheit 2 nicht einfach übertragen, sondern in wesentlichen Teilen neu strukturieren. Je stärker bestehende Anbindungen heute in M365 eingebettet sind, desto geringer ist ihre direkte Übertragbarkeit in die Zielumgebung. Daraus ergeben sich vor allem in den Bereichen Security und Compliance, Künstliche Intelligenz und Dateien- und Informationsmanagement erhebliche konzeptionelle und technische Prüfbedarfe.

3.5.3.6 Organisatorische Soll-Analyse

Die organisatorische Soll-Analyse für Untersuchungseinheit 2 zeigt, welche Veränderungen ein Wechsel von M365 zu openDesk organisatorisch mit sich bringen würde. Die Einschätzungen basieren auf Rückmeldungen der Experten zu den vier Organisationsdimensionen. Trotz des systematischen Vorgehens bleiben die Antworten Experteneinschätzungen, sie liefern aber einen klaren Datenpunkt dazu, wo sich die Organisation bei einem Exit von M365 organisatorisch neu ausrichten müsste. Im Wesentlichen sind folgende, zusammenfassende Punkte:

- Vendor-Management: Heute profitiert die Organisation von einer strategischen Fokussierung auf einen dominanten Anbieter und einem Generalunternehmer-Modell mit überschaubarem Steuerungsaufwand: M365 liefert eine weitgehend vollständige Suite, in der viele Funktionen integriert „aus einer Hand“ kommen. OpenDesk deckt zwar zentrale Kollaborations- und Produktivitätsfunktionen ab, ersetzt M365 aber nicht vollständig. Statt eines klaren Hauptlieferanten entstünde damit ein Ökosystem aus Produktanbieter (ZenDiS), Hoster und weiteren Spezialisten, ergänzt durch Eigenleistungen der zentralen Informatik. Die Experten erwarten, dass der Aufwand im Vendor-, Vertrags- und Sourcing-Management steigt, weil zusätzliche Verträge koordiniert und technische wie organisatorische Abhängigkeiten aktiv gesteuert werden müssen.
- Exit-Fähigkeit: Die Exit-Fähigkeit verbessert sich aus Sicht der Experten nicht automatisch: Der wesentliche Lock-in wird weniger durch das Tool selbst als u.a. auch durch die über Jahre gewachsenen Arbeitsweisen, Prozesse und Benutzergewohnheiten bestimmt. Auch in einer neuen, modular zusammengesetzten Lösung würde sich mittelfristig ein faktischer Lock-in einstellen; ein späterer Wechsel wäre erneut ein grosses Change-Projekt.
- Mehr Einfluss auf die Produktentwicklung: Gegenüber M365 sehen die Experten einen klaren Vorteil in den Mitsprache-Möglichkeiten: Über Community-Kanäle, User-Groups und den direkten Dialog mit ZenDiS könnte die Verwaltung spezifische Anforderungen der öffentlichen Hand besser einbringen, anstatt eine herstellergetriebene Roadmap zu akzeptieren. Dieser Einfluss ist jedoch vor allem auf den openDesk-Kern bezogen.
- Mehr interne Governance und Architekturarbeit: Zwar übernimmt ZenDiS einen Teil der Architektur- und Integrationsarbeit innerhalb des openDesk-Stacks, doch ein M365-Ersatz umfasst zusätzliche Komponenten ausserhalb von openDesk. Die Bewertung, Auswahl und Integration dieser Zusatzkomponenten liegt vollständig bei der eigenen Informatik. Damit steigt der Bedarf an Architektur Boards, Richtlinien und Entscheidungsprozessen, die das Zusammenspiel von openDesk und den ergänzenden Produkten steuern. Die heutige, stark auf Microsoft ausgerichtete Architektur Governance müsste erweitert werden.
- Mehr Integrationsaufgaben: Im openDesk-Szenario rechnen die Experten damit, dass sich der Aufwand im Engineering und in der Integration erhöht. Gründe sind insbesondere die zusätzliche Integration und Betrieb von Komponenten die nicht durch openDesk abgedeckt werden.
- Skill-Shift: Linux Know-how ist in der Organisation grundsätzlich vorhanden, liegt heute aber eher im Backend Bereich. Für einen openDesk Betrieb wäre dieses Wissen verstärkt im Workplace und Kollaborationsumfeld gefragt (Container Plattform, Troubleshooting im Stack), was einen spürbaren Skill Shift und zusätzliche Weiterbildung erfordert. Gleichzeitig wird betont, dass qualifiziertes Personal mit OSS und Linux Kompetenzen im Markt schwerer zu finden ist und Rekrutierungen Zeit- und Kostenintensiv sind.
- Release-Management und Testing: Die Möglichkeit, Releases gemeinsam mit Hoster und Anbieter zu planen, wird grundsätzlich positiv bewertet. Gleichzeitig erwarten die Experten, dass in der Praxis eher grössere, seltener eingespielte Release-Pakete entstehen, die einen erhöhten fachlichen und technischen Testaufwand mit sich bringen. Insgesamt ist daher davon auszugehen, dass der Koordinations- und Testaufwand im openDesk-Szenario mindestens gleich hoch, tendenziell aber höher ausfallen würde – insbesondere, weil ohne

zusätzliche Arbeiten in Testing und Koordination mit Komponenten ausserhalb der Suite erforderlich werden.
- User Adoption: Untersuchungseinheit 2 weist heute eine hohe Nutzerakzeptanz und ein starkes Management-Commitment für M365 auf. Die Mitarbeitenden sind an die bekannten Oberflächen und Workflows gewöhnt. M365 gilt intern als moderner Standardarbeitsplatz. Ein Wechsel auf openDesk würde daher einen substanziellen Change-Aufwand bedeuten: neue Oberflächen, teilweise andere Bedienkonzepte und eine veränderte Kollaborationslogik müssten eingeführt und erklärt werden.

Die Experten sehen zwar zusätzliche Mitsprache- und Gestaltungsmöglichkeiten, gehen aber davon aus, dass die bestehenden organisatorische Strukturen und Aufgaben primär auf M365 ausgerichtet sind und für ein openDesk-Szenario deutlich ausgebaut und umorganisiert wer-den müssten

3.5.3.7 Finanzielle Soll-Analyse

Die finanzielle Soll-Analyse für die Untersuchungseinheit betrachtet die potenziellen Kostenwirkungen eines Wechsels von der heute etablierten M365-Plattform hin zur OSS-basierten Suite openDesk. Methodisch folgt sie demselben Vorgehen wie bei Untersuchungseinheit 1. Auch hier ist eine exakte Bestimmung der Soll-Finanzen ohne konkrete Offerten, verbindliche Leistungsdefinitionen und detaillierte Lastenhefte nicht möglich. Die nachfolgenden Angaben beruhen jedoch auf einem strukturierten, am in Kapitel 3 beschriebenen Kostenmodell ausgerichteten Vorgehen. Die wesentlichen Kostenblöcke eines möglichen openDesk-Szenarios wurden gemeinsam mit Fachpersonen der Untersuchungseinheit 2 entlang der relevanten Kostenkategorien durchgearbeitet und plausibilisiert.
Aus Vertraulichkeits- und Darstellungsgründen werden wiederum nur aggregierte Ergebnisse, Grössenordnungen und Kostentendenzen ausgewiesen. Die Werte sind als indikative, gemeinsam validierte Schätzungen zu verstehen und stellen keine verbindliche Kalkulationsgrundlage dar.
Wiederkehrende Kosten
Die M365-E5-Abonnements bilden heute den wesentlichen Einzelposten in der direkten, M365 allozierbaren Kostenstruktur. Im openDesk-Szenario würden sich die direkten Lizenzkosten reduzieren, da openDesk-SaaS-Lizenz bzw. Enterprise-Support-Lizenz wesentlich unter den heutigen E5-Tarifen liegen (siehe Aufstellung im Abschnitt 3.5.2.9). Gleichzeitig entstehen neue Kostenblöcke, die heute durch Microsoft „mitgebündelt“ werden:
- Hosting/Infrastruktur: Während M365 die gesamte Workplace-Infrastruktur als Service bereitstellt, wären für openDesk entweder ein dedizierter SaaS-Provider oder eigene Hosting-Ressourcen zu finanzieren. Wie stark diese Leistungen vom Hoster übernommen werden, hängt von der konkreten Vertragsgestaltung ab. Die Experten gehen davon aus, dass der Hoster zwar zentrale Betriebsaufgaben (z. B. Plattform-Betrieb, Basis-Monitoring)

übernehmen würde, ein wesentlicher Teil der Integrations- und Abstimmungsarbeiten aber bei der eigenen Informatik verbleibt.
- Security-Stack: Heute sind wesentliche Security-Funktionen in den E5-Lizenzen enthalten. Im Soll-Szenario müssten MDM, Endpoint-Schutz, Data-Loss-Prevention und weitergehende Identity-Schutzmechanismen teilweise durch Drittprodukte abgedeckt werden. Das Kostenmodell weist hierfür einen eigenständigen Block aus, der einen relevanten Teil der Einsparung bei den M365-Security-Komponenten wieder kompensiert.

Die heutige M365-Landschaft ist so ausgelegt, dass ein grosser Teil der Komplexität zum Hersteller ausgelagert ist. Im Kostenmodell sind für Engineering & Integration aktuell rund 1.5 FTE ausgewiesen.

Im openDesk-Soll-Bild rechnen die Experten mit 2.25 FTE-Engineering-Aufwand:
- Der Integrationsaufwand ist bei einer OSS-Landschaft höher, da mehrere „Best-of-Breed"-Module (openDesk, Security etc.) mit eigenem Release-Zyklen zusammenspielen müssen. Die Abstimmung und das Testing der Interoperabilität erfordern eine dedizierte Koordinationsstelle. Dies auch im Bewusssein, dass ZenDiS und der Hoster ein Teil der Arbeit übernehmen wird.
- Zusätzlich sind Komponenten zu integrieren und zu betreiben, die heute in M365 enthalten sind (z. B. Intune-Ersatz, Purview-/DLP-Funktionen, MDM).

Einmalige Kosten
Die Experten rechnen mit folgenden Grobschätzungen für die wichtigsten Transformationsblöcke:
- Datenmigration: Für die technische Migration und Bereinigung von E-Mail-Archiven, SharePoint-Daten und OneDrive-Inhalten werden 2.5 Mio. CHF veranschlagt. Als Referenz dient die ursprüngliche M365-Einführung (Datenmigration) mit rund 2 Mio. CHF; für den Wechsel auf eine OSS-Suite wird aufgrund höherer Komplexität ein Faktor angesetzt.
- Anpassungskosten (Fachanwendungen, Makros, Vorlagen, Add-ins): Ebenfalls 2.5 Mio. CHF sind für das Umschreiben bzw. Anpassen von Fachanwendungen, VBA-Makros, Vorlagen und Add-ins vorgesehen, die nicht kompatibel zu den OSS-Formaten (z. B. ODF) sind. Als Referenz dient die M365-Einführung und die damalige Anpassung der Fachapplikationen. Die Experten betonen, dass diese Schätzung ohne detaillierte Analyse jeder einzelnen Anwendung erfolgt und je nach tatsächlicher Komplexität nach oben oder unten abweichen kann.
- Schulung & Adoption: Den grössten Einzelposten bilden mit 3.9 Mio. CHF die Schulungs- und Adoptionskosten. Hier wird angenommen, dass, analog zur ursprünglichen M365-Einführung, bei der rund 1 Mio. CHF für die Adoption aufgewendet wurde, die gesamte Verwaltung erneut geschult werden muss. Grundlage ist eine Annahme von vier Schulungstagen pro Verwaltungsmitarbeitenden zu je 650 CHF pro Tag (direkte Schulungskosten und kalkulatorischer Arbeitszeitausfall). Dieser Block spiegelt die Erwartung wider, dass der Wechsel weg von der etablierten Microsoft-UX einen erheblichen

Change-Management-Aufwand nach sich zieht, welche zirka 1 Personentag-Schulung pro wesentlicher Komponentengruppe bedarf.
- Rekrutierungskosten für zusätzliches Engineering-Personal: Um den erwarteten Anstieg im Engineering- & Integrations-Team zu realisieren, geht die Untersuchungseinheit davon aus, dass 1–2 zusätzliche Fachpersonen rekrutiert werden müssen. Unter der Annahme von rund 30'000 CHF Rekrutierungskosten pro Person (Suche, Selektion, Onboarding) entstehen hierfür einmalige Zusatzaufwände von rund 60'000 CHF. Im Vergleich zu den übrigen Transformationsblöcken ist dieser Betrag zwar klein, für eine Organisation dieser Grösse aber nicht vernachlässigbar.

In Summe ergeben sich damit exemplarische direkte einmalige Transformationskosten von rund 9.0 Mio. Die heutigen, direkt zuordenbaren jährlichen M365 Kosten der Untersuchungseinheit liegen bei rund 1.255 Mio. CHF (Lizenzen, Backup/DR, Engineering, externe Unterstützung). Die geschätzten Transformationskosten entsprechen damit etwa dem sieben- bis achtfachen eines Jahresbudgets der aktuellen M365 Nutzung. Selbst wenn die laufenden Kosten einer OSS basierten Lösung langfristig leicht günstiger ausfallen würden, müssten diese einmaligen Investitionen über viele Jahre amortisiert werden.

Aus Sicht der befragten Experten ist ein Wechsel daher finanziell nur dann zu rechtfertigen, wenn strategische Motive wie digitale Souveränität, Risikoreduktion gegenüber Drittstaatszugriffen oder politische Vorgaben klar im Vordergrund stehen und bewusst höher gewichtet werden als kurzfristige Kostenvorteile.

3.5.4 Ergebnisse der Validierungs-Partner

Zur Validierung der im Rahmen der Untersuchungseinheiten gewonnenen Ergebnisse wurden mehrere weitere Organisationen befragt. Die Validierungspartner beantworteten einen standardisierten Fragenkatalog. Die Antworten bestätigen, die in den Untersuchungseinheiten identifizierten Muster in wesentlichen Punkten und schärfen zugleich die Einschätzung spezifischer Aspekte.

3.5.4.1 Technische Validierung

Die Validierungspartner zeigen insgesamt ein heterogenes, aber in Teilen vergleichbares Bild zur Nutzung von M365. Im Folgenden werden die wichtigsten Dienste differenziert dargestellt.

- Videokonferenzen und Chat: Teams wird von einem Teil der Validierungspartner als zentrale Lösung für Chat und Besprechungen eingesetzt, teils inklusive Telefonie. Andere Validierungspartner nutzen alternative Lösungen (z. B. Cisco-basierte Telefonie und Chat) und setzen Teams gar nicht oder nur ergänzend ein.
- E-Mail und Kalender: Bei den meisten Validierungspartner ist Exchange On-Premise nach wie vor die dominierende Plattform für Endbenutzer-Postfächer. Ein Validierungspartner nutzt vorwiegend Exchange Online für Endbenutzer-Postfächer.

- Dateiablage: Ein Validierungspartner nutzt ausschliesslich SharePoint Online. Zwei Validierungspartner nutzen SharePoint On-Premise, davon eine mit teilweiser SharePoint Online Nutzung für das Intranet. Zwei Validierungspartner haben SharePoint nicht im Einsatz. Nur eine Organisation hat OneDrive im Einsatz.
- Office-Applikationen: Alle Validierungspartner setzen weiterhin auf die klassischen Desktop-Clients von Word, Excel, PowerPoint und Outlook als primäres Arbeitsmittel. Bei einigen Validierungspartner ist zudem ein Zugang zu den Online-Varianten vorhanden.
- Low Code, Business Intelligence, und Automatisierung: Die meisten Validierungspartner nutzen Power Apps, Power BI und Power Automate nicht oder nur punktuell. Ein Validierungspartner nutzt Anwendungen dieser Kategorie umfassend und ein weiterer Validierungspartner plant die künftige Nutzung.
- Sicherheit und Compliance: Intune, Purview und Sentinel werden derzeit von den meisten Validierungspartner noch nicht eingesetzt. Einzelne Validierungspartner prüfen bzw. planen jedoch den zukünftigen Einsatz dieser Lösungen, etwa Purview für Sensitivity Labels, Intune für das Gerätemanagement oder Sentinel für erweitertes Security Monitoring. Insgesamt zeigt sich damit, dass diese Themen zwar punktuell an Relevanz gewinnen, im aktuellen Einsatzstand jedoch bei der Mehrheit der Validierungspartner noch keine breite Anwendung finden.

Die Nutzung von M365 ist bei den Validierungspartnern insgesamt sehr heterogen: Einige Organisationen setzen M365-Dienste (v. a. Teams, SharePoint Online, Exchange Online) bereits umfassend ein, andere nutzen weiterhin überwiegend On-Premise-Lösungen oder alternative Produkte. Insbesondere Funktionen wie Low Code, Business Intelligence, und Automatisierung sowie Security- und Compliance-Dienste (Intune, Purview, Sentinel) werden meist nur punktuell genutzt oder befinden sich erst in der Planungsphase.

Einschätzung bezüglich Herausforderungen bei einem Wechsel auf OpenDesk
Auf Basis des Fragebogens wurden verschiedene potenzielle Herausforderungen bei der Migration bewertet. Insgesamt ergibt sich folgendes Bild:

- Makros und Excel-Skripte: Alle Organisationen bewerten die Möglichkeit, dass Makros nicht vollständig migriert werden können, als problematisch bis kritisch. Insbesondere in Bereichen mit intensiver Makro-Nutzung (z. B. HR- und Verwaltungsabteilungen) wird dies als wesentliches Risiko bei einer Ablösung von M365 gesehen. Es wird von erheblichen Aufwänden für individuelle Anpassungen ausgegangen.
- SharePoint-spezifische Metadaten, Workflows und Versionsattribute: Ein Teil der Validierungspartner, in denen SharePoint-Workflows und Metadaten nur punktuell oder kaum genutzt werden, stuft das Risiko eines Verlusts als gering ein. Bei anderen Validierungspartner mit komplexen Workflow-Lösungen wären hingegen Neuentwicklungen mit beträchtlichem Aufwand verbunden.

- Teams- und Copilot-Chatverläufe: Teams-Chatverläufe werden überwiegend als wenig kritisch eingeschätzt. Copilot-Funktionen sind bei den meisten Validierungspartnern noch nicht produktiv im Einsatz, ein Wegfall wird entsprechend derzeit als unproblematisch betrachtet.
- Integrationen: Drei Validierungspartner verfügen über mehrere Integrationen in M365. Im Falle eines Wechsels wird es als wesentlich erachtet, dass viele dieser Anbindungen an Fachanwendungen neu entwickelt oder durch alternative Lösungen ersetzt werden müssten.
- Technische Rahmenbedingungen von OpenDesk: In mehreren Antworten wird hervorgehoben, dass für einen On-Premise-Betrieb von OpenDesk Kubernetes-Know-how erforderlich wäre. Manche Validierungspartner verfügen aktuell nicht über entsprechende Kompetenzen und bevorzugen daher alternative Plattformen (z. B. OpenShift). Zudem wird darauf hingewiesen, dass Open-Source-Software nicht automatisch sicher ist, sondern Sicherheitslücken aktiv geschlossen werden müssen.

Die Einschätzung zeigt, dass insbesondere die Migration von Makros/Excel-Skripten und bestehenden Integrationen in M365 als zentrale Risiken mit hohem Anpassungsaufwand gesehen werden. Demgegenüber werden der Wegfall von Teams- und Copilot-Chats wenig kritisch eingeschätzt, während für den Betrieb von OpenDesk vor allem fehlendes Kubernetes-Know-how und der aktive Umgang mit Sicherheitslücken in Open-Source-Software als zusätzliche Herausforderungen genannt werden.

3.5.4.2 Organisatorische Validierung

Die Validierungspartner bestätigen die in den Untersuchungseinheiten identifizierten Muster auch aus organisatorischer Sicht weitgehend, zeichnen je nach Ausgangslage aber ein differenziertes Bild. Während M365 insbesondere im Bereich des digitalen Arbeitsplatzes heute organisatorisch breit verankert ist, wird für ein openDesk-Szenario übergreifend ein höherer Bedarf an neuen Kompetenzen, stärkerer Architektur-Governance und aufwändigerer Lieferantensteuerung gesehen.

Im Folgenden werden die wichtigsten organisatorischen Themenfelder differenziert dargestellt.

- Organisatorische Verankerung von M365: Das Bild der heutigen organisatorischen Ausrichtung auf M365 fällt heterogen aus. Eine durchgängige Verankerung über die gesamte Organisation hinweg wird nur vereinzelt bestätigt. Verbreiteter ist eine ausgeprägte Verankerung im Bereich des digitalen Arbeitsplatzes (Kollaboration, Office), während in der übrigen IT-Landschaft zahlreiche weitere Technologien koexistieren. Mehrere Organisationen befinden sich zudem noch im Aufbau ihrer strategischen und Governance-Grundlagen. Mehrfach wird darauf hingewiesen, dass der strategische Kurs von Microsoft die Ausrichtung künftig stärker in Richtung M365 verschiebt, auch dort, wo heute noch OnPremise-Lösungen dominieren.
- Kompetenzprofil der IT-Teams: Die Mehrheit der Validierungspartner erwartet, dass ein Wechsel auf openDesk einen relevanten Auf- bzw. Umbau der Kompetenzprofile in den IT-

Teams erfordern würde. Wo die Lücken liegen, wird unterschiedlich beurteilt: Teils sind Infrastruktur-Kompetenzen (z. B. Linux, Container-Plattformen) bereits vorhanden, während openDesk-spezifisches sowie Integrations-Know-how (Schnittstellen, API- und Middleware-Ebene) als fehlend benannt wird. Vereinzelt wird weniger der technische als der rechtliche Kompetenzbedarf hervorgehoben, insbesondere hinsichtlich der Lizenzmodelle im Open-Source-Umfeld. Der Bedarf an zusätzlichen Kompetenzen wird damit breit bestätigt, betrifft je nach Organisation aber unterschiedliche Schwerpunkte.

- Architektur- und Technologie-Governance: Überwiegend wird erwartet, dass eine openDesk-basierte Lösung den Bedarf an klaren Architektur- und Technologievorgaben (z. B. Referenzarchitektur, Standard-Stacks, Freigabeprozesse) erhöht. Der mit der Lösung verbundene Zugewinn an architektonischer Flexibilität wird demgegenüber zurückhaltender und teils ausdrücklich getrennt vom gestiegenen Steuerungsbedarf beurteilt. Offene Schnittstellen und Datenformate werden als zentraler potenzieller Vorteil hervorgehoben, dessen konkrete Ausprägung im Einzelfall jedoch noch nicht abschliessend beurteilt werden kann.
- Erwartete Dienstleisterlandschaft für openDesk: Die Mehrheit teilt die Einschätzung, dass der Markt an Dienstleistern und Fachexperten für eine openDesk-basierte Lösung kleiner ausfällt und daraus ein erhöhtes organisatorisches Risiko entstehen kann. Für einzelne Komponenten bestehen bereits Anbieter; das Ökosystem rund um die integrierte Suite gilt jedoch als noch im Aufbau und in seiner Tragfähigkeit abhängig von der weiteren Verbreitung sowie davon, dass sich Anbieter gezielt auf openDesk ausrichten. Im Vergleich wird das Microsoft-Ökosystem als deutlich grösser eingeschätzt; zugleich wird die geringere Bindung an einen einzelnen Anbieter gegenüber einem Single-Vendor-Modell als Vorteil anerkannt.
- Supplier Management bei openDesk: Mehrheitlich wird erwartet, dass sich die Lieferantensteuerung bei einem Wechsel auf openDesk komplexer gestaltet, da neben einer zentralen Trägerorganisation ggf. mehrere spezialisierte Drittanbieter für Hosting, Integration, Betrieb und Support einzubinden und zu koordinieren wären. Das Ausmass wird jedoch stark vom gewählten Betriebsmodell und der Integrationstiefe abhängig gemacht: Ein SaaS-Bezug «aus einer Hand» über eine Trägerorganisation reduziert den Koordinationsaufwand, während ein selbst betriebenes oder tief integriertes Modell ihn erhöht. Ergänzend wird die sicherheitstechnische Prüfung von Updates als anspruchsvolle Zusatzaufgabe genannt. Vereinzelt wird der Zuwachs beim eigentlichen Lieferantenmanagement als überschaubar eingestuft, dafür aber ein deutlich höherer interner Betriebs- und Integrationsaufwand erwartet.

Insgesamt bestätigen die Validierungspartner die organisatorische Grundtendenz der Untersuchungseinheiten: Ein Wechsel verschiebt ggf. die Rolle der internen IT tendenziell vom Service-Konsumenten zum Service-Integrator und erhöht die Anforderungen an Kompetenzen, Architektur-Governance und Lieferantensteuerung. Wie stark diese Effekte ausfallen, hängt massgeblich von der Ausgangslage, dem gewählten Betriebsmodell und

der Integrationstiefe ab; ein Teil der Mehraufwände verlagert sich dabei von der reinen Vendor-Koordination in den internen Betrieb.

3.5.4.3 Regulatorische Validierung

Die Validierungspartner zeigen ein heterogenes, in den strukturellen Kernfragen jedoch konvergentes Bild der regulatorischen Ist-Situation. Im Folgenden werden die wichtigsten Themenfelder differenziert dargestellt.

- Politische Legitimation: Die Mehrheit der Validierungspartner verfügt über einen formellen Regierungsratsbeschluss mit expliziter Risikoakzeptanz. Eine Organisation stützt sich auf themenspezifische Teilbeschlüsse ohne ausdrückliche Gesamt-Risikoakzeptanz. Eine durchgängig formalisierte Risikoakzeptanz auf Regierungsebene ist damit verbreitetes, aber nicht universelles Modell.
- Konsultation der Datenschutzaufsicht: Alle Validierungspartner haben die zuständige kantonale bzw. städtische Datenschutzaufsicht formell konsultiert, durchgängig verbunden mit Auflagen oder Vorbehalten. Die Datenschutzstellen agieren gestaltend-begleitend mit. Bei mehreren Organisationen ist der Handlungsspielraum für tiefere Schutzbedarfsklassen noch im Aufbau.
- Klassifikationsrestriktionen: Das Bild reicht von klarem Ausschluss höherer Vertraulichkeitsstufen mit operativ durchgesetzter Klassifikation (Freigabe bis und mit «vertraulich» bzw. «intern») über teilweise bestehende, aber noch nicht formell verankerte Einschränkungen bis hin zum vollständigen Fehlen eines im M365-Kontext anwendbaren Klassifikationssystems. Wo Klassifikationsregimes bestehen, wird deren konsistente operative Durchsetzung übergreifend als zentrale Herausforderung benannt.
- Schlüsselhoheit: Bei der Mehrheit der Validierungspartner liegt die Schlüsselverwaltung beim Anbieter, vereinzelt wird ein Customer Managed Keys flächendeckend eingesetzt. Eigene Schlüsselhoheit wird einerseits als Voraussetzung für höhere Vertraulichkeitsstufen anerkannt, andererseits wird auf funktionale Einschränkungen in kollaborativen Szenarien hingewiesen.
- Blaulichtorganisationen: Mehrheitlich besteht eine separate regulatorische Beurteilung. Kritische Daten werden teils ausschliesslich in On-Premise-Fachsystemen bearbeitet. Sektorspezifische Einschränkungen (insb. polizeiliche Vollzugsprozesse) werden anerkannt, die operative Abgrenzung ist jedoch nicht durchgängig trennscharf. Systematische technische Alternativlösungen bestehen nur teilweise, primär über bestehende Fachanwendungen, mehrere Organisationen arbeiten mit Behelfslösungen.
- Politischer Druck: Die Ausprägung reicht von regelmässigen parlamentarischen Vorstössen Druck bis zu bislang keinem nennenswerten politischen Druck. Inhaltlich verlagert sich der Diskurs zunehmend von klassischen Datenschutzfragen hin zu Fragen der digitalen Souveränität.

Die regulatorische Tragfähigkeit der M365-Nutzung hängt bei den Validierungs-partnern weniger an der Plattformwahl als an der Reife der Steuerungsinstrumente: formelle Risikoakzeptanz, durchgesetzte Klassifikation, Schlüsselhoheit und belastbare Exit-Konzepte. Während politische Legitimation und Aufsichtskonsultation überwiegend etabliert sind, bleiben Klassifikationsdurchsetzung und Schlüsselhoheit organisationsübergreifend eine Herausforderung.

Einschätzung bezüglich regulatorischer Wirkung eines Wechsels auf eine Alternativlösung

Auf Basis des Fragebogens wurde die regulatorische Reduktionswirkung eines Wechsels auf eine Alternativlösung sowie die Priorisierung der Auswahlkriterien bewertet. Insgesamt ergibt sich folgendes Bild:

- Reduktion von Rechtsrisiken durch Hosting- und Rechtsraumwahl: Die Mehrheit der Validierungspartner bestätigt, dass ein Hosting in der Schweiz bzw. EU ohne direkte US-Vertragsbeziehungen bestimmte Rechtsrisiken (z. B. Behördenzugriffe) reduzieren könnte. Die Reduktionswirkung setzt voraus, dass keine Organisation mit niedrigerem Datenschutzniveau in der Verarbeitungskette enthalten ist.
- Risikoexposition: Im aggregierten Ranking zu den für die Organisationseinheiten wichtigsten Attribute einer Alternativlösung dominieren Vertraulichkeit und Einschränkung des Zugriffs durch ausländische Behörden (Lawful Access), gefolgt von Kontrollrechten über Daten und Schlüssel sowie Verfügbarkeit (insbesondere im Blaulichtbetrieb). Vendor Lock-in und Betriebssouveränität werden anerkannt, in der Priorisierung jedoch tendenziell nachgelagert.
- Bewertungskriterien für eine M365-Alternative: Mehrheitlich unter die Top-5 priorisiert werden funktionale Parität mit M365, Integrationsfähigkeit in bestehende Systeme und Fachanwendungen, Hosting-Standort (CH/EU), Kosten (Betrieb und Migration) sowie Verfügbarkeit von Fachpersonal und Dienstleistern. Ergänzend mehrfach genannt werden Exitfähigkeit, Sicherheitsfunktionalität sowie Krisenbetrieb und Resilienz. Rechtsstaatliche Zugriffsgarantien und Datenhoheit/Schlüsselkontrolle werden nur von einem Teil der Validierungspartner unter die Top-5 gesetzt.

Die regulatorische Reduktionswirkung einer Alternativlösung tritt nur unter qualifizierten Hosting- und Vertragsbedingungen ein und wird in der konkreten Auswahlentscheidung von funktionalen und betrieblichen Kriterien überlagert.

3.5.4.4 Finanzielle Validierung

Die Validierungspartner bestätigen die finanziellen Grundmuster der Untersuchungseinheiten, weisen aber auf eine erhebliche Bandbreite und eine teils eingeschränkte Schätzbarkeit hin. Mehrere Aussagen sind ausdrücklich vom Projektscope, vom Betriebsmodell und von der

politischen Risikoabwägung abhängig. Im Folgenden werden die wichtigsten finanziellen Themenfelder differenziert dargestellt.

- Kostenstruktur der heutigen M365-Nutzung: Die Mehrheit der Validierungspartner bestätigt eine lizenzgetriebene Kostenstruktur in der vom Studienmodell angenommenen Grössenordnung, mit den Lizenzen als grösstem Block, gefolgt von internem Personalaufwand und externen Dienstleistungen. Abweichungen ergeben sich vor allem bei stark On-Premise-geprägten Organisationen, bei denen der Personalaufwand einen grösseren Anteil einnimmt, sowie dort, wo die direkt M365-bezogenen Kosten nur einen kleinen Teil eines breiteren IT-Budgets ausmachen. Insgesamt stützt das Bild die Annahme, dass reine Lizenzpreisvergleiche zu kurz greifen und Betrieb, Personal sowie ergänzende Dienste einzubeziehen sind.
- Laufende Kosten einer Alternative: Bei den laufenden jährlichen Gesamtkosten einer Alternative wie openDesk reicht das Bild von etwas höher über ungefähr gleich bis deutlich niedriger; mehrheitlich werden sie als in etwa vergleichbar mit der heutigen M365-Lösung eingeschätzt. Dies bestätigt die Einschätzung der Untersuchungseinheiten, wonach sich die laufenden Kosten beider Lösungen in einer ähnlichen Grössenordnung bewegen.
- Einmalige Transformationskosten: Die Einschätzung der einmaligen Transformationskosten ist heterogen und von erheblicher Unsicherheit geprägt; mehrere Validierungspartner sehen sich derzeit nicht in der Lage, eine belastbare Schätzung abzugeben. Massgeblich ist der Projektscope, insbesondere ob eine Gesamtmigration erfolgt oder primär neue Services parallel aufgebaut werden und ob bestehende Lizenzen (z. B. Office, Exchange- oder SharePoint-Server) weiter anfallen. Soweit eine Schätzung erfolgt, werden die Transformationskosten auf mindestens ein bis zwei, teils mehr als zwei M365-Jahreskosten beziffert. Die Validierung bestätigt damit die Richtung substanzieller, dominierender Einmalkosten, deren konkrete Höhe jedoch stark vom gewählten Vorgehen abhängt.
- Schulungsaufwand: Die Schätzungen zum Schulungsaufwand pro Mitarbeitenden variieren deutlich, von weniger als einem Tag bis zu mehreren Tagen. Mehrfach wird zwischen formalem Schulungsaufwand (tendenziell tiefer) und verstecktem Aufwand für die Einarbeitung im Arbeitsalltag (tendenziell höher) unterschieden. Teilweise sollen Grundlagen über eLearning-Module im Rahmen der individuellen Weiterbildung vermittelt werden. Die Bandbreite verdeutlicht, dass der Schulungs- und Change-Aufwand ein relevanter, methodisch aber unterschiedlich angesetzter Projektkostenblock ist.
- Zahlungsbereitschaft für Souveränität: Die Bereitschaft, dauerhaft einen Mehrbetrag für digitale Souveränität zu tragen, ist heterogen und vielfach noch nicht abschliessend geklärt. Das Bild reicht von keiner Bereitschaft zu Mehrkosten über eine Bereitschaft von bis zu rund 20 Prozent jährlicher Mehrkosten bis hin zu Organisationen, die dies derzeit nicht beurteilen können. Mehrfach wird betont, dass es sich letztlich um eine politische Entscheidung handelt, die noch zu treffen ist, oder dass mittel- bis langfristig eher Einsparungen als Mehrkosten erwartet werden. Dies bestätigt die Einschätzung, dass ein Wechsel als bewusst getragene, politisch zu legitimierende Investition zu verstehen ist.
- Planbarkeit der Kosten: Mehrheitlich wird erwartet, dass sich die Gesamtkosten einer Alternative langfristig mindestens ebenso gut planen und steuern lassen wie jene von M365. Als Gründe werden eine klare Projekt- und Zielsteuerung sowie ein grösserer Einfluss auf die

Anbieterin genannt. Einschränkend wird darauf hingewiesen, dass dies die Wahrung der Kompatibilität und den Fortbestand des Produkts voraussetzt. Eine Organisation beurteilt die Planbarkeit zurückhaltender.

3.6 Risiken

Die nachfolgenden Ausführungen erläutert die im Rahmen dieser Studie erkannten Risiken.

Im Rahmen der vorliegenden Studie wurde bewusst auf eine einheitliche numerische Bewertung der Risiken (z. B. 1–5) verzichtet. Die beschriebenen Risiken sind stark von der jeweiligen Ausgangslage und Risikokultur der einzelnen Verwaltungseinheiten abhängig.

Die konkrete Einstufung (z. B. Eintrittswahrscheinlichkeit und Auswirkung auf einer Skala von 1–5) soll durch die zuständigen Organisationen selbst vorgenommen werden, basierend auf ihren eigenen Risikomatrizen und Governance-Prozessen. Die vorliegende Studie liefert hierfür die strukturierte Grundlage und benennt erkannte Risiken.

3.6.1 Dynamische Lizenz- und Preismodelle

Weder bei Microsoft noch bei OSS-basierten Alternativen sind Lizenz- und Servicepreise langfristig stabil:

- M365: Die Einführung neuer Angebotsvarianten (z. B. des E7-Angebots) sowie laufende Anpassungen von Funktionsbündeln und Preisstrukturen zeigen, dass Microsoft sein Lizenzportfolio regelmässig weiterentwickelt. Dies betrifft sowohl die inhaltliche Zusammenstellung der Pakete als auch die Preisgestaltung und die Zuordnung von Funktionen zu Lizenzstufen.
- openDesk / Alternativen: Bei openDesk sind zum Zeitpunkt des Verfassens der Studie Verhandlungen mit potenziellen Schweizer Hosting-Partnern im Gange; sowohl Lizenz- als auch Hosting-Komponenten befinden sich noch in einer Phase der Marktreifung. Wie bei jungen wie etablierten Angeboten gleichermassen ist davon auszugehen, dass sich Preise und Geschäftsmodelle im Zuge der weiteren Marktentwicklung verändern können.
- Einfluss neuer KI-Funktionalitäten: KI-basierte Funktionen werden den digitalen Arbeitsplatz voraussichtlich wesentlich prägen. Erste Angebote werden bereits über zusätzliche Lizenzstufen oder optionale Module vermarktet. Es ist zu erwarten, dass zukünftige Produktivitätsgewinne stark von solchen KI-Erweiterungen abhängen und damit auch neue, heute noch schwer prognostizierbare Lizenz- und Preismodelle entstehen, die preislich ggf. wesentlich über die bestehenden Basispakete hinausgehen. Für die Budgetplanung entsteht dadurch eine Unsicherheit: Solche KI-Funktionen werden bereits heute teils als kostenpflichtige Zusatzstufen und nicht als Bestandteil der Basispakete angeboten, sodass eine flächendeckende Ausrollung die Arbeitsplatzkosten über das heutige Niveau hinaus erhöhen kann. Der künftige Funktionsumfang und die zugehörigen Preismodelle sind zum jetzigen Zeitpunkt nicht verlässlich abschätzbar.

Damit wird deutlich: Weder beim Verbleib auf M365 noch bei einem Wechsel zu openDesk können heutige Preisniveaus als dauerhaft gesichert betrachtet werden. Die Kostenentwicklung,

insbesondere im Zusammenhang mit neuen KI-Leistungen, bleibt in beiden Fällen ein Steuerungsgegenstand, der regelmässig zu überprüfen ist.

3.7 Projektrisiken (Migration / Exit)

Bei einem Exit-Szenario hin zu einer alternativen Plattform entstehen klassische Projektrisiken:

- Termin- und Budgetrisiken: Ein Umstieg kann länger dauern und teurer werden als geplant (z. B. komplexere Datenmigration, zusätzliche Integrationsaufwände, höherer Schulungsbedarf).
- Scope-Risiken: Während des Projekts können neue Anforderungen auftauchen oder bisherige Annahmen (z. B. zur Funktionsparität) sich als unvollständig erweisen. Ebenso können regulatorische Änderungen während der Projektlaufzeit zusätzliche Anforderungen an Datenhaltung, Security oder Auditierbarkeit nach sich ziehen und dadurch den Leistungsumfang verändern.
- Ressourcenrisiken: Engpässe bei internen Schlüsselpersonen oder externen Spezialisten (insbesondere OSS-/openDesk-Expertise) können den Projektverlauf verzögern.
- Qualitätsrisiken: Im Rahmen der Migration können Datenverluste, Dateninkonsistenzen oder die fehlerhafte Übernahme von Berechtigungen auftreten. Zudem besteht das Risiko unzureichender Nachvollziehbarkeit bzw. Auditierbarkeit nach der Migration (z. B. lückenhafte Protokollierung).

3.8 Betriebliche Risiken und Verschiebung des Risikotyps

Für eine Gesamtbewertung ist es hilfreich, zwei Risikodimensionen klar zu trennen:

1. Souveränitäts- und Rechtsrisiken (z. B. Lawful Access, Datenstandort, Einflussmöglichkeiten auf Produktentwicklung),
2. Betriebs-, Stabilitäts- und Cyberrisiken (z. B. Komplexität der Architektur, Integrationsaufwand, Reifegrad des Betriebsmodells, Cybersicherheitsniveau und Eignung für den Enterprise-Einsatz).

Diese beiden Risikotypen sind grundsätzlich unabhängig voneinander:

Eine lokal gehostete, sehr souveräne Lösung (z. B. openDesk in einer Schweizer oder hoheitlich kontrollierten Umgebung) kann Souveränitätsrisiken reduzieren, gleichzeitig könne diese Lösung theoretisch ein höheres Betriebsrisiko aufweisen, etwa durch:

- erhöhte Integrationskomplexität (Security-Stack, IAM, Backup),
- geringere Marktreife im Massenbetrieb,
- zusätzliche Abhängigkeit von kleineren Hosting- und Integrationspartnern.

Eine international betriebene Hyperscaler-Lösung wie M365 könnte demgegenüber:

- ein sehr hohes Niveau an Betriebsstabilität, Cybersicherheit und Skalierbarkeit bieten, beispielsweise durch die nahtlose Weiterführung des Betriebs in redundanten Umgebungen,
- gleichzeitig aber höhere Souveränitäts- und Rechtsrisiken mit sich bringen (insbesondere im Kontext von Drittstaatszugriffen und eingeschränkter Einflussnahme auf die Roadmap).

Ein Wechsel von M365 zu einer Alternative wie openDesk bedeutet somit keine automatische Risikoabnahme sondern lediglich ein veränderte Risikoexposition.

3.8.2 M&A-Risiko und Marktdynamik

Der Markt für Workplace-Suiten und integrierte Kollaborationsplattformen ist zwar überschaubar, dennoch bestehen relevante Dynamiken:

- Firmenübernahmen und Fusionen: Ein Anbieter kann verkauft werden, neue Eigentümer können Strategie, Preispolitik oder Umgang mit Souveränität und Datenschutz ändern. Entsprechende Fälle, in denen etablierte Open-Source-Lösungen im Zuge einer Übernahme unter die Kontrolle eines grossen proprietären Anbieters gelangten, sind in der Vergangenheit aufgetreten.[8] Umgekehrt existieren Governance-Modelle, die gezielt gegen solche Übernahmerisiken absichern: So ist etwa der Anbieter Infomaniak in eine Stiftungsstruktur eingebettet, die eine feindliche Übernahme erschweren und die langfristige strategische Unabhängigkeit schützen soll.[9]
- Veränderung von Lizenz- und Geschäftsmodellen: Produkte oder einzelne Komponenten können stärker proprietär werden, Funktionen können in höhere Lizenzstufen verlagert oder eingestellt werden.
- Konsolidierung und Marktaustritte im Ökosystem: Insbesondere kleinere Dienstleister im Umfeld von openDesk oder anderen OSS-basierten Lösungen können ihr Portfolio ändern oder vom Markt verschwinden, was die Verfügbarkeit von Know-how beeinflusst. Vergleichbare Konsolidierungs- und Marktaustrittsrisiken bestehen grundsätzlich auch im Microsoft-Ökosystem, etwa bei spezialisierten Implementierungs- und Integrationspartnern. Bei einem noch jungen und weniger dicht besetzten Anbieterumfeld wirken sich solche Bewegungen jedoch stärker auf die verfügbare Know-how-Basis aus.

3.8.3 Risiko der Benutzerakzeptanz und Nutzerfreundlichkeit

Ein wesentliches Risiko betrifft die Akzeptanz eines neuen Arbeitsplatzes durch die Mitarbeitenden. Viele Nutzerinnen und Nutzer sind aus dem privaten Umfeld an Microsoft-Oberflächen gewöhnt. Ein Wechsel auf eine anders gestaltete Suite führt erfahrungsgemäss zu Umgewöhnung und vorübergehenden Produktivitätseinbussen, unabhängig davon, ob die neue Lösung technisch oder strategisch Vorteile bietet, Vergleichbare Effekte treten im Übrigen nicht nur beim Wechsel des Anbieters auf, sondern ebenso bei grösseren Versionssprüngen innerhalb derselben Suite, etwa bei einer grundlegend überarbeiteten Benutzeroberfläche. Die Umgewöhnung ist damit weniger eine Frage der Abkehr von einem bestimmten Anbieter als vielmehr eine generelle Begleiterscheinung wesentlicher Veränderungen der Arbeitsumgebung. Bleibt diese Umgewöhnung unzureichend begleitet, besteht das Risiko, dass Funktionen als umständlicher wahrgenommen werden und die Umstellung länger dauert als erforderlich. Entscheidend ist daher nicht, ob eine Umstellung

[8] Europäische Kommission, Fusionskontrolle: Kommission gibt geplante Übernahme von Sun Microsystems durch Oracle frei, URL: ec.europa.eu/commission/presscorner/detail/en/ip_10_40, abgerufen am 14. August 2026.
[9] Infomaniak, Infomaniak secures its independence and its DNA for the long term, URL: https://news.infomaniak.com/en/infomaniak-foundation-sovereign-cloud/, abgerufen am 14. August 2026.

Akzeptanzfragen aufwirft, sondern wie sie durch geeignete Begleitmassnahmen aufgefangen wird.

In der Diskussion und Entscheidungen um Alternativen zu M365 wird dieses Risiko (wie in dieser Studie) tendenziell aus einer fachlichen Perspektive von Fachpersonen betrachtet. Die Sicht der „ganz normalen“ Mitarbeitenden, mit ihren alltäglichen Arbeitsabläufen, Erwartungen und Gewohnheiten, ist relevant für die Mitigation dieses Risikos.

3.8.4 Cybersicherheitsrisiken

Ein Wechsel von M365 zu einer alternativen Plattform verändert nicht nur das Souveränitäts- und Betriebsmodell, sondern auch das Cybersicherheitsprofil der Organisation. Dabei ist wichtig festzuhalten, dass weder M365 noch eine Alternative per se „sicher“ oder „unsicher“ ist. Vielmehr verschieben sich die sicherheitsrelevanten Verantwortlichkeiten, Angriffspunkte und Steuerungsmechanismen. Insbesondere sind folgende Cybersicherheitsrisiken zu berücksichtigen:

- Erhöhte Komplexität der Sicherheitsarchitektur: Während bei M365 viele Sicherheitsfunktionen auf einer gemeinsamen Plattform mit konsistenten Identitäten, Rollenmodellen und Telemetriedaten basieren, erfordert eine alternative Zielarchitektur häufig die Kombination mehrerer Produkte und Anbieter. Diese höhere Modularität kann strategische Vorteile bringen, erhöht aber gleichzeitig die Komplexität bei Härtung, Konfiguration, Monitoring, Incident Response und Patch-Management. Schnittstellen zwischen den Komponenten können dabei selbst zu zusätzlichen Angriffsflächen werden.
- Abhängigkeit von lokaler Betriebs- und Integrationsfähigkeit: Mit zunehmender Eigenverantwortung für Hosting, Integration und Sicherheitsorchestrierung steigt die Bedeutung der internen und externen Betriebsfähigkeiten. Sicherheitslücken, Fehlkonfigurationen oder verzögerte Reaktionen auf Schwachstellen können sich stärker auf das Gesamtrisiko auswirken, wenn Schutzmechanismen nicht durch einen breit industrialisierten Plattformbetrieb mitgetragen werden. Der Sicherheitsstandard hängt damit stärker von der Qualität des gewählten Betriebsmodells, der Hoster, Integrationspartner und der eigenen Governance ab.
- Risiken im Schwachstellen- und Patch-Management: In einer stärker modularen Open-Source-basierten Umgebung müssen sicherheitsrelevante Updates verschiedener Komponenten koordiniert, getestet und zeitgerecht eingespielt werden. Auch wenn offene Komponenten grundsätzlich transparent und gut überprüfbar sein können, entsteht das Risiko, dass Schwachstellenmanagement, Dependency-Tracking und Patch-Prozesse organisatorisch anspruchsvoller werden als in einer stark standardisierten SaaS-Plattform.
- Unterschiede in Detektions- und Reaktionsfähigkeit: Ein zentrales Risiko besteht darin, dass die Erkennung von Sicherheitsvorfällen und die koordinierte Reaktion auf Angriffe in einer alternativen Umgebung zunächst weniger ausgereift oder weniger durchgängig integriert sein kann. Dies betrifft insbesondere die Korrelation von Ereignissen über Identitäten, Endgeräte, E-Mail, Dateiablagen und Kollaborationsdienste hinweg. Ohne zusätzliche Investitionen in Logging, SIEM/SOC-Anbindung, Alarmierung und Response-Prozesse kann die Fähigkeit zur frühzeitigen Erkennung und wirksamen Eindämmung von Angriffen sinken.

- Cyberrisiken während der Migrations- und Parallelbetriebsphase: Besonders erhöht ist die Cyberrisikoexposition während der Transition. In Migrationsphasen bestehen temporär parallele Identitäten, doppelte Datenhaltungen, neue Schnittstellen, Übergangskonfigurationen und provisorische Betriebsprozesse. Diese Übergangssituation kann zu zusätzlichen Schwachstellen, unklaren Verantwortlichkeiten und erhöhter Angriffsfläche führen. Die Migrationsphase ist daher nicht nur ein Projekt-, sondern auch ein eigenständiges Sicherheitsrisiko.
- Lieferketten- und Drittparteirisiken: Bei modularen Zielarchitekturen verteilt sich die Sicherheitsverantwortung stärker auf mehrere Akteure, etwa Produktanbieter, Hosting-Partner, Integratoren und Komponentenhersteller. Dadurch steigen die Anforderungen an die Sicherheitsprüfung und Steuerung der Lieferkette. Sicherheitsmängel oder Verzögerungen bei einzelnen Partnern können sich unmittelbar auf die Gesamtlösung auswirken.

3.9 Fazit

Die Analyse zeigt, dass M365 heute weit mehr als eine einzelne Anwendung ist: Es handelt sich um ein breites und tiefes Ökosystem aus u.a. Kollaboration, Sicherheit, Identität, Compliance und Automatisierung, welche tief in organisatorische, technische und unternehmensarchitektonische Aspekte integriert sind. Gerade diese Vielseitigkeit des Ökosystems macht den Betrieb effizient, erschwert aber gleichzeitig einen 1:1-Ersatz auf technischer, organisatorischer und finanzieller Ebene.

openDesk als Beispiel einer Alternative zu M365 erweist sich als eine interessante Alternative mit Stärken bei einzelnen Aspekten der digitalen Souveränität, insbesondere bei Offenheit und Einflussmöglichkeiten auf die Weiterentwicklung. Aufgrund des jüngeren Ökosystems und der noch offenen Finanzierungs- und Betriebsstrukturen bei openDesk bestehen hinsichtlich Verfügbarkeit, langfristiger Planungssicherheit und Zukunftsfähigkeit noch grössere Unsicherheiten als bei etablierten Lösungen. Die Studie macht deutlich, dass eine heutige, vollständige Ablösung von M365 mit erheblichen Transformationsaufwänden verbunden wäre. Aus heutiger Sicht wäre ein solcher Schritt nur im Rahmen eines bewusst gefällten, politisch getragenen Entscheids vertretbar, inklusive der Bereitschaft, Mehrkosten, Stillstand oder gar Rückschritte bei der Digitalen Transformation in Kauf zu nehmen.
Finanziell verschiebt sich der Schwerpunkt bei einem Wechsel weg von lizenzierten Komplettservices hin zu stärker personal- und integrationsgetriebenen Betriebsaufwänden. Dabei ist zu berücksichtigen, dass Investitionen in Hosting- und Dienstleistungsstrukturen in der Schweiz einen Teil der Wertschöpfung in die heimische Wirtschaft verlagern und damit industrie- und standortpolitische Effekte entfalten können. Aus einer übergeordneten, staatlichen Perspektive kann die Bewertung dabei anders ausfallen als aus Sicht einer einzelnen Verwaltungseinheit: Einmalkosten liessen sich allenfalls föderal koordiniert tragen, während sich mögliche Wertschöpfungs- und Souveränitätseffekte erst gesamthaft entfalten. Ob und in welchem Umfang sich daraus tatsächlich Vorteile ergeben, wäre politisch zu diskutieren.

Insgesamt verdeutlicht die Studie: Die Frage „M365 beibehalten oder Alternativen stärken?“ ist weniger eine rein technische Abwägung, sondern eine strategische Weichenstellung zwischen

Effizienz des etablierten Ökosystems und dem gezielten Aufbau digitaler Souveränität. Welche Option gewählt wird, ist letztlich eine politische Entscheidung. Der Aufbau digitaler Souveränität gelingt dabei in vielen Bereichen wirtschaftlicher und tragfähiger, wenn Gemeinwesen ihr Vorgehen aufeinander abstimmen, statt es einzeln zu beschreiten. Wo die erforderlichen Investitionen, der Kompetenzaufbau oder die Bündelung der Nachfrage die Möglichkeiten eines einzelnen Gemeinwesens übersteigen, liegt die Antwort nicht im Verzicht auf Souveränität, sondern in koordinierter Zusammenarbeit über die föderalen Ebenen hinweg und im Zusammenwirken mit der Wirtschaft als Angebotsseite. Eine abgestimmte Nachfrage schafft das erforderliche Mengengerüst und sichert die langfristige Verfügbarkeit tragfähiger Lösungen, ohne den Raum für Wettbewerb, Experimente und lokale Innovation einzuschränken. Arbeit liefert eine sachliche Grundlage, um diese bewusst und informiert treffen zu können.

3.10 Ausblick

Die vorliegende Studie hat bewusst ein klares Alternativ-Szenario („all-or-nothing“) betrachtet, um die Konsequenzen einer vollständigen Ablösung von M365 durch eine Alternative wie openDesk sichtbar zu machen. Dies schliesst jedoch andere, graduelle Entwicklungspfade nicht aus.

Zwischen einem vollständigen Verbleib im M365-Ökosystem und einer vollständigen Alternative liegen mehrere Zwischenoptionen. Denkbar sind beispielsweise Szenarien, in denen:

- einzelne Funktionsbereiche (z. B. Dateiablage, Kollaboration, bestimmte Kommunikationsdienste) schrittweise durch souveräne Alternativen ersetzt werden, während andere Komponenten vorerst bei M365 verbleiben
- sensible Daten vermehrt lokal oder in einer Schweizer Cloud gehalten werden, während die Benutzer weiterhin mit vertrauten Werkzeugen wie Word, Excel oder PowerPoint arbeiten
- hybride Modelle etabliert werden, bei denen M365 bewusst auf Kernfunktionen reduziert und parallel eine souveräne Umgebung aufgebaut wird, die bei Bedarf weiter ausgebaut werden kann.

Solche Mischszenarien wurden im Rahmen dieser Anschlussstudie nicht im Detail analysiert, erscheinen aber als naheliegende nächste Fragestellung. Sie könnten es ermöglichen, digitale Souveränität schrittweise zu stärken und gleichzeitig die Benutzerakzeptanz zu sichern, indem bewährte Werkzeuge dort weitergenutzt werden, wo dies fachlich, finanziell, technisch und regulatorisch vertretbar ist.

Anhang A: Weitere Informationen zu openDesk

Integrationen und Migrationsfähigkeit
Die openDesk Lösung setzt auf offene Standards (REST, OIDC/OAuth, LDAP, WebDAV, CalDAV/CardDAV), sodass individuelle Integrationen von Fachanwendungen möglich sind. Da es keine 1:1-Entsprechungen zur Microsoft-Welt gibt, erfordert jede Integration eine individuelle Bedarfsanalyse, auf deren Basis die Umsetzung geplant wird. Microsoft-spezifische Integrationen (z. B. SharePoint-Anbindungen) erfordern in der Regel individuelle Entwicklungen oder Adapterlösungen. Beispielsweise sind folgende Integrationen möglich:
- SSO-Integration: Fachanwendungen können über Keycloak/Nubus ins SSO eingebunden werden.
- Datei-Integration: Nextcloud WebDAV-Schnittstelle ermöglicht direkte Einbindung in viele Anwendungen.
- E-Mail/Kalender: Standard-IMAP/CalDAV/CardDAV-Schnittstellen für bestehende Anwendungen.
- Windows Explorer: Nextcloud als Netzlaufwerk einbindbar.
- Bei der Anbindung von KI-Diensten setzt openDesk auf Flexibilität: Betreiber können sowohl lokale als auch externe Sprachmodelle einbinden.

openDesk enthält kein natives PSTN-Angebot im Standard-Paket. Jitsi (Videokonferenz-Komponente via Nordeck) integriert die SIP-Komponente „Jigasi", über die eine Einwahl per Telefon möglich ist, vorausgesetzt, ein externer SIP-Server und SIP-Trunk werden bereitgestellt (durch den Betreiber oder einen Telefondienstleister).

openDesk bietet mit offenen Standards Flexibilität bei der Integration verschiedenster Fachanwendungen und Dienste. Jede Integration erfordert jedoch eine individuelle Bedarfsanalyse, auf deren Basis die Umsetzung geplant werden kann. Spezifische Integrationen können individuelle Entwicklungen oder Adapterlösungen erfordern.
Bei einer Migration von M365 zu openDesk ist eine detaillierte Planung und Anforderungsanalyse notwendig, um Informationsverluste zu minimieren. Folgende Übersicht gibt eine grundsätzliche Einordnung der Migrationsfähigkeit verschiedener Daten entlang der Funktionsbereiche:
- Kommunikation und Kollaboration:
  - Es gibt Migrationspfade von Microsoft Exchange/Outlook zu OX AppSuite. Eine verlustfreie Migration von E-Mail- & Kalender-Inhalten und Ordnerstrukturen ist grundsätzlich möglich.
  - Teams-Chatverläufe lassen sich nicht verlustfrei in Element (Matrix) übertragen. Es ist kein unterstützter Migrationspfad vorhanden.
- Produktivitäts- und Geschäftsanwendungen:
  - Microsoft Office-Formate (.docx, .xlsx, .pptx) werden von Collabora Online unterstützt. Gewisse Formatierungen (bspw. Einzelne Schriften oder Layouts) können zum Teil nicht oder nur mit Abweichungen angezeigt werden.

  - Skripte und Makros, beispielsweise basierend auf Visual Basic for Applications oder Visual Basic Script, können in der Regel nicht verlustfrei migriert werden.
- Datei- und Informationsmanagement:
  - SharePoint-spezifische Metadaten, Workflows und Versionierungsattribute lassen sich nicht vollständig in Nextcloud übertragen und erfordern individuelle Migrationsskripte. Gewisse Inhalte müssten gegebenenfalls aus Sharepoint in das Zielsystem XWiki migriert werden.

Zentrale Office Dokumente und E-Mail und Kalender-Inhalte können grundsätzlich migriert werden. Bei einer Migration von M365 zu openDesk muss jedoch mit Informationsverlusten gerechnet werden, beispielsweise in den Bereichen von Skripten, SharePoint-Metadaten, und Teams-Chatverläufen.

openDesk basiert auf offenen Standards (u.a. REST, OIDC, LDAP, WebDAV, CalDAV/CardDAV) und ermöglicht die Integration von Fachanwendungen, wobei jede Anbin-dung eine individuelle Bedarfsanalyse erfordert. E-Mail-, Kalender- und Office-Dokumente lassen sich grundsätzlich migrieren, während Teams-Chatverläufe, VBA-Makros und SharePoint-Metadaten nicht verlustfrei übertragbar sind. Eine detaillierte Anforderungs- und Migrationsplanung ist daher Voraussetzung für den Wechsel.

Betriebsprozesse und Release-Management

Betriebsprozesse
Das übergeordnete Service-Management Framework (oft basierend auf ITIL), die Rollenmodelle sowie die Logik des Service-Level-Reportings bleiben grundsätzlich bestehen, die inhaltliche Ausgestaltung einzelner Prozesse verändert sich jedoch erheblich. Die wesentlichen Veränderungen beim Wechsel von M365 zu einem hoster-managed openDesk Lösung sind u.a. folgende:

- Incident Management: Der Hoster wird zum Single Point of Contact und ersetzt den Herstellersupport von Microsoft mit dessen SLAs, Support-Portalen und Knowledge-Base-Artikeln. Eskalationspfade sind neu zu definieren. Bei einem Open-Source-Stack erfolgt die Tiefensuche bei Bedarf über Community-Kanäle der jeweiligen Komponenten (Nextcloud, Collabora, OpenProject, Element/Matrix) statt über einen einzelnen Hersteller. Ticketkategorien und die Known-Error-Datenbank müssen entsprechend angepasst werden.
- Change Management: Der Unterschied liegt vor allem in der Steuerung von Releases. Während M365 Updates weitgehend herstellergetrieben ausrollt, erfolgen diese im openDesk-Umfeld abgestimmt mit Hoster und ZenDiS. Für die Kundenorganisation ergibt sich damit ein anderer Koordinationsbedarf, ohne dass die Release-Verantwortung vollständig bei ihr liegt. Testing und Validierung bleiben in beiden Modellen erforderlich. Bei M365 ist von einem hohen Niveau herstellerseitiger Qualitätssicherung auszugehen, fehlerhafte Releases lassen sich jedoch auch dort nicht ausschliessen.

- Problem Management: Der Eigenleistungsanteil kann steigen. Root-Cause-Analysen bei M365 beschränken sich häufig auf das Nachverfolgen herstellerseitiger Incidents. Bei openDesk ist das Betreiberteam des Kunden gemeinsam mit dem ausgewählten Hoster näher an Code und Infrastruktur. Dadurch sind schnellere Lösungen möglich, die Verantwortung wächst jedoch entsprechend. Dependency-Tracking erfolgt über mehrere OSS-Komponenten statt über eine integrierte Suite.
- Service Request / Request Fulfillment: Der Service-Katalog muss neu gemappt werden (Teams zu Element/Jitsi, SharePoint zu Nextcloud, OneDrive zu Nextcloud Files, Planner zu OpenProject).
- Configuration Management (CMDB): Die Configuration Items sind neu aufzunehmen: Nextcloud-Instanzen, Collabora Online, Keycloak, OpenProject, Univention UCS als Identity-Layer sowie weitere Komponenten. Schnittstellen zum Hosting-Partner sind sauber zu dokumentieren; die Shared Responsibility zwischen Betreiberteam und Hoster-Partner muss explizit ausgewiesen werden.
- Knowledge Management: Die bestehende Knowledge Base im Workplace-Engineering und –Support verliert einen erheblichen Teil ihrer Gültigkeit. Microsoft-365-Artikel sind durch openDesk-Äquivalente zu ersetzen. Endnutzerschulungen stellen dabei einen relevanten Aufwandstreiber dar.

Supplier / Contract Management
Der Wechsel führt weg von einem einzelnen Vendor (Microsoft) hin zu einem Hosting-Partner mit OSS-Upstream-Abhängigkeiten. SLAs mit dem Hosting-Partner sind zu verhandeln (siehe oben) insbesondere zu Verfügbarkeit, Patch-Fenstern, Backup und Restore, Exit-Strategie sowie Datenlokation. Das Hosting-SLA tritt faktisch an die Stelle des Microsoft-SLAs.

Release-Management
Microsoft kommuniziert keine konsolidierte Kennzahl über sämtliche Plattform-Changes; publiziert wird lediglich die Anzahl neuer Features. Gemäss offizieller Mitteilung des Herstellers vom Dezember 2025: In den zurückliegenden zwölf Monaten wurden mehr als 1’100 neue Features zur Plattform hinzugefügt,[10] wobei für 2026 eine weitere Welle von Erweiterungen überCopilot, Intune, Exchange Online und Defender angekündigt wurde.

Diese Feature-Anzahl bildet das Gesamtvolumen jedoch nur unvollständig ab. Hinzu kommen regelmässige Build-Updates der Desktop-Applikationen über die verschiedenen Update-Kanäle sowie Backendseitige Änderungen in den Cloud-Diensten. Microsoft unterhält für die M365 Apps mehrere parallele Update-Kanäle, unter anderem Current, Monthly Enterprise und Semi-Annual, für die jeweils fortlaufend Versions- und Build-Nummern mit zugehörigen Release Notes veröffentlicht werden.[11] Steuerungsseitig erfolgt die Verteilung über ein gestuftes Modell:

[10] OneAdvanced, Microsoft 365's 2026 upcoming changes, 16. Dezember 2025. URL: https://www.oneadvanced.com/resources/new-features-new-prices-microsoft-365s-2026-upcoming-changes/, abgerufen am 14. August 2026.
[11] Microsoft Learn, Update history for Microsoft 365 Apps (listed by date). URL: https://learn.microsoft.com/en-us/officeupdates/update-history-microsoft365-apps-by-date, abgerufen am 14. August 2026.

Standard Release ist der Standardweg, bei dem Updates mit breiter Verfügbarkeit ausgerollt werden, Targeted Release ermöglicht ausgewählten Nutzenden oder ganzen Organisationen den frühzeitigen Bezug neuer Funktionen zu Validierungszwecken.[12] Die Kommunikation erfolgt dabei über M365 Roadmap und Message Center.
In Summe ist eine Grössenordnung von mehreren Tausend Einzeländerungen pro Jahr, abhängig von Zählmethode und Abgrenzung plausibel.

Für openDesk liegt die Release-Strategie öffentlich dokumentiert vor. OpenDesk folgt einem strukturierten Release-Zyklus: Major-Releases sind auf das dritte Quartal jedes Jahres terminiert, mit Planungsbeginn im ersten Quartal; Minor-Releases erfolgen monatlich an Montagen in einem Vier-Wochen-Rhythmus.[13] Ergänzt wird dieser Takt durch anlassbezogene Patch-Releases, insbesondere bei sicherheitsrelevanten Korrekturen. Der Patch-Workflow umfasst Identifikation, Schweregrad-Bewertung, Entwicklung auf dedizierten Hotfix-Branches, automatisierte und manuelle Qualitätssicherung in einer produktionsnahen Staging-Umgebung, eine formale Freigabe durch Product Owner oder Release Manager sowie die Auslieferung über CI/CD-Pipelines in definierten Deployment-Fenstern, bei kritischen Problemen auch ausserhalb des Regelrhythmus.[14]

Die Praxis bestätigt diese Kadenz. Innerhalb weniger Monate wurden mehrere aufeinanderfolgende Versionen veröffentlicht, wobei einzelne Releases gezielt Sicherheitslücken in Komponenten wie OpenProject adressierten. Für die Suite-Ebene ergibt sich damit eine jährliche Grössenordnung von einem Major-Release, rund zwölf Minor-Releases und typischerweise zehn bis fünfundzwanzig Patch-Releases, also insgesamt etwa 25 bis 40 Suite-Releases pro Jahr.
Für betreiberseitige Planbarkeit relevant: openDesk-SaaS-Installationen werden gemäss dem zugehörigen SLA automatisch aktualisiert. Self-Hosted-Installationen folgen separaten Upgrade- und Migrationshinweisen.[15]

Da openDesk als integrierte Suite mehrere Open-Source-Produkte bündelt, liegt die eigentliche Änderungsfrequenz deutlich höher als die der Suite-Releases. Die Plattform basiert auf Komponenten von Collabora, Element, Nextcloud, Nordeck, Open-Xchange, Univention, OpenProject und XWiki.[16] Jedes dieser Upstream-Projekte verfolgt einen eigenen Release-Zyklus mit Major-, Minor- und Patch-Versionen. Kumuliert ergeben sich auf Komponenten-Ebene

[12] Microsoft Learn, Set up the Standard or Targeted release options for Microsoft 365. URL: https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365?view=o365-worldwide
[13] ZenDiS, Release Management – openDesk Documentation. URL: https://docs.openDesk.eu/operations/releases/, abgerufen am 14. August 2026.
[14] ZenDiS (2024–2025): Neuigkeiten und Blog openDesk. URL: https://www.openDesk.eu/de/blog, abgerufen am 14. August 2026.
[15] ZenDiS, openDesk 1.11: Kontinuierliche Verbesserungen und Optimierungen. URL: https://www.openDesk.eu/de/blog/openDesk-1-11, abgerufen am 14. August 2026.
[16] Netzwerk SDS, openDesk-Seite mit Liste der Schweizer Betreiber, URL: https://netzwerksds.ch/openDesk/, abgerufen am 14. August 2026.

mehrere hundert Einzeländerungen pro Jahr, die jedoch durch das ZenDiS-Release-Engineering konsolidiert, getestet und gebündelt ausgeliefert werden.

Der quantitative Unterschied, grob mehrere Tausend Plattform-Changes bei M365 gegenüber mehreren Hundert konsolidierten Komponenten-Changes bei openDesk, ist weniger entscheidend als die qualitative Verschiebung der Release-Charakteristik:

- M365 liefert Änderungen kontinuierlich, weitgehend hersteller-getrieben und für den Betreiber nur begrenzt steuerbar. Die Planbarkeit einzelner Changes ist gering; das Change-Management reagiert überwiegend auf herstellerseitige Ankündigungen.
- openDesk hingegen bündelt Änderungen in planbare, monatliche Suite-Releases mit definierten Wartungsfenstern. Die Release-Hoheit liegt, im Self-Hosted- oder hoster-managed Betriebsmodell, beim Betreiber beziehungsweise beim Hosting-Partner. Dies reduziert das Volumen ungeplanter Changes, erhöht jedoch den Eigenanteil an Testing, Validierung und internen Change-Prozessen.

Das ITIL-basierte Service-Management-Framework bleibt grundsätzlich bestehen, die inhaltliche Ausgestaltung einzelner Prozesse verändert sich jedoch, insbesondere in den Bereichen Change-, Problem- und Knowledge-Management. Während M365 mehrere Tausend Änderungen pro Jahr kontinuierlich und herstellergetrieben ausliefert, bündelt openDesk Änderungen in rund 25–40 planbare Suite-Releases mit definierten Wartungsfenstern. Damit verlagert sich die Release-Hoheit von Microsoft auf den Betreiber bzw. Hosting-Partner, was sowohl die Steuerbarkeit als auch den Eigenanteil an Testing und Validierung sowie die Souveränität erhöht.

Anhang B: Abkürzungen

Abkürzung	Begriff
AD	Active Directory
API	Application Programming Interface
BI	Business Intelligence
BYOD	Bring Your Own Device
CalDAV	Calendar Distributed Authoring and Versioning
CapEx	Capital Expenditure
CHF	Schweizer Franken
CIO	Chief Information Officer
CI/CD	Continuous Integration / Continuous Deployment
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
Copilot	Microsoft Copilot
DLP	Data Loss Prevention
DMS	Dokumentenmanagementsystem
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DVS	Digitale Verwaltung Schweiz
E2E	Ende-zu-Ende
EU	Europäische Union
FIDO2	Fast Identity Online 2
FISA	Foreign Intelligence Surveillance Act
FTE	Full-Time Equivalent
HSM	Hardware Security Module
IAM	Identity and Access Management
IKT	Informations- und Kommunikationstechnologie
IMAP	Internet Message Access Protocol
ISDS	Informationssicherheit und Datenschutz
ISG	Informationssicherheitsgesetz
IschV	Informationsschutzverordnung
ISV	Informationssicherheitsverordnung
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
KI	Künstliche Intelligenz

M365	Microsoft 365
M&A	Mergers and Acquisitions
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi-Factor Authentication / Multi-Faktor-Authentifizierung
ODF	Open Document Format
OIDC	OpenID Connect
OpEx	Operational Expenditure
OSS	Open Source Software
PaaS	Platform as a Service
PDF	Portable Document Format
PIM	Privileged Identity Management
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RZ	Rechenzentrum
SaaS	Software as a Service
SDS	Souveräne Digitale Schweiz
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOC	Security Operations Center
SSO	Single Sign-On
TBM	Technology Business Management
TCO	Total Cost of Ownership
TOM	Technische und organisatorische Massnahmen
UCC	Unified Communication and Collaboration
URL	Uniform Resource Locator
US	Vereinigte Staaten
VBA	Visual Basic for Applications
VPN	Virtual Private Network
WebDAV	Web Distributed Authoring and Versioning
XDR	Extended Detection and Response

Anhang C: Abbildungen und Tabellen