Im abschließenden Teil der Artikelserie beleuchten wir On-Premises Lösungen. Obwohl der Trend deutlich in die Richtung von Cloud-Services zeigt, sind die klassischen Lösungen im SAP-Umfeld nach wie vor weit verbreitet. Die Übergänge sind dabei fließend. Neben den zwei vorgestellten Lösungen in diesem Artikel existieren z.B. auch On-Premises Lösungen für Omada und IBM Security Verify aus dem Teil 3. Auf der Gegenseite bietet One Identity schon längst nicht mehr nur den klassischen Weg über die Installation der Software auf hauseigenen Servern an.

Wie die Artikelserie hoffentlich verdeutlicht, stehen Unternehmen buchstäblich vor der Qual der Wahl. Alle vorgestellten Lösungen haben ihre Stärken und Schwächen und somit ihre Nische im Markt gefunden bzw. erkämpft. Daher beachten Sie bitte auch in diesem Artikel, dass die Einschätzungen **keineswegs als abschließend betrachtet werden können** und **keine individuelle Beratung** ersetzen. Für die Aufgabe der Produktauswahl bietet consiness eine vorgefertigte Evaluierungsmatrix an, auf die wir am Ende des Artikels eingehen werden.

- Teil 1: Das Ende einer Ära: Die Zukunft nach SAP IDM
- Teil 2: SAP – Cloud Identity Services, GRC edition for SAP HANA
- Teil 3: Cloud Services
- Teil 4: On-Premises Lösungen: z.B. One Identity, SIVIS

Der Aufbau des Artikels gliedert sich wie folgt:

- Option A: SIVIS
- Option B: One Identity by Quest
- Unser Angebot: Die consiness Produktevaluierung

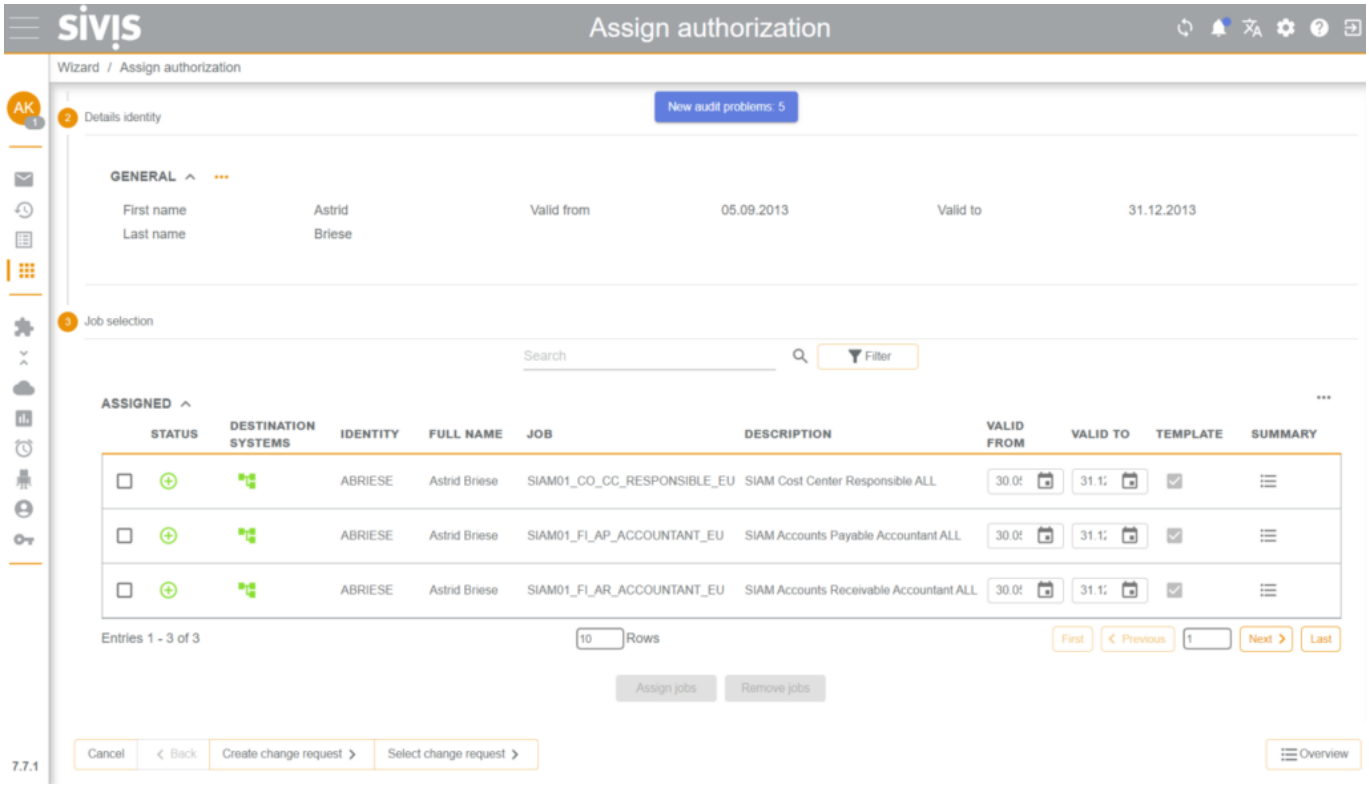
Option A: SIVIS

SIVIS ist ein Produkt, welches vor allem erfahrenen Administratoren in der Identitäts- und Berechtigungsverwaltung auf Anhieb gefallen wird. Die Software entstammt von dem gleichnamigen Unternehmen aus Karlsruhe und ist somit „made in Germany“. Aus unserer Sicht ergibt das einen signifikanten Vorteil, da die Problemstellungen bei SAP-zentrischen Anwendungen vor allem im DACH-Raum bekannt sind. So verwundert nicht, dass es sich hier um eine ABAP-basierte Lösung handelt, welche ein erweitertes Konstrukt auf der Basis klassischer SU01-Nutzerkonten und PFCG-Rollen bietet. Somit steht SIVIS mehr oder weniger in direkter Konkurrenz zum hauseigenen Produkt GRC seitens SAP.

Der Funktionsumfang von SIVIS klar erkennbar aus den alltäglichen Anforderungen des Identitäts- und Berechtigungsmanagements in komplexen SAP Lösungen entstanden. So verwundert nicht, dass SIVIS mit einer eigenen Engine für die Risikoanalyse von SAP-Berechtigungen auf Objektebene ausgeliefert wird. Auch die in SAP-Kreisen weitverbreitete Lösung für Privileged Access Management (SAP GRC Firefighter) kann SIVIS vollständig ersetzen, so dass in den meisten Fällen keine Integration mit Lösungen von Drittanbietern notwendig ist.

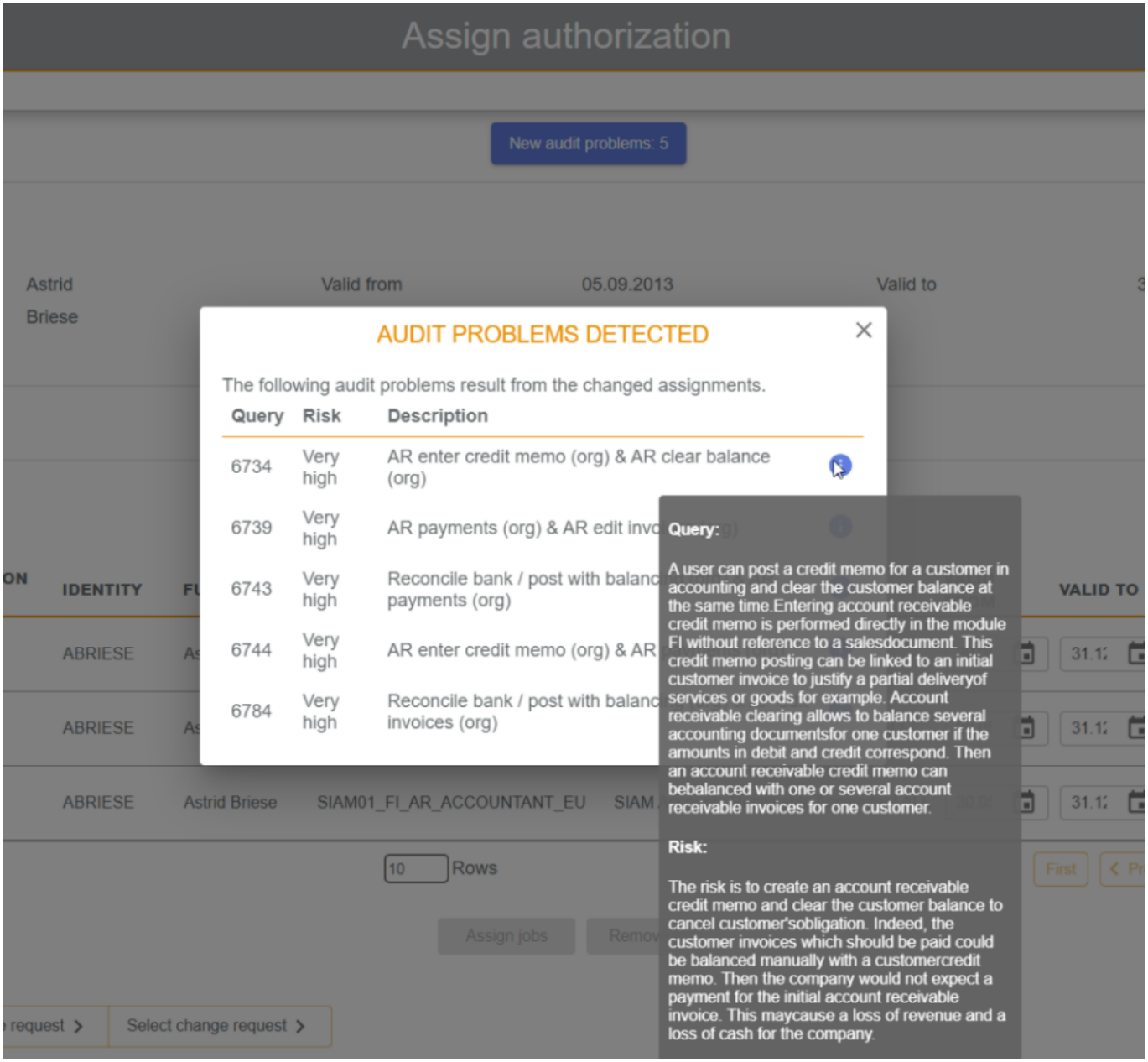
Einstieg in SIVIS über die SAP GUI

Die in die Jahre gekommenen Dynpro Oberflächen von ABAP werden von SIVIS mit einer optisch ansprechenden, modernen UI unterstützt. In dem folgenden Beispiel ist eine Rollenzuweisung erkenntlich, welche auf Arbeitsplatz-Rollen basiert und sofort mit der integrierten Risiko-Engine auf eventuelle Probleme hinweisen kann. Die Arbeitsplätze müssen sich dabei längst nicht auf SAP ABAP-basierte Berechtigungen beschränken, sondern können mit über 4000 Konnektoren mit allen erdenklichen Anwendungen integriert werden. Dazu gehören auch klassische Integrationen wie SAP BI, HCM, Active Directory und Cloud-Anwendungen.



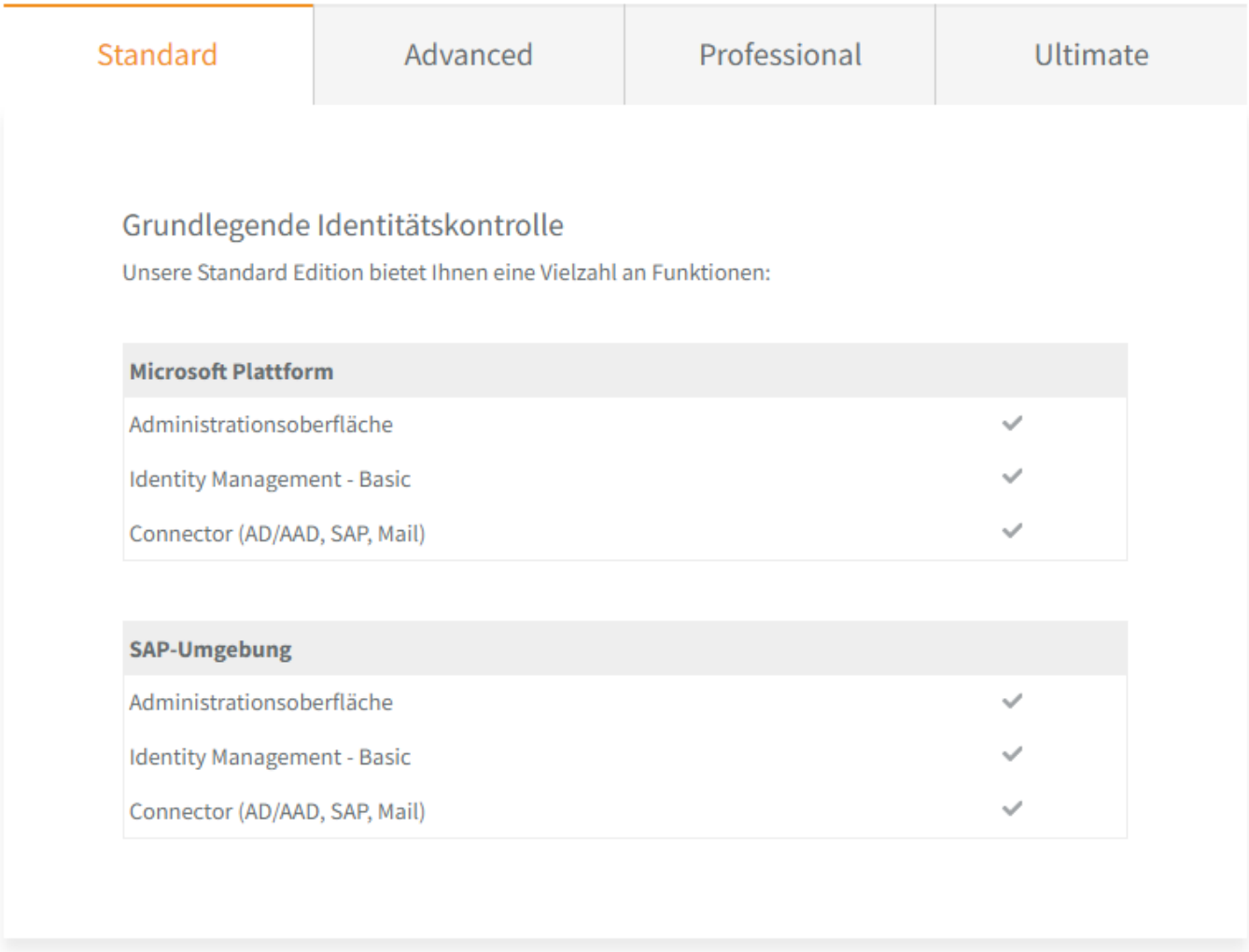
Zuweisung von Berechtigungen in der Custom-UI

Positiv hervorzuheben ist an dieser Stelle, dass die Regelwerke für kritische Berechtigungen und Funktionstrennungskonflikte nicht nur technisch, sondern auch fachlich und detailliert dargestellt werden. Damit ist die Lösung auch für Fachbereiche in der Rolle als Risiko-Eigner geeignet.



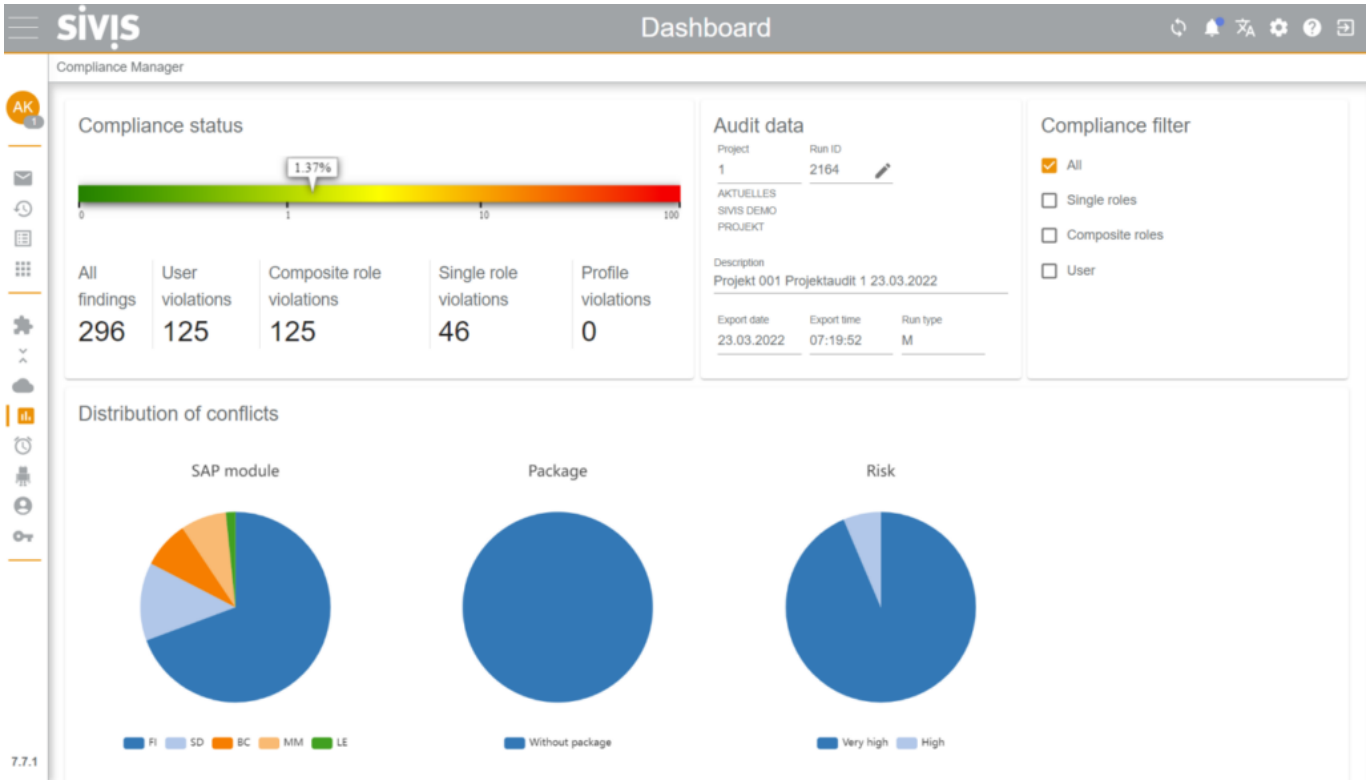
Risikoprüfung mit nicht-technischen Erläuterungen

Angeboten wird SIVIS grundsätzlich in 4 verschiedenen Editionen, welche sich im Funktionsumfang und der Konnektivität unterscheiden. Der Preis der Lösung ergibt sich grundsätzlich aus dem gebuchten Funktionsumfang und der Anzahl verwalteter Identitäten. Auch wenn es keine genauen Auskünfte über Preise auf der Webseite gibt, ist davon auszugehen, dass SIVIS sich preislich unterhalb einer vergleichbaren SAP-Lösung befindet.



SIVIS Editionen in der Übersicht

Abschließend werfen wir einen Blick auf das Dashboard des Compliance-Managers, welcher möglichst übersichtlich und „Management-tauglich“ den Status revisionskritischer Berechtigungen dokumentiert. Auch für Berechtigungs-Manager ist das Dashboard die erste Anlaufstelle zum bereinigen oder mitigieren von Problemen im Berechtigungskonzept.



Compliance Manager in Aktion

Vorteile

- SAP-nahe Lösung von hochspezialisierter Firma für IAM
- Plattformen für Microsoft und SAP
- Kundennähe mit direktem Draht zum Hersteller
- Attraktiveres Preismodell als bei der Konkurrenz von SAP
- Integrierte Engine für Risikoanalyse, die auf SAP-ABAP-Objektebene heruntergebrochen werden kann
- Integrierte Lösung für Privileged Access Management (PAM)

Nachteile

- Keine Fiori-Oberflächen für SAP
- Vergleichsweise kleiner Anbieter

Einschätzung

Wir wurden durch ein Projekt eines unserer Partner bei einem Großkunden auf SIVIS aufmerksam. In einer Demonstration mit SIVIS konnten wir die Lösung gegen die,

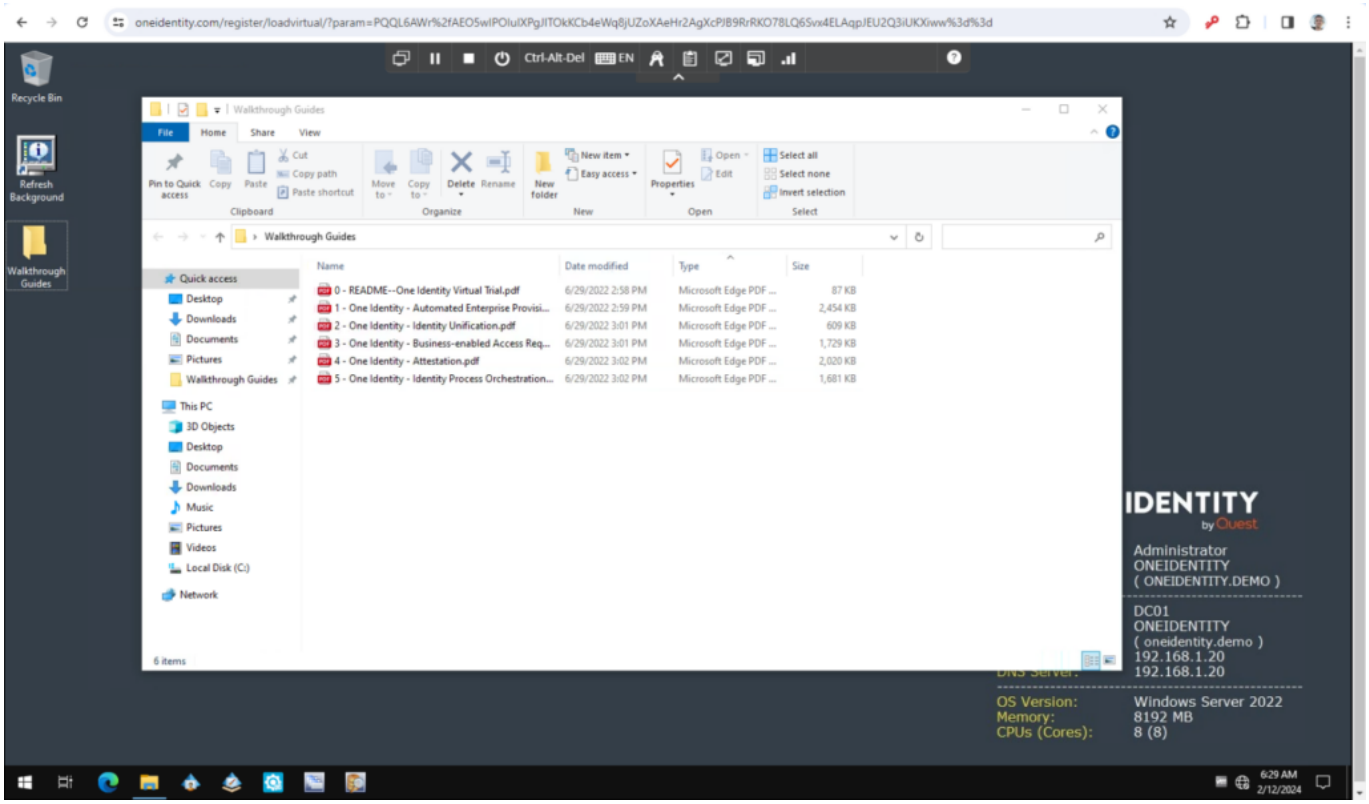
teilweise sehr speziellen, Anforderungen einer unserer bestehenden IDM-Kunden evaluieren. Bei keinem der anderen vorgestellten Optionen dieser Artikelserie können wir eine derart hohe Trefferquote und „out-of-the-box“ Unterstützung verzeichnen. Während viele Lösungen bei Themen wie Erweiterbarkeit, PAM, Berechtigungsrisikoanalysen und spezielle Provisionierungs-Szenarien im SAP-Umfeld auf Integration mit Drittanbietern verweisen müssen, kann SIVIS all diese Kriterien von sich aus erfüllen. In Kombination mit der unkomplizierten und zielorientierten Architektur überrascht es nicht, dass Kunden langfristig auf SIVIS setzen. Wir können eine klare Empfehlung für hochkomplexe und SAP-lastige Architekturen aussprechen.

Option B: One Identity by Quest

Vorab gesagt: One Identity ist vermutlich die komplexeste und mit über 11.000 Kunden am weitesten verbreitete On-Premise IAM-Lösung auf dem Markt. Auch die insgesamt 3.500 weltweiten Mitarbeiter in 39 Ländern weisen darauf hin, dass man es hier mit einem wahren Schwergewicht in der Branche zu tun hat, welches sich neben dem Identity und Access Management mit Themen wie Data-Governance, Sicherheit, Migration, Replikation und Schnittstellen beschäftigt.

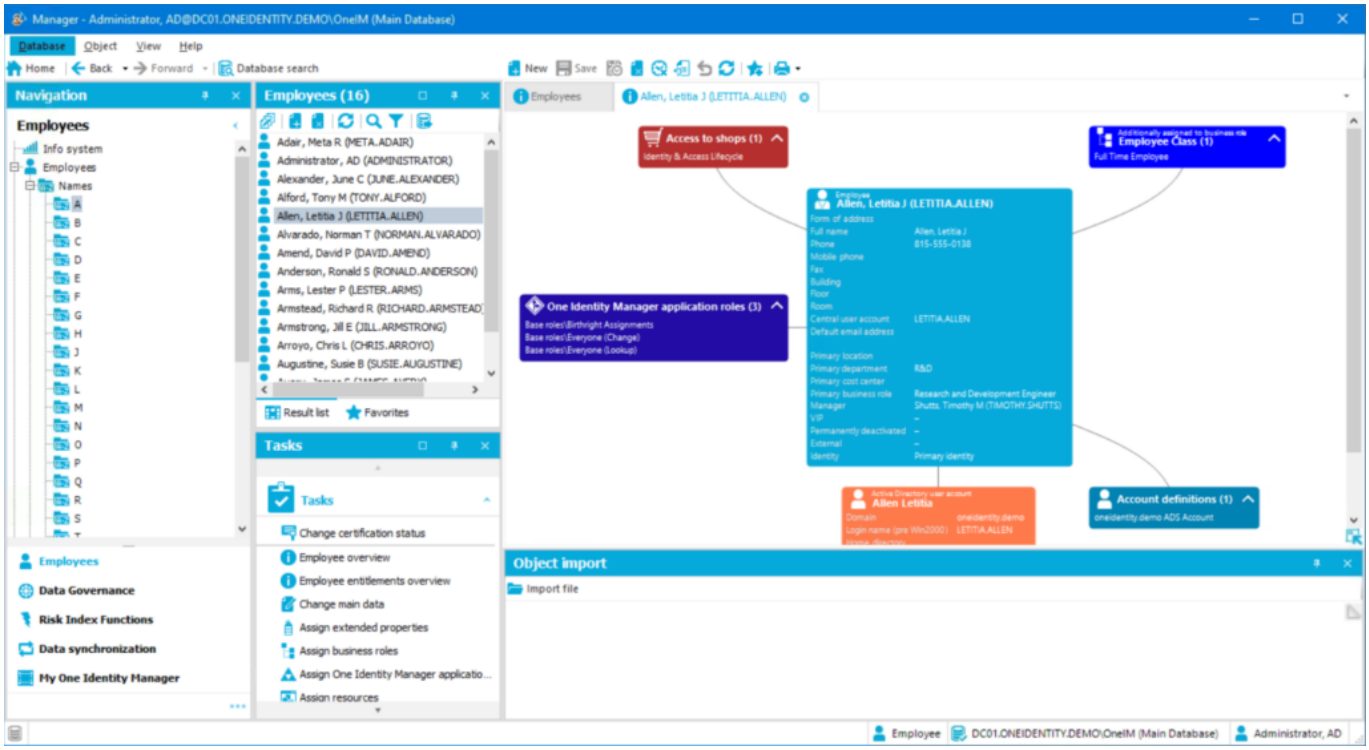
Quest bietet mit One Identity Starling ihre Expertise mittlerweile auch in der Cloud an. Dieser Artikel soll sich jedoch auf das „klassische“ on-Premise Produkt fokussieren. Wie bereits mehrfach erwähnt, ist eine abschließende Betrachtung aller Optionen nahezu unmöglich.

Wir lassen uns gern korrigieren, aber ein wirklich einmalig und geniales Angebot von Quest ist, dass hier binnen von einer Minute eine Trial-Version in einer virtuellen Umgebung für interessierte Kunden bereitgestellt werden kann. Ein Feature, welches sonst nur Cloud-Anwendungen liefern können. Dementsprechend ist auch denkbar, den vollständigen Betrieb der On-Premises Lösung auf eine Cloud-Instanz auszulagern. Schließlich bedeutet Cloud in vielen Fällen erstmal nur, dass eine Software auf einem „anderen Server“ läuft.



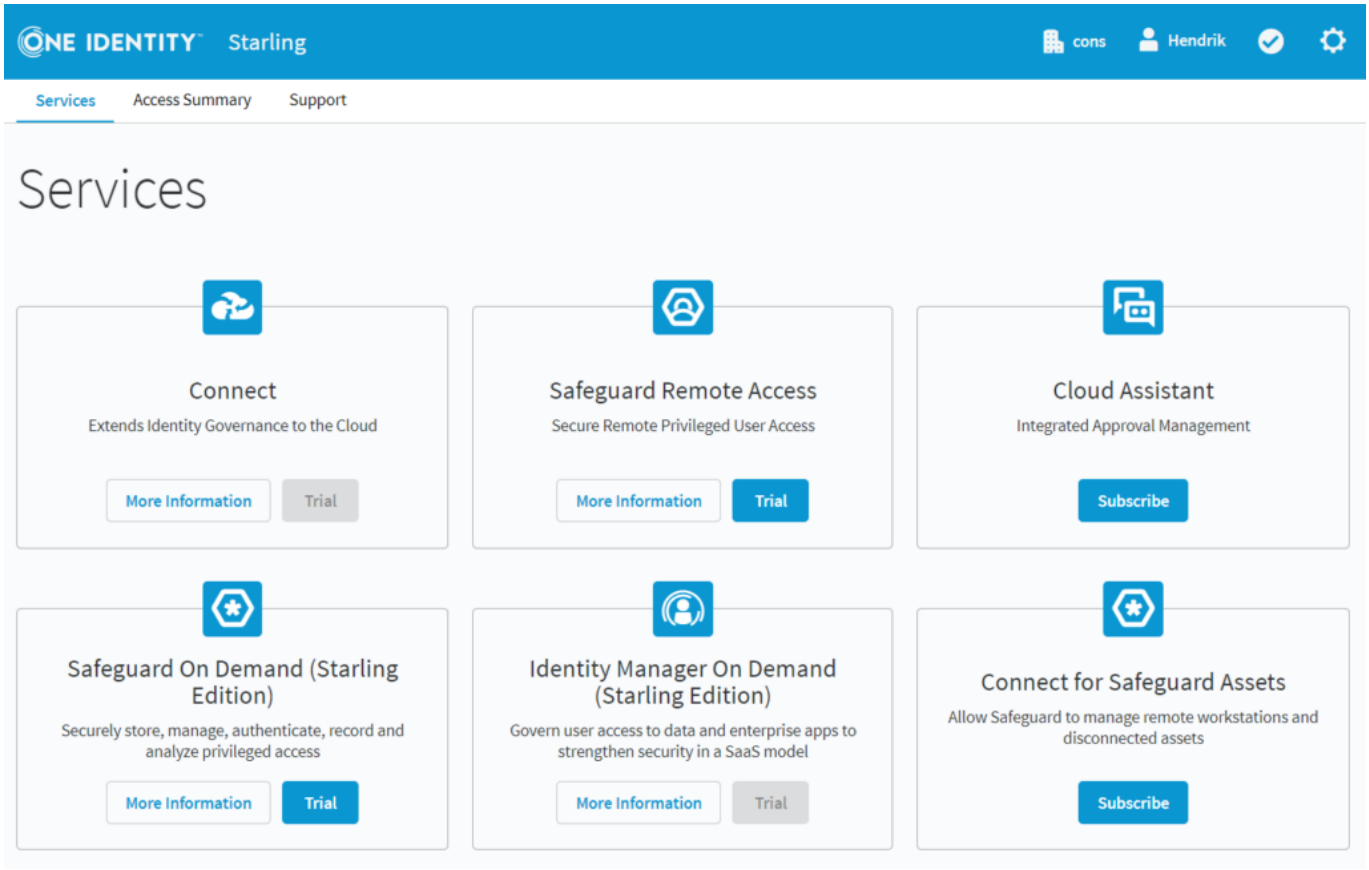
Trial-Version im Browser als virtueller Desktop bereitgestellt

Schon direkt nach dem Login bekommt der Anwender einen Eindruck, mit was für einer Lösung man es hier zu tun hat: Es gibt 5 Hauptapplikationen, die direkt angesteuert werden können: Den Manager, Designer, Synchronization Editor, Object Browser und die Job Queue Info. Der Technologie-Stack basiert auf .NET und liefert nahezu unendliche Möglichkeiten eigenes Customizing und/oder Entwicklungen vorzunehmen.



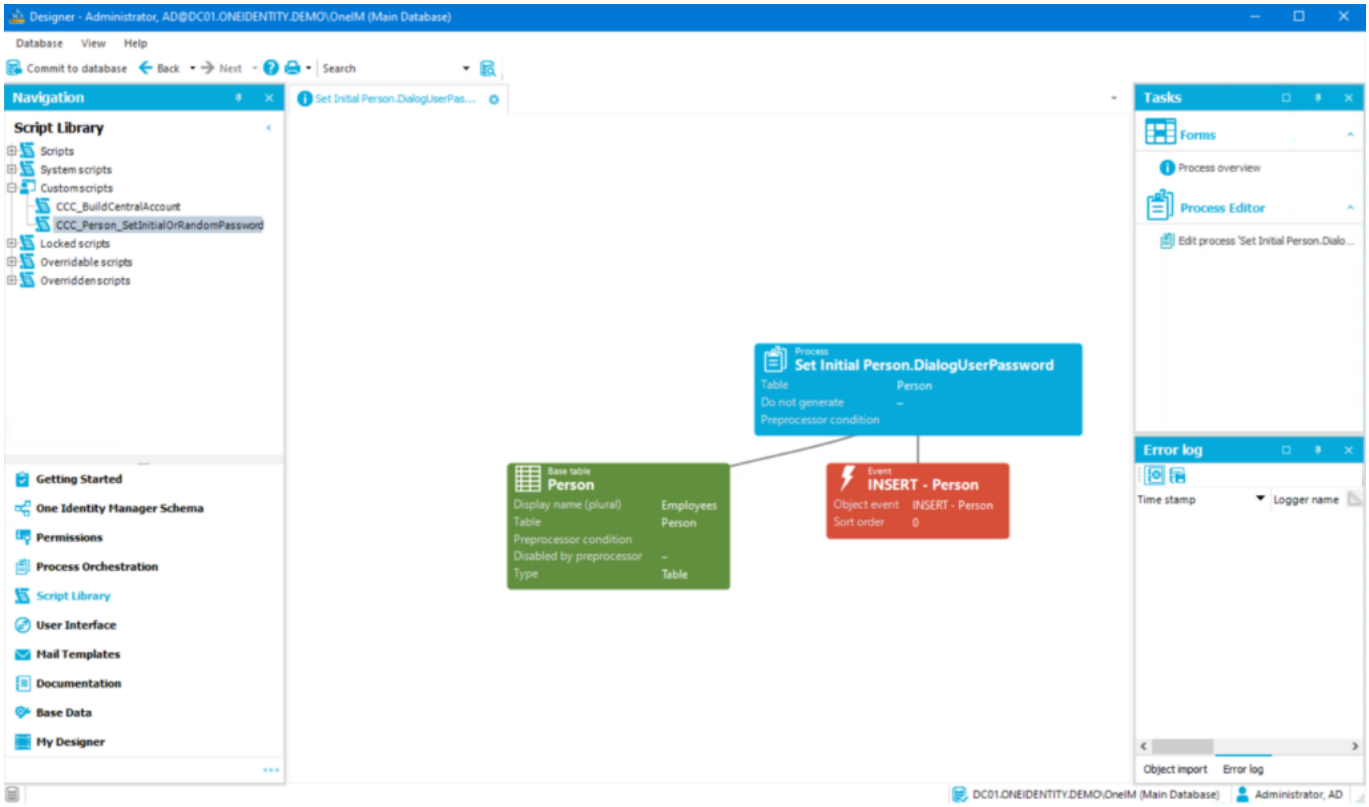
Ansicht einer Identität im Manager

Die Oberflächen der klassischen Edition bewerten wir als etwas „eingestaubt“, jedoch funktional. In dem Manager können Sie Personen in einer Art Telefonbuch nachschlagen und erhalten eine grafische Übersicht der Identitätsdaten, Zugänge und Berechtigungen. Auch die wichtigsten Funktionen wie die Zuweisung neuer Privilegien sind nur einen Klick entfernt. Ein Blick in One Identity Starling offenbart, dass Service- bzw. Cloud-basierte Identity Services in einem deutlich zeitgerechteren Design ausgerollt werden.



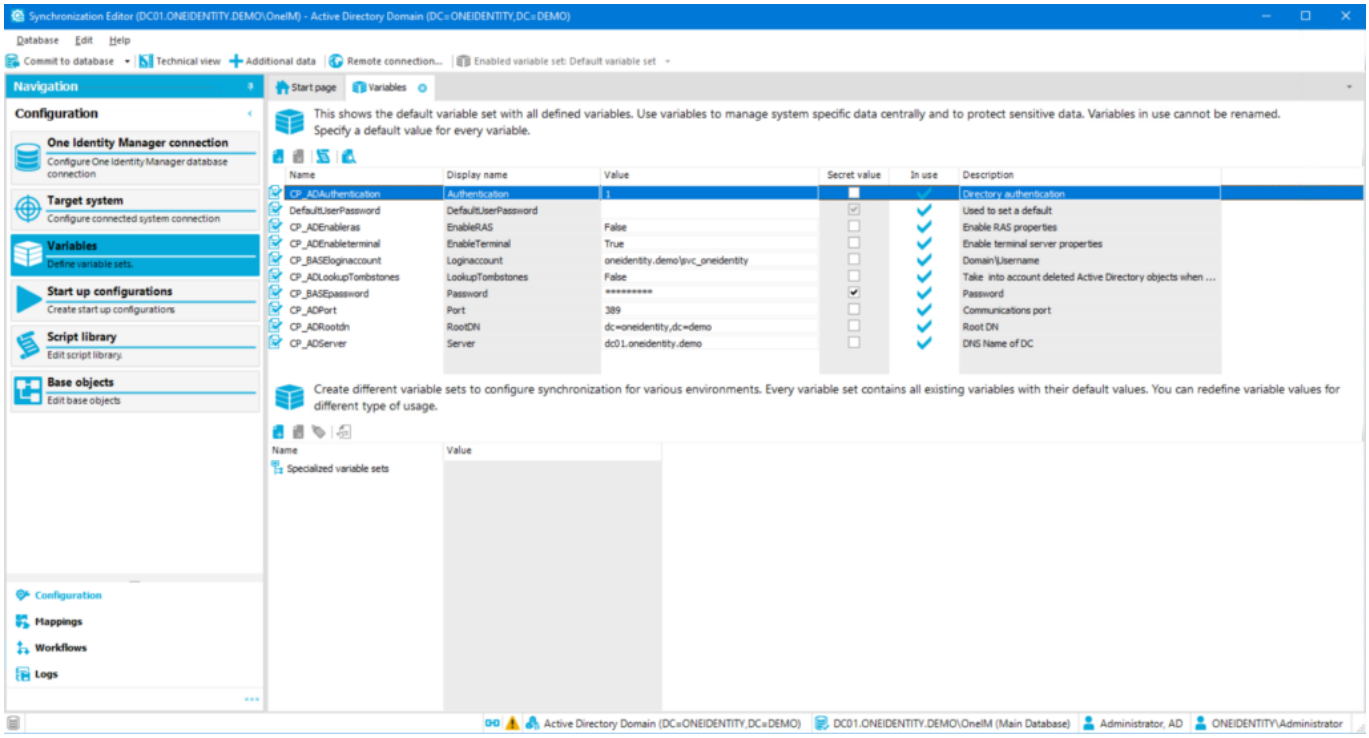
One Identity Starling inkl. On Demand Identity Manager

Um einen weiteren Eindruck zum Thema Individualisierung zu geben, zeigen wir folgend Möglichkeiten um Scripts und Konnektoren bzw. Synchronisations-Szenarien zu pflegen. Der Script-Editor bettet sich mit einer grafischen Oberfläche in das System ein, so dass Schnittstellen und Zusammenhänge direkt sichtbar werden.



Designer mit Script Library

Ein großer Vorteil von SAP-Software (bzw. SAP IDM) war aus unserer Sicht schon immer, dass hochkomplexe Szenarien und kundenspezifische Eigenheiten durch Anpassungen abgebildet werden können. Ohne zu bewerten, ob eine Rückführung auf Standard-Prozesse nicht die bessere Alternative wäre, sollten bei One Identity keine Anforderungen aufgrund technischer Restriktionen unlösbar bleiben.



Hochdetaillierter Synchronization Editor

Um sich mit der Welt von One Identity vertraut zu machen, wird die One Identity University prominent beworben. Je nach Anforderungsprofil lassen sich hier Schulungen in unterschiedlichen Umfängen und fachlich bzw. technischem Tiefgang buchen. Für Dienstleister kann der Einstieg gut und gern einen ganzen Monat Schulungen bedeuten. Diesen Wettbewerbsvorteil mit dem gewissen „Burggraben“ der One Identity-Spezialisten dürfte alteingesessenen SAP-Beratern bekannt vorkommen.

Zum Thema Preisgestaltung können wir von Quest leider keine öffentlichen Informationen erhalten. Die Erfahrung aus unserem Umfeld zeigt, dass man sich hier in etwa auf der Höhe einer vergleichbaren SAP-Lizenzierung befindet. Dies kann jedoch stark von Kunde zu Kunde variieren.

Vorteile

- Etablierte Lösung vom Marktführer
- Höchste Anpassbarkeit und Komplexität, die stark an SAP IDM erinnert
- Bereitstellung in der Cloud möglich
- Sehr gut dokumentiert und klarer Schulungs-Pfad durch die One Identity University

Nachteile

- Komplexe Architektur
- Umfangreiche Ausbildung für Administratoren / Entwickler notwendig
- SAP-spezifische Szenarien wie PAM und Risikoanalysen benötigen Integration von SAP GRC

Einschätzung

Wie in der Vorstellung schon erwähnt, bietet One Identity unzählige Möglichkeiten, sich eine maßgeschneiderte IAM-Lösung zu bauen. Das ist für potentielle Kunden entweder gut oder schlecht. Oft wird erst einige Zeit nach einer IAM-Einführung klar, welche besonderen Anforderungen und Details im Unternehmen existieren. Bei One Identity sollten Prinzipiell alle denkbaren Szenarien mit Bordmitteln umsetzbar sein. Damit sehen wir One Identity als Lösung an, die vom Typ her am ehesten SAP Identity Management entspricht und ähnliche Flexibilität liefert. Der größten Unterschiede sind jedoch, dass One Identity mit deutlich mehr out-of-the-box Features, einer deutlich größeren Kundenbasis und einer viel längeren Historie auf dem IAM-Markt punkten kann. Weiterhin schläft Quest nicht und bietet die Lösung mittlerweile auch als Cloud-Service an. Für uns ist erkennbar, warum One Identity Marktführer ist. Die einzigen Nachteile der Lösung bestehen aus unserer Sicht darin, dass sie recht komplex erscheint und SAP-Integrationsszenarien nie der Hauptfokus der international agierenden Firma waren.

Unser Angebot: Die consiness Produktevaluierung

Consiness bietet eine spezialisierte Produktevaluierung für Identity and Access Governance (IAG)-Lösungen an, die auf die individuellen Gegebenheiten unserer Kunden abgestimmt ist. Dabei nutzen wir einen vorgefertigte Methodik, um die verfügbaren Optionen systematisch zu analysieren.


consiness Produktevaluierungs-Matrix

- **Scoring:** Gewichtete Bewertung von Lösungen anhand deren Produktmerkmalen und Rahmenbedingungen.
- **Kostenaufstellung:** Grobe Kalkulation der laufenden- und Investitionskosten für eine Lösung über einen Zeitraum von 10 Jahren.
- **Roadmap:** Modell-Projektplanung für die Einführung der neuen Lösung.
- **Entscheidung:** Abschließende Ausarbeitung einer vertret- und nachvollziehbaren Entscheidung gegenüber den Stakeholdern.

Die vorgestellte Methodik unterstützt Unternehmen dabei, fundierte Entscheidungen zu treffen, sei es bei der initialen Auswahl einer IGA-Lösung oder bei der Überprüfung bereits getroffener Entscheidungen. So stellen wir sicher, dass die ausgewählten Lösungen optimal den Anforderungen entsprechen und zukunftssicher sind. Eine detaillierten Einblick in die consiness Produktevaluierung werden wir demnächst auf LinkedIn veröffentlichen.

Zusammenfassung

Mit diesem Beitrag endet unsere Artikelserie, in der wir in vier Teilen diverse Optionen aufgezeigt haben. Jede dieser Optionen hat ihre eigene Nische und Daseinsberechtigung, wodurch sie verschiedene Anforderungen und Präferenzen abdeckt. Trotz der detaillierten Darstellung aller Möglichkeiten kann eine präzise Evaluierung der Produkte basierend auf den individuellen Kundenbedürfnissen nicht

ersetzt werden. Es bleibt essenziell, dass Sie Ihre spezifischen Anforderungen und Erwartungen sorgfältig analysieren, um die für Sie optimale Wahl zu treffen. Da selbstverständlich noch viele weitere Lösungen existieren, die es nicht in die Artikelserie geschafft haben, behalten wir uns vor, auf diese in der Zukunft in diesem Rahmen einzugehen.

Abschließend hoffen wir, dass wir Sie nicht gelangweilt haben und gleichzeitig einen guten Überblick über die weite Welt der IGA-Lösungen aus der Sicht einer SAP-Beratung geben konnten.

Über den Autor

Hendrik Winkler ist Partner der consiness und Lead Architekt für Identity und Access

Management Lösungen. Er kann auf umfangreiche Expertise in SAP ABAP, GRC, Cloud-Technologien und SAP Identity Management zurückgreifen. Mit über zehn Jahren in der IT-Branche hat er sich auf die Entwicklung und Implementierung von komplexen IAM-Systemen spezialisiert, wobei er stets ein Auge auf Sicherheit, Benutzerfreundlichkeit und Compliance hat.

Der Artikel ist auch bei Linkedin erschienen:

https://www.linkedin.com/pulse/das-ende-einer-%25C3%25A4ra-teil-44-on-premises-l%25C3%25B6sungen-hendrik-winkler-u3dse