



# TREASURYLOG

Informationen für Treasurer und Finanzverantwortliche, seit 1992 herausgegeben von Schwabe, Ley & Greiner

## Zwischen Weiterentwicklung und Sicherheit Spannungsfeld in unruhigen Zeiten

### s. 8 **Wie passt ein Roboter in die Funktionentrennung?**

Automatisierung führt zu Wandel in der Treasury-Organisation.

### s. 12 **Entscheidungsfindung zur SWIFT- Anbindung**

Komplex aber machbar.

### s. 22 **Sustainable Finance**

Wie die EU Standards für nachhaltige Finanzierungen setzt.

### s. 26 **Der Aufstieg von Ransomware**

Wie Sie sich vor Angriffen aus dem Darknet schützen.

**2021**



SCHWABE, LEY & GREINER

# GESUCHT: HERAUSRAGENDE LEISTUNGEN IM TREASURY

## Auszeichnung „Digital Treasury Excellence“

Das Finanzsymposium ruft in diesem Jahr die „Digital Treasury Excellence“-Auszeichnung ins Leben. Damit sollen Projekte im Bereich der digitalen Transformation hervorgehoben werden. Der Preis würdigt Treasury-Abteilungen und -Teams, die sich durch herausragende Leistungen hervortun.

### Ihre Vorteile als Finalist:

Tickets für das Symposium -  
Projektvorstellung im TreasuryLog -  
EUR 5.000,- für wohltätige Zwecke -

### Anmeldeschluss: 31. März 2021

Eine Jury aus Praktikern wird alle Einreichungen eingehend prüfen und drei Finalisten küren, aus denen die Teilnehmer des Finanzsymposiums den Sieger mittels Abstimmung wählen. Der Gewinner der „Digital Treasury Excellence“ wird am 22. April 2021 während des virtuellen Galaabends bekannt gegeben und gebührend gefeiert.

### Mehr erfahren Sie unter:

[www.finanzsymposium.com/dte](http://www.finanzsymposium.com/dte)



# DTE

DIGITAL TREASURY EXCELLENCE

# Liebe Leserinnen und Leser!

**M**it Freude dürfen wir Ihnen die erste Ausgabe des TreasuryLog 2021 präsentieren. Wir haben auch in diesem Heft versucht, jene Themen zu beleuchten, die Sie in den letzten Wochen und Monaten besonders intensiv beschäftigt haben und die verstärkt von unseren Kunden nachgefragt wurden.

## Langfristige Veränderungen in der Treasury-Organisation zu erwarten?

Sie werden daher feststellen, dass wir einen Fokus auf die Themen Organisation und Sicherheit gelegt haben. Dieser Schwerpunkt ist unter anderem der Tatsache geschuldet, dass uns das Arbeiten im Home-Office, angesichts der aktuellen Entwicklungen, noch über einen längeren Zeitraum begleiten wird. Vielleicht bleibt der über Jahrzehnte praktizierte Büroalltag in dieser Ausprägung sogar ein Dinosaurier einer vergangenen Zeit und wir werden uns an eine deutlich flexiblere Arbeitsweise gewöhnen müssen. Wird sogar die langbewährte organisatorische Funktionentrennung von Front-, Middle- und Back-Office durch verstärkte Digitalisierung bzw. Automatisierung überflüssig? Braucht es im Gegenzug zusätzliche Funktionen im Treasury? Dass diese Fragen den Treasurern unter den Nägeln brennen, hat sich nicht zuletzt bei unserem Treasury Summit gezeigt, der dieses Mal wieder mit den „Elefanten“ aus dem deutschsprachigen Raum stattgefunden hat.

## Daten- und Systemsicherheit im Krisenmodus nicht an erster Stelle

Dass sich Arbeitsweisen vermutlich nachhaltig ändern werden, manifestiert sich auch darin, dass viele Arbeitsabläufe, die notdürftig, quasi „über Nacht“ digitalisiert wur-

den, inzwischen Routine sind. Auch im Bereich der technischen Ausstattung wurde in den letzten Monaten massiv nachgebessert: Laptops wurden angeschafft, Remote-Zugriffe eingerichtet und die Möglichkeiten und Bandbreiten des Datenaustauschs massiv erweitert. Daten- und System-sicherheit standen aufgrund der „Operation am offenen Herzen“ nicht immer an erster Stelle. Viele Unternehmen sind daher nun damit beschäftigt, diesen Aspekt zu optimieren und Sicherheitsvorkehrungen zu erhöhen. Ein Beitrag zur aktuellen Bedrohungslage durch Cyberattacken soll hier entsprechend zur Sensibilisierung beitragen.

## Finanzsymposium ebenfalls aus dem Home Office zu erreichen

Apropos Sicherheit: Weiterhin unzufriedenstellende Infektionsentwicklungen, Verlängerung des Lockdowns und der unsichere Ausblick auf April zwingen uns, 2021 ein rein digitales Finanzsymposium zu veranstalten. Wir finden es einerseits sehr schade, dass wir uns weiterhin nicht persönlich treffen können, andererseits sehen wir darin aber die spannende Herausforderung, Ihnen ein digitales Event in noch nie dagewesener Qualität zu bieten. Wir haben die letzten Monate nicht untätig verstreichen lassen und ein ausgefeiltes Veranstaltungskonzept erstellt, das Sie in vielen Belangen buchstäblich überraschen wird. Wir trachten danach, auch 2021 wieder neue Maßstäbe mit unserem virtuellen Symposium zu setzen.

Wir wünschen Ihnen ein erfolgreiches Jahr 2021 und hoffen, Sie im April virtuell am Finanzsymposium zu treffen!

*Philip Tüttö*

## Inhalt

- |  |  |
|--|--|
| <p><b>4 Risikopositionsermittlung</b><br/>„Den Beipacktext sorgfältig lesen ...“</p> <p><b>6 Zinsrisiko im Niedrigzinsumfeld</b><br/>Trotz Negativzinsen kann es sinnvoll sein, sich jetzt fixe Zinsen zu sichern.</p> <p><b>8 Wie passt ein Roboter in die Funktionentrennung?</b><br/>Automatisierung entwickelt die Treasury-Organisation weiter</p> <p><b>10 Zurück in die Treasury-Zukunft</b><br/>Ausblick auf das diesjährige Finanzsymposium</p> <p><b>12 Entscheidungsfindung zur SWIFT-Anbindung</b><br/>Die Optionen übersichtlich dargestellt</p> <p><b>15 Champions League statt Kreisklasse</b><br/>Interview mit Nils Ostendorf, Director Global Treasury bei IFCO, zu seiner Erfahrungen mit der SWIFT-Anbindung</p> | <p><b>18 „Wir haben den Bedarf erkannt“</b><br/>Interview mit Ralf Klein, Senior Account Director Corporates bei SWIFT</p> <p><b>20 Die „Großen“ geben den Takt vor</b><br/>Learnings aus dem Treasury-Summit 2020</p> <p><b>22 Sustainable Finance:</b><br/>Nicht „grün“ = „braun“?</p> <p><b>26 Der Aufstieg von Ransomware</b><br/>Zum Leidwesen der Unternehmen werden Cyber-Angriffe immer professioneller</p> <p><b>28 Voll digitalisiertes Garantiegeschäft</b><br/>Interview mit Ludgar Janßen, Geschäftsführer bei Digital Vault Services</p> <p><b>30 Neuer Partner, neue Fachabteilung</b><br/>Informationen in eigener Sache</p> |
|--|--|

**Offenlegung nach § 25 Mediengesetz: Herausgeber + Medieninhaber:** Schwabe, Ley & Greiner Gesellschaft m.b.H., Beratung, Gertrude-Fröhlich-Sandner-Straße 3, 1100 Wien, Österreich, Tel.: +43-1-585 48 30, Fax: +43-1-585 48 30-15, E-Mail: info@slg.co.at, URL: www.slg.co.at **Geschäftsführer:** Jochen Schwabe, Christof Ley, Utz Greiner, Martin Winkler, Georg Ehrhart, Philip Tüttö **Grundlegende Richtung:** Unabhängige und objektive Information für Finanzverantwortliche, Treasurer und Banker im deutschsprachigen Raum **Autoren und Mitarbeiter in dieser Ausgabe:** Johannes Asamer, Günther Bauer, Thomas Dirnbauer, Georg Ehrhart, Bernhard Kastner, Oliver Lipusz, Hannes Lorenz, Gudrun Schmid, Thomas Schörner, Philip Tüttö, Cornelia Wenny, Fabian Zaiser **Produktion und Anzeigenverwaltung:** Schwabe, Ley & Greiner **Grafische Umsetzung:** dolezal:media, Susanne Dolezal-Ortner **Druck:** Print Alliance HAV Produktions GmbH, Druckhausstraße 1, 2540 Bad Vöslau **Auflage:** 18.000 Stück. Namentlich gekennzeichnete Beiträge müssen nicht der Meinung der Redaktion entsprechen.

TreasuryLog ist auch online zu lesen auf [www.slg.co.at/Publikationen](http://www.slg.co.at/Publikationen)



## Risikopositionsermittlung – „Den Beipacktext sorgfältig lesen ...“

„Eighty percent of the job in foreign-exchange exposure management is analyzing what the exposures are and staying on the top of the change, which happens all the time. That's the dog work of the business – identifying what the true exposures are.“  
Ein Zitat von C. Weller von Duracell, dem wir nach unserem FX-Risiko Projekt bei der Cheplapharm Arzneimittel GmbH mehr als nur zustimmen können.

### Der Autor:



**Fabian Zaiser**  
ist Berater bei  
Schwabe, Ley &  
Greiner

Zunächst deutete vieles auf einen Standardprozess bei der FX-Risikoquantifizierung hin. Cheplapharm hat Verkäufe, die durch ihre lokalen Vertriebspartner in der dortigen Währung erfolgen, ohne über eigene Tochtergesellschaften im jeweiligen Land zu verfügen. Die Cashflows aus den Umsätzen fließen damit in die Risikoposition des Konzerns mit ein. So oder so ähnlich verlief die Identifikation der Cashflows für die meisten Quellen. Einkäufe, Debitoren- und Kreditorenzahlungen sowie die M&A-Transaktionen in Fremdwährung konnten im Laufe des Projekts identifiziert werden. Treasury-Zahlungen waren ohnehin im erst kürzlich eingeführten Treasury System (TMS) enthalten.

### SAP FI und SAC als Datenbasis für kurz und langfristige Planung

Dies ist allerdings nur der erste Schritt, müssen doch die tatsächlichen Geldwertungsfaktoren ebenso berücksichtigt werden. Ein für Januar budgetierter Eingang von 20.000 USD bedeutet nicht, dass man dieses Geld auch im selben Monat einnimmt. Die Debitoren- und Kreditorenzahlungen werden täglich mit den enthaltenen Fälligkeiten aus SAP exportiert und ins TMS, sowohl für die kurzfristige Disposition als auch für die Risikopositionsermittlung, übernommen. Die überfälligen Forderungen und Verbindlichkeiten wurden den Erfahrungen entsprechend in den ersten Monat geschoben.

Etwas schwieriger war die Analyse bei den Plancashflows. Hier wurden nach Kunden und Medikamenten verschiedene Zahlungsziele festgelegt. Die Sales Planung steht in der SAP Analytic Cloud (SAC) zur Verfügung was nahe legt, auch die Zahlungsziele dort zu hinterlegen, ebenso die Risikowährungen. Leichter war es bei den M&A-Zahlungszielen, da diese exakt in den Verträgen spezifiziert werden.

Es folgt der dritte Schritt: die Berücksichtigung des Risikohorizonts je Währung. Wie lange ist Cheplapharm im Risiko? Dazu wurde identifiziert, wie oft Preise angepasst werden können. Je länger der Zeitraum der Preisfixierungen ist, desto länger ist auch der Risikohorizont. Da wurden durchaus deutliche Unterschiede festgestellt: Während die meisten Produkte jedes Jahr neu angepasst werden können, gab es auch solche mit einer Preisfixierung auf drei Jahre. Als Ergebnis der Analyse wurde ein standardisierter Prozess eingeführt. Dieser identifiziert die Risikopositionen auf Basis der währungsdifferenzierten Liquiditätsplanung. Die individuellen Geldwertungsfaktoren berechnen das Cashflow Datum und anschließend werden sie mit dem richtigen Risikohorizont in die Berechnung überführt.

### Wo USD drauf steht ist nicht USD drinnen...

Oberflächlich betrachtet, hätte man das Projekt an diesem Punkt abschließen können. Es ist jedoch rat-

sam, jedes Geschäftsmodell auf Abweichungen vom Standard zu untersuchen. Und eine solche Besonderheit gibt es auch bei Cheplapharm: die sogenannten Erlöse aus „Transitional Services Agreements“ (TSA). Dabei kauft Cheplapharm bereits auf dem Markt existierende Medikamente und nimmt diese langfristig in das eigene Portfolio auf.

Während der Laufzeit der TSA-Verträge hat Cheplapharm zwar die offizielle Lizenz des Produkts erworben, allerdings wickelt der ursprüngliche Hersteller nach wie vor noch den Vertrieb ab. Einmal im Monat werden die Verkäufe abgerechnet und der Erlös dann häufig in USD oder CHF an Cheplapharm bezahlt.

Der Haken an der Sache ist folgender: Die Cashflow-Währung, die in den TSA-Verträgen geregelt ist, ist nicht die Risikowährung. Cheplapharm erzielt aus diesen Vereinbarungen zwar Einnahmen in USD oder CHF, allerdings werden die Verkäufe lokal durch den ursprünglichen Hersteller überwiegend in der lokalen Währung berechnet. Wieviel EUR Cheplapharm schlussendlich einnimmt, hängt also nicht nur vom Wechselkurs EUR zu der Abrechnungswährung ab, sondern auch vom Wechselkurs zwischen der lokal eingenommenen Währung und der Abrechnungswährung.

Zeitlich sieht es so aus: Der ehemalige Lizenzinhaber verkauft das Medikament im Markt und nimmt einen bestimmten Betrag ein. Am Ende des Monats wird der Umsatz bekanntgegeben und 30 Tage später fließt dieser in der Abrechnungswährung bei Cheplapharm ein. Daraus ergeben sich aus einem individuellen Zahlungseingang zwei verschiedene Risikopositionen. Zum einen eine Long-Position – also ein Zahlungseingang – in der lokalen Verkaufswährung gegenüber der Abrechnungswährung, mit dem Horizont des Umsatzmonats. 30 Tage später entsteht eine Long-Position in

der Abrechnungswährung gegenüber der lokalen Verkaufswährung. Das Risiko der Abrechnungs- und damit der tatsächlichen Cashflow-Währung besteht daher nur für einen Monat in der Zukunft.

### Fundierte Basis für die Risikoberechnung und Hedge Simulation

Die so ermittelten Cashflows und Exposures werden im TMS System von Technosis verwaltet, wo auch die Liquiditätsplanung daraus berichtet wird. Die als Exposure gekennzeichneten Risikopositionen werden anschließend in die SLG RiskEngine importiert. Dort wird die Risikoberechnung sowie die Simulation der erforderlichen Hedges durchgeführt. Durch die vielen unterschiedlichen Währungen zeigt sich der „Nutzen“ des Korrelationseffektes, womit die Absicherungsvolumina entscheidend reduziert werden. Die Risikosteuerung erfolgt auf Basis eines festgelegten Gesamtrisikos, das als Prozentsatz des Ergebnisses definiert ist.

Rückblickend kann man dem einleitenden Zitat voll zustimmen: Ein Großteil des Projekts galt der korrekten Identifizierung der Risikopositionen. Wenn diese Ermittlung falsch ist, so ist jede noch so gut überlegte Absicherungsstrategie nicht zielführend, vielleicht sogar kontraproduktiv, da sie von falschen Zahlen ausgeht.

Ein weiteres Mal hat sich in diesem Projekt gezeigt, wie gefährlich es sein kann, nur der Cashflow-Währung allein zu folgen. Unternehmen haben verschiedene Geschäftsmodelle, die berücksichtigt werden müssen. Indirekte Währungsrisiken werden dabei oft nicht bedacht. Deswegen der Ratschlag: Zeit und Know-how in eine detaillierte Vorbereitung und Analyse aller Cashflow-Arten stecken, sowie das Geschäftsmodell und die Systematik im Detail analysieren – damit die Risikoposition dann auch wirklich passt. ▲

**Jens Remmers**, Head of Treasury & Investor Relations bei Cheplapharm Arzneimittel GmbH



**Christian Plottke**, Investor Relations & Treasury, Cheplapharm Arzneimittel GmbH



### Über CHEPLAPHARM

CHEPLAPHARM ist ein deutsches Pharmaunternehmen mit Hauptsitz in Greifswald, das Marken- und Nischenprodukte in über 120 Ländern weltweit anbietet. Das Unternehmen in Familienbesitz ist auf ausgewählte Wirkstoffe und Indikationen spezialisiert und legt seinen Fokus auf eine international ausgerichtete Buy-And-Build-Strategie. In enger Zusammenarbeit mit seinen Geschäftspartnern erzielt CHEPLAPHARM nachhaltige jährliche Wachstumsraten. Es gehört seit Jahren zu den wachstumsstärksten Pharmaunternehmen Europas. Geldeingänge sowie -ausgänge können somit in mehr als 50 verschiedenen Währungen anfallen. FX-Risiko-Management ist daher für Cheplapharm von großer Bedeutung.

Weitere Informationen finden Sie unter [www.cheplapharm.com](http://www.cheplapharm.com).

**Pressestelle:** CHEPLAPHARM Arzneimittel GmbH, Ziegelhof 24, 17489 Greifswald, [presse\(at\)cheplapharm.com](mailto:presse(at)cheplapharm.com)

# Zinsrisiko im Niedrigzinsumfeld

Wenn die Zinsen unter dem Nullpunkt verharren, wird aus variabel defacto auch fix. Dabei kann es sinnvoll sein, sich jetzt fixe Zinsen zu sichern.

Der Autor:



**Bernhard Kastner**  
ist Manager bei  
Schwabe, Ley &  
Greiner

**W**ir leben im Euroraum schon seit Mitte 2015 mit negativen Geldmarktzinsen. Die längerfristigen Zinsen, wie die Swap-Sätze, sind nun bis zu einer Laufzeit von 15 Jahren ebenfalls negativ. Damit stellt sich die Frage, welche Konsequenz das auf das Zinsrisiko-Management haben kann. Wie hoch ist das Cashflow-Risiko tatsächlich, wenn der 3-Monats-Euribor steigt, wenn gleichzeitig die Finanzierung bei einem Floor von 0 Prozent abgeschlossen wurde? Wie ändert sich das Barwertrisiko dadurch? Wäre es nicht sinnvoll, jetzt eher eine langfristige Zinsbindung einzugehen, um das negative Niveau zu sichern und wie sichert man ein variables Darlehen mit einer Zinsuntergrenze bei 0 Prozent?

## Was ist eigentlich variabel?

Führte bis vor einiger Zeit ein Anstieg der kurzfristigen Zinsen zu höheren Zinskosten bei einem variabel verzinsten Darlehen, so gilt das momentan nur bedingt. Bei einem Zinssatz von minus 0,5 Prozent müsste dieser um mehr als 50 Basispunkte steigen, damit bei einem Darlehen mit Zinsuntergrenze von 0 Prozent die Zinskosten höher werden. Damit führen aber alle Zinsänderungen die kleiner als 0,5 Prozent sind (oder wenn die Zinsen weiter sinken) zu keiner Änderung der zu bezahlenden Zinsen. Von variabler Verzinsung kann damit nicht wirklich gesprochen werden.

Diese Situation hat natürlich eine Auswirkung auf das Zinsrisiko. Die Tabelle (generiert mit der SLG-RiskEngine) zeigt ein Finanzierungsportfolio mit verschiedenen Zinsbindungen. Positionen mit variabler Verzinsung sind in der ersten Spalte (< 1 Jahr) zu sehen. Diese führen zu einem Cashflow-Risiko von TEUR 303. Wird die Zinsuntergrenze als eingebetteter Floor für das Darlehen von EUR 250 Mio.

berücksichtigt, so reduziert sich das Risiko auf TEUR 64. Auf der anderen Seite steigt aber das Wertrisiko um EUR 0,9 Mio. an, da der Marktwert des Floors einem Barwertrisiko ausgesetzt ist. Gibt es Limits für Cashflow- und Barwertrisiko, so ist der Floor mit einzubeziehen. In der Marktwertbetrachtung des Finanzportfolios zeigt sich, dass durch den Floor der negative Barwert höher ist (EUR -851 Mio. vs. EUR -861 Mio.).

Geht man davon aus, dass die Geldmarktzinsen in naher Zukunft negativ bleiben, so sind auch die variablen Finanzierungen als fix anzusehen. Allerdings sind Zinserhöhungen ja keineswegs ausgeschlossen. Ein Anstieg der Zinsen in ein paar Jahren ist nicht unrealistisch. Deshalb kann es durchaus sinnvoll sein, jetzt das geringe Zinsniveau durch fest verzinsten Darlehen zu fixieren bzw. variable Darlehen zu sichern – sofern die Zinsrisiko-Limits das erlauben.

## Sicherung eines variablen Darlehens mit Zinsuntergrenze

Diese Sicherung des aktuellen niedrigen Zinsniveaus kann durch einen Zins-Swap erreicht werden. Die Ausgestaltung des Zins-Swaps sollte zu den zu sichernden Darlehen passen. Ist das Darlehen beispielsweise an den 3-Monats-Euribor gebunden, so ist ein Payer-Swap abzuschließen, bei dem die fixen Zinsen an die Bank zu zahlen sind und man den 3-Monats-Euribor erhält.

Hat das Darlehen eine Zinsuntergrenze bei 0 Prozent, also einen Floor mit dem Strike 0 Prozent, sollte auch die variable Seite des Swaps einen entsprechenden Floor aufweisen. Allerdings ist für die Zinsoption eine Prämie zu zahlen. Diese Prämie kann zu Beginn vollständig bezahlt werden (upfront) oder

EUR-Zinsen im Zeitverlauf seit Anfang 2008

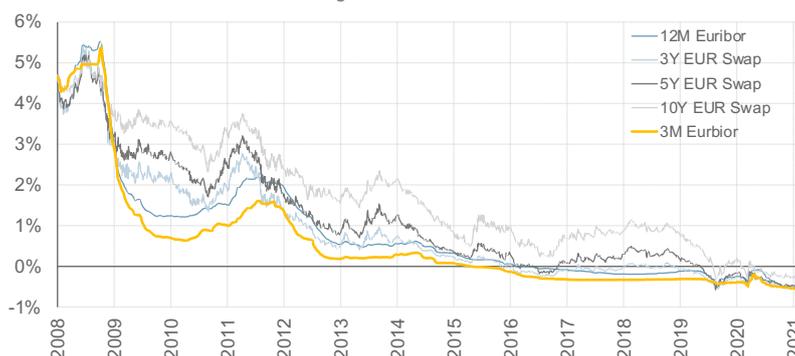


Abb. 1: **Zinsentwicklung**

Die Geldmarktzinsen (wie 3-Monats-Euribor) sind schon seit einigen Jahren negativ. Hinzu kommt, dass nun auch die längerfristigen Zinsen (z. B. 10-Jahres-Swapsatz) ebenfalls negativ sind (Quelle: Refinitiv).

## Zinsbindungsbilanz

	Nominale nach Zinsbindung					Gesamt	Zinszahlungen		Marktwertsensitivität	
	< 1 Jahr	1 - 3 Jahre	3 - 5 Jahre	5 - 10 Jahre	> 10 Jahre		in TEUR	in %	Barwert	Modified Duration
Kontokorrent-Konten	14.290	0	0	0	0	14.290	0	0,00%	14.302	0,08
Festgelder	35.000	0	0	0	0	35.000	12	0,04%	35.088	0,25
Summe Finanzaktiva	49.290	0	0	0	0	49.290	12	0,02%	49.390	0,20
Kontokorrent-Konten	-600	0	0	0	0	-600	0	0,02%	-601	0,08
Bankdarlehen	-250.000	-38.000	-200.000	-38.000	0	-526.000	-4.263	0,81%	-546.518	2,59
Anleihe	0	0	0	0	-300.000	-300.000	-4.500	1,50%	-353.860	9,40
Summe Finanzpassiva	-250.600	-38.000	-200.000	-38.000	-300.000	-826.600	-8.763	1,06%	-900.979	5,26
<b>Netto vor Derivate</b>	<b>-201.310</b>	<b>-38.000</b>	<b>-200.000</b>	<b>-38.000</b>	<b>-300.000</b>	<b>-777.310</b>	<b>-8.751</b>	<b>1,13%</b>	<b>-851.589</b>	<b>5,56</b>
Zins-Floors (eingebettet)	250.000	0	0	0	0	250.000	-1.225	-0,49%	-6.750	
<b>Netto nach Derivate</b>	<b>48.690</b>	<b>-38.000</b>	<b>-200.000</b>	<b>-38.000</b>	<b>-300.000</b>	<b>-527.310</b>	<b>-9.976</b>	<b>1,89%</b>	<b>-858.339</b>	<b>5,56</b>

## Zinsrisiko diversifiziert

	Cashflow-Risiko vor Derivate	Wertrisiko vor Derivate	Cashflow-Risiko nach Derivate	Wertrisiko nach Derivate
Zinsrisiko	303	38.033	64	38.916

## Abb. 2: Zinsrisikobericht der SLG-RiskEngine

Das Finanzportfolio besteht aus kurzfristig verzinsten Anlagen und Finanzierungen (< 1 Jahr), sowie aus Finanzierungen mit einer Zinsbindung > 1 Jahr. Durch den eingebetteten Floor in der variablen Finanzierung reduziert sich das Cashflow-Risiko von TEUR 303 auf TEUR 64 und das Wertrisiko steigt um etwa EUR 0,9 Mio.

(und das wird von Banken wesentlich häufiger angeboten) sie wird in den Fixzinssatz eingepreist. Der Fixzinssatz ist also höher.

Ein Zins-Swap für fünf Jahre weist aktuell einen Zinssatz von etwa minus 0,45 Prozent auf. Die Prämie für einen entsprechenden Floor beträgt etwa 2,7 Prozent upfront bzw. 0,52 Prozent pro Jahr. Das führt zu einem Festzinssatz von plus 0,07 Prozent bei einem Floor bei 0 Prozent. Diese Berechnung basiert auf Interbanksätzen und wäre noch durch Bankmargen zu ergänzen. Der fixierte Gesamtzins-

satz (ohne Margen) beträgt 0,07 Prozent anstatt 0 Prozent variabel (solange die Zinsen negativ sind) für eine Laufzeit von fünf Jahren.

Es ist also möglich, bei dem aktuell sehr niedrigen Zinsniveau ein variabel verzinstes Darlehen zu einem leicht positiven Zinssatz zu fixieren. Allerdings ist dafür eine Prämie zu bezahlen, die in einen Festzinssatz üblicherweise eingerechnet wird. Gerne unterstützen wir Sie bei der Analyse des Zinsrisikos und bei der Festlegung einer Zinsrisiko-Strategie in diesem Niedrigzinsumfeld. ▲

Einfach. Sicher. Flexibel.  
Erfahren. Persönlich.

trinity

YOUR TREASURY. YOUR WAY. OUR SOFTWARE.

Professionelles Treasury für den Mittelstand – schnell eingeführt

[www.trinitytms.com](http://www.trinitytms.com)



Digitalisierung und Automatisierung im Treasury reduzieren die Bedeutung der herkömmlichen Funktionentrennung.

## Wie passt ein Roboter in die Funktionentrennung?

Die Funktionentrennung soll sicherstellen, dass unvereinbare Tätigkeiten nicht miteinander vermischt werden. Es wird sorgfältig unterteilt in Handel, Abwicklung und Risiko-Controlling. Durch den technologischen Fortschritt ist es heute allerdings möglich, viele Prozessschritte zu automatisieren. Kann aber angesichts fortschreitender Automatisierung und Digitalisierung auch die gewohnte dreiteilige Aufstellung mit Front-, Middle-, und Back-Office über Bord geworfen werden?

Der Autor:



**Günther Bauer**  
ist Partner bei  
Schwabe, Ley &  
Greiner

„Das Treasury ist nach dem Prinzip der Funktionentrennung aufgebaut und umfasst Front- (FO), Middle- (MO) und Back-Office (BO).“ So oder so ähnlich ist die Aufbauorganisation in vielen Großkonzernen beschrieben. Kleinere Unternehmen, mit geringerer Personalausstattung, streben eine ähnliche Aufstellung an, erreichen diese aber meist nur durch Einbeziehung weiterer Abteilungen. Das kann beispielsweise das Rechnungswesen sein.

Damit soll sichergestellt werden, dass alle Transaktionen ordnungsgemäß erfasst, bewertet und abgewickelt werden. In Anlehnung an die Bankenwelt hat das Prinzip der Funktionentrennung eine lange Tradition. Damals, in Zeiten von papierhaften Händlerzetteln, eingeschränktem Zugriff auf Systeme und vielen intransparenten Prozessschritten, war das natürlich eine sehr sinnvolle Gliederung. Und dass mangelhafte Kontrollen zu Missbrauch und finanziellen Schäden geführt haben, belegen nicht zuletzt diverse Beispiele aus der Vergangenheit, wie Bearings Bank, Metallgesellschaft oder Société Générale.

### Digitalisierung führt zu erhöhter Transparenz

Angesichts des steigenden Digitalisierungsgrades vieler Treasury-Prozesse konnte die Transparenz deutlich erhöht werden. Handelsgeschäfte, die früher per Telefon abgeschlossen und mühsam papierhaft dokumentiert wurden, werden heute über internetbasierte Plattformen, die alle Vergleichsangebote transparent und übersichtlich darstellen, gehandelt. Bestätigungen, früher per Fax von den jeweiligen Geschäftspartnern übermittelt, sind heute in Matching-Plattformen mit allen Details für jeden berechtigten Nutzer sichtbar. Auch die notwendigen Zahlungen müssen nicht mehr manuell erstellt werden, sondern je nach Kontrahent und Währung wird auf manipulationssichere Vorlagen zugegriffen.

In Treasury-Systemen werden alle Informationen gebündelt. Dies erfolgt idealerweise über automatische Schnittstellen – und nicht durch manuelle Eingaben. Dadurch werden einerseits Fehleranfälligkeit und Manipulationsmöglichkeiten minimiert und andererseits die Arbeitsbelastung reduziert. Das System

nimmt auch meist eine automatisierte Bewertung und Buchung der Geschäfte vor. Diese wurden bei der Implementierung aufgesetzt, vom Prüfer abgenommen und greifen auf importierte Marktdaten zurück.

Und jeder Nutzer, der über die entsprechenden Berechtigungen verfügt, kann alle Informationen im System jederzeit einsehen. Das gilt auch für etwaige Änderungen während der Laufzeit. Zusätzlich kann über Kontroll- bzw. Audit-Berichte überprüft werden, ob vordefinierte Prozesse auch eingehalten werden.

### Automatisierung ersetzt manuelle Prozessschritte

Dieses idealtypische Beispiel zeigt, dass durch Digitalisierung und Automatisierung die traditionelle Funktionentrennung in der Tat obsolet wird. Wenn Handel, Abwicklung und Risiko-Controlling durch den „Roboter“ erfolgen, sind dafür auch keine separaten Bereiche mehr notwendig.

Aber ist tatsächlich für alle Treasury-Geschäfte ein solch hoher Automatisierungsgrad umsetzbar? Und wer kümmert sich um Ausnahmen, wenn diese dann doch auftreten?

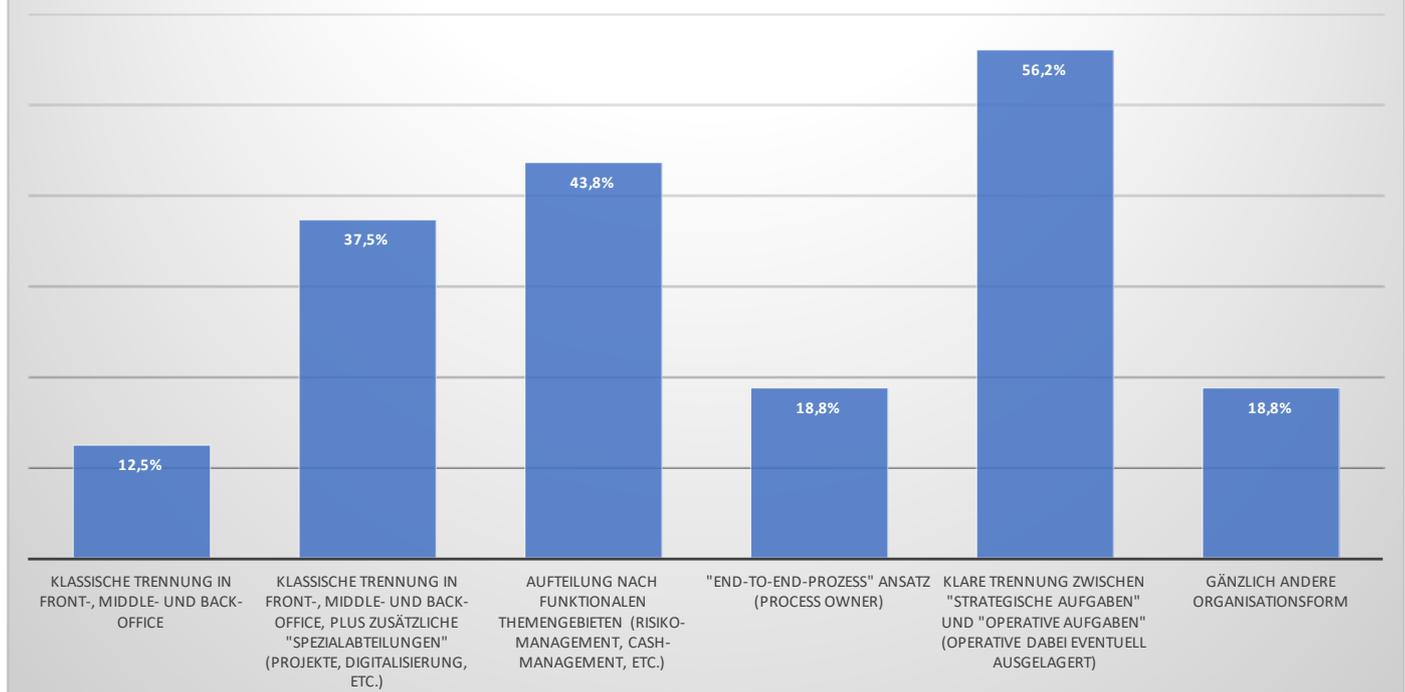
Bei der Neustrukturierung einer Treasury-Abteilung sollte man also nicht nur den simplen Idealfall – meist der Prozess der FX-Sicherungen – vor Augen haben. Vielmehr sollte man auch Prozesse berücksichtigen, die (noch) keinen so hohen Automatisierungsgrad aufweisen. Und oftmals beginnt dieser geringere Grad an Automatisierung bereits bei Zinsderivaten, die dann doch telefonisch gehandelt und manuell bestätigt werden müssen.

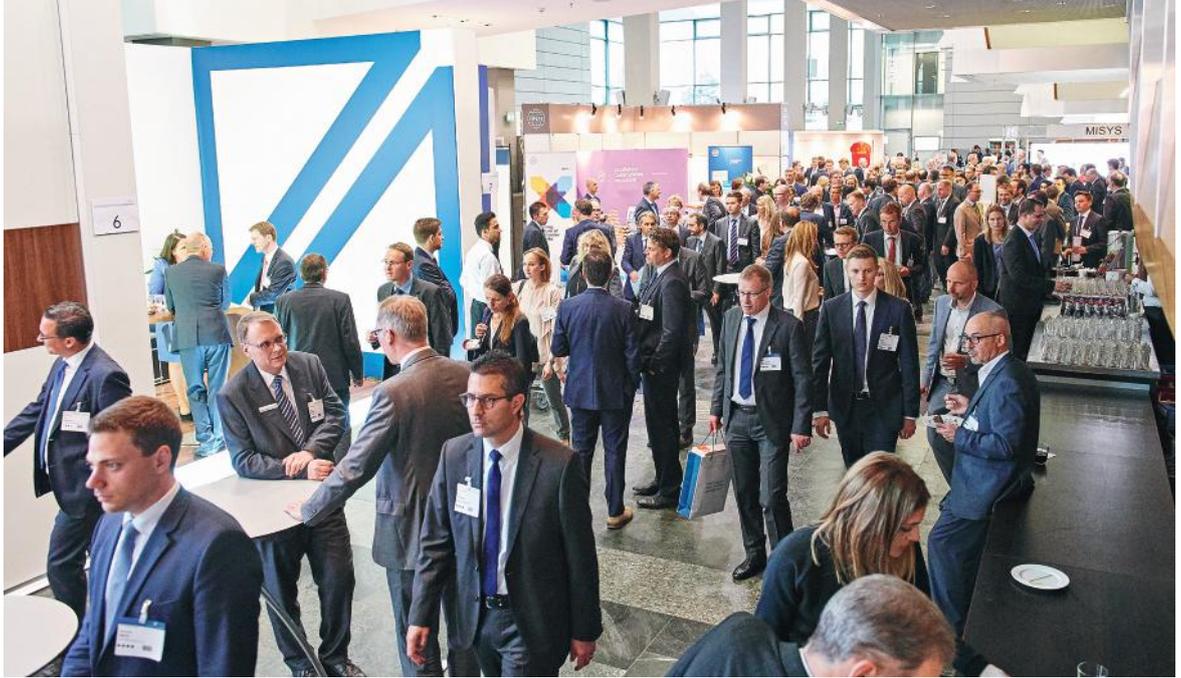
### Treasury-Organisationen im Wandel

Diese differenzierte Betrachtungsweise spiegelt sich auch in den Ergebnissen einer Befragung wider, die wir im Zuge des letztjährigen Treasury Summits bei den 17 teilnehmenden Großunternehmen durchgeführt haben. Eine Beibehaltung der klassischen Trennung zwischen Front-, Middle- und Back-Office wird von 50 Prozent der Teilnehmer für das Jahr 2025 vorhergesagt. Der Rest der Befragten geht von Unterteilungen eher nach inhaltlichen Themen oder einer Unterscheidung zwischen strategischen und funktionalen Aufgaben aus.

Die Umfrage ist aufgrund ihrer geringen Grundgesamtheit natürlich nicht repräsentativ, zeigt aber dennoch eine Tendenz: In vielen Bereichen wird durch Digitalisierung und Automatisierung die Funktionentrennung an Bedeutung verlieren. Dafür treten strategische Fragestellungen vermehrt in den Vordergrund. Solange aber Automatismen nicht für alle Treasury-Prozesse durchgängig umgesetzt sind, wird ein vollständiger Verzicht nicht darstellbar sein. Die digitalen Möglichkeiten müssen sich somit noch weiter verbreitern, um wirklich disruptive Änderungen zu bewirken. ▲

## Wie wird Ihre Treasury-Funktion im Jahr 2025 organisiert sein?





# Zurück in die Treasury-Zukunft

Wie veranstaltet man ein Finanzsymposium in begegnungsfeindlichen Zeiten? Indem man es neu erfindet. Wie wir die Treasury-Community in diesem Jahr zusammenbringen.

## Die Autoren:



**Thomas Schörner**  
ist Partner bei  
Schwabe, Ley &  
Greiner



**Oliver Lipusz**  
ist Leiter Events bei  
Schwabe, Ley &  
Greiner

**S**ich unter Treasurern per Handschlag in Mannheim begrüßen – das war zuletzt 2019 möglich. Jetzt, 2021, fahren wir unser Finanzsymposium wieder hoch, mit allem, was uns an Technik und Ideenreichtum zur Verfügung steht. Vergessen Sie alles, was Sie im vergangenen Jahr an virtuellen Veranstaltungen gesehen oder besucht haben – das „Finanzsymposium 4.0“ nimmt das Konferenzgeschehen der Zukunft vorweg.

Als Teilnehmer bewegen Sie sich aktiv im Geschehen, anstatt zum Videokonsumenten zu mutieren. Für dieses Vor-Ort-Gefühl haben wir diverse Formate entwickelt, die dafür sorgen, dass Sie auf der virtuellen Konferenz so ähnlich kommunizieren können wie live im Kongresszentrum in Mannheim. Wenn Sie ab Mittwoch, 21. April um 11 Uhr den Startknopf drücken, sind Sie an allen Schauplätzen dabei, auf einer einzigen Plattform, ohne zusätzliche Logins. Sollte Ihnen das Programm zu dicht erscheinen, oder Sie zwischendurch vom Tagesgeschäft eingeholt werden, ist das auch kein Problem. Wir stellen Ihnen alle Inhalte das ganze Jahr zur Verfügung. Treasury- 365 sozusagen, wobei Sie bestimmen, was Sie wann konsumieren wollen.

## **Parship für Treasurer: Die richtigen Menschen, Ideen und Ressourcen gezielt zusammenzubringen**

In diesem Jahr verkuppeln wie Sie nach allen Regeln der Kunst! Wir legen es zwar nicht darauf an, dass sich unsere Kunden gleich „paarweise verabschieden“, sehr wohl aber werden wir „Matchmaking“ unter Gleichgesinnten betreiben: Jeder Besucher und Aussteller gibt im Zuge der Anmeldung seine fachspezifischen Interessen bzw. Angebote bekannt; die

Themenauswahl dringt dabei in sämtliche Spezifika der allgemeinen Treasury-Bereiche vor, von Unternehmensfinanzierung über Risiko-Management bis Digitalisierung. Ein Matchmaking-Tool sondiert die Übereinstimmungen und schlägt Ihnen Vorträge, Aussteller und Treasurer-Kollegen zum virtuellen Treff vor, sei es zu zweit oder in einer exklusiven Gruppe: So können bis zu 15 Personen im „Treasury Café“ über die aktuellen Herausforderungen diskutieren, von denen sich im abgelaufenen Jahr mehr als genug angesammelt haben dürften.

## **Interviews mit Mehrwert fürs Treasury**

Mit dem neuen Format „Studio-Interview“ laden wir Experten zu Gesprächen, die das gesamte Treasury-Spektrum ausleuchten, aber auch thematisch erweitern: Neben CFOs, die herausragenden Treasury-Teams vorstehen, äußern sich Fachleute aus Nicht-Treasury-Bereichen wie virtuelles Marketing, Volkswirtschaft oder Gesundheit, etwa dazu, wie Kommunikation und Personalführung in virtuellen Räumen funktionieren. Aspekte, die über den Tellerrand von Treasury hinausblicken lassen. Ein weiteres Interviewformat, diesmal mit „Zwischenruffunktion“, finden Sie bei den Anbietern selbst: Diese stehen sowohl dem Interviewer (in bewährter Moderatorenrolle: TV-Präsenter Markus Brock) als auch den Besuchern Rede und Antwort zu ihren Dienstleistungen.

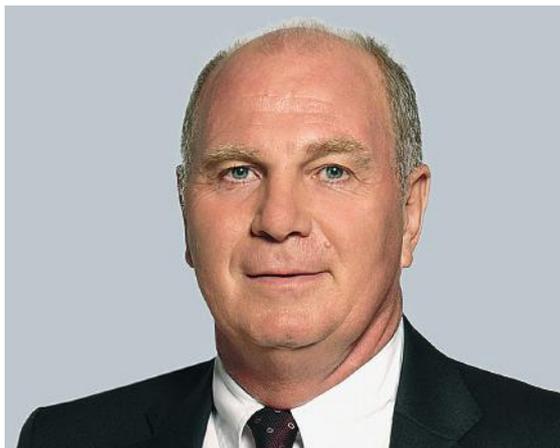
## **Im Dialog mit Hoeneß und Gabriel**

Das langbewährte Grundgerüst des Finanzsymposiums behalten wir aber bei – zum Teil auch vor Ort auf den Bühnen im Kongresszentrum in Mannheim. Renommierte Treasury-Praktiker diskutieren auf den Foren zu Treasury-Kernfragen und Technology

& Innovation vor breitem virtuellen Publikum, Systemanbieter und Banken stellen gemeinsam mit Kunden ihre Lösungen in Workshops vor. Zur Abrundung der Veranstaltung haben wir wieder prominente Gastredner eingeladen: Den Auftakt am Mittwoch übernimmt FC Bayern-Legende Uli Hoeneß („Strategie und Führung im Sport und im Unternehmertum“), während der Ausklang am Freitag von einem politischen Schwergewicht gestaltet wird: Der ehemalige Bundesaußenminister Sigmar Gabriel spricht über das europäisch-amerikanische Verhältnis („Von der Luft- zur Zugbrücke“). Zusatzbonus der digitalen Teilnahme: Via Chat können Sie Ihre Fragen direkt an die Redner richten, wenn Sie als Zuhörer nicht im Abseits stehen oder mehr über transatlantische Befindlichkeiten wissen wollen.

### Digitalisierungs-Preis

Als Treasury-Berater sind wir laufend in Digitalisierungsprozesse unserer Kunden eingebunden und wissen daher zu würdigen, welche Initiativen effektiv sind. Beim diesjährigen Finanzsymposium wollen wir herausragende Leistungen in der digitalen Transformation einem breiten Publikum sichtbar machen und rufen die Auszeichnung „Digital Treasury Excellence“ ins Leben. Eine Jury, bestehend aus Digitalisierungsexperten der Treasury-Gemeinde, erstellt bis kurz vor dem Symposium eine Short-



Eröffnet am 21. April um 11 Uhr das Finanzsymposium: Gastredner Uli Hoeneß.

list aus den eingereichten Projekten – und Sie als Besucher küren im Laufe der Veranstaltung den Sieger. Den Preis überreichen wir bei der feierlichen Gala am Donnerstagsabend der Konferenzwoche.

### Feiern, aber „richtig“

Apropos Galaabend: Der wird auch dieses Jahr stattfinden. Unsere Events-Maschinerie entfaltet derzeit ihre geballte Kreativität, um Sie nicht nur mit Bits & Bytes abzuspeisen. Bleiben Sie am Donnerstagabend jedenfalls dran: Es wird wieder analog. ▽

# corima

Das modulare Software-System für die Umsetzung von Lösungen in sämtlichen Bereichen von Treasury und Corporate Finance

Front office Back office

- Management von Finanzierungsgeschäften (Darlehen und Eventualverbindlichkeiten)
- mit Berücksichtigung flexibler Zins-, Kapitalzahlungs- und Gebührenstrukturen
- sowie Covenant-Vorgaben und Hinterlegung von Sicherheiten
- eingebunden in die unterliegenden Kreditlinien
- zur Verwaltung und Verbuchung der unternehmensweiten Finanzierungsposition

...in einem integrierten System



COPS GmbH  
Wien - Wetzlar - Hamburg - Prag  
info@corima.solutions  
www.corima.solutions

# corima

## corima

risk management back office

cash management liquidity planning

front office accounting





Es gibt verschiedene Optionen einer Anbindung ans SWIFT-Netzwerk. Um die optimale Lösung zu finden, bedarf es einer sorgfältigen Analyse.

## Entscheidungsfindung zur SWIFT-Anbindung: komplex aber machbar

Die Option einer SWIFT-Anbindung steht für viele Unternehmens-Treasurys im Raum. Die unterschiedlichen Umsetzungsmöglichkeiten und Unsicherheiten, die in vielen Berichten und Beratungsangeboten beispielsweise zum Thema Customer Security Programme geschürt werden, machen eine Entscheidung alles andere als einfach.

### Die Autorin:



**Gudrun Schmid**  
ist Partner bei  
Schwabe, Ley &  
Greiner

Der „Choice Overload“ beschreibt eine Theorie aus der Wirtschaftswissenschaft. Dieser besagt, dass Menschen von vielen Auswahlmöglichkeiten überfordert werden und als Reaktion oftmals gar keine Entscheidung treffen. Zu viele Optionen verwirren – das gilt vor allem, wenn es sich um komplexe Zusammenhänge handelt. Die Frage der optimalen Bankanbindung gehört sicherlich zu dieser Kategorie und – leider – gibt es auch hier mehr als eine Variante.

Unternehmen im DACH-Raum steht mit dem Electronic Banking Internet Communication Standard (EBICS) eine kostengünstige Möglichkeit zur direkten Anbindung ihrer lokalen Banken und oft auch deren weltweiter Niederlassungen zur Verfügung. Diese reicht bei einem globalen Footprint in der Regel aber nicht aus. Eine Anbindung an das

SWIFT-Netzwerk wird allerspätestens dann relevant, wenn ausgehende Zahlungen über unterschiedlichste nicht EBICS-fähige Banken eine kritische Masse erreichen.

Die Vielzahl der konkreten Umsetzungsmöglichkeiten machen die Frage nach dem „Wie?“ aber einigermaßen komplex. Für das Gros der Unternehmen ist hier nur eines schnell klar: Für eine eigene, intern betriebene SWIFT-Infrastruktur („Alliance Access“) gibt es weder den Bedarf noch einen Business Case. In die nähere Auswahl kommen zumeist die folgenden Alternativen:

- ▲ SWIFT Alliance Lite2 (AL2) bzw. neu SWIFT Alliance Cloud (AC)
- ▲ SWIFT Lite for Business Applications (L2BA)
- ▲ SWIFT Service Bureaus (SSB)

Anbindungsvariante	SWIFT Alliance Lite2 (AL2)*	SWIFT Lite for Business Applications (L2BA)	SWIFT Service Bureau (SSB)
Was ist das?	SWIFT-eigene Cloud, die in die im Unternehmen genutzten ERP bzw. TMS integriert werden kann	in bestehende Systemlösungen voll integrierter Alliance Lite-Zugang	Nutzung der SWIFT-Infrastruktur eines SWIFT-zertifizierten Service Bureaus („shared infrastructure“)
Wer sind die für den Unternehmens-Zahlungsverkehr relevanten Anbieter?	SWIFT	u. a. TMS- und ZV-Anbieter wie z.B. Bellin, Kyriba, SAP, Serrala, TIS	im DACH-Raum v. a. Bottomline, Broadridge, EFiS, Fides, FIS, Finastra, van den Berg
Ist die Lösung für den Zahlungsverkehr ohne zusätzliche Software nutzbar?	Nein – AL2 benötigt ein zusätzliches Tool für die Zahlungsfreigabe.	Ja – Freigabe über integrierte ZV-Lösung	Abhängig vom Anbieter; in der Regel werden ZV-Lösungen geboten, meist jedoch mit begrenztem Funktionsumfang.
Wieviel Unterstützung bekommt der Kunde beim Customer Security Programme durch seinen Anbieter?	21 verpflichtende Kontrollen. Standard-Vorgaben und Support von SWIFT, der auch allen anderen Kunden (L2BA, SSB) zur Verfügung steht.	15 verpflichtende Kontrollen. Durch die Integration in die Anbieterlösung sind viele Kontrollen über die Standard-Architektur des Anbieters erfüllt. Die konkreten To-Dos auf Kundenseite sind begrenzt.	17 verpflichtende Kontrollen. SSBs arbeiten mit standardisierten Setups, die bereits viele der vorgegeben Kontrollen erfüllen. Der lokale Footprint beim Kunden ist aber durch z.B. die VPN-Anbindung an das SSB größer als bei L2BA.

Abb. 1: **Relevante SWIFT-Anbindungsvarianten für das Unternehmens-Treasury**

\* zukünftig SWIFT Alliance Cloud (AC)

Welche Lösung am besten passt, hängt dabei immer von den spezifischen Anforderungen und Gegebenheiten im Unternehmen ab. Aus unserer Erfahrung mit SWIFT-Auswahlprojekten wissen wir, dass die Entscheidungsfindung sehr anspruchsvoll ist und vor allem von folgenden Faktoren abhängt:

- ▲ Welche ERP-Systeme und Zahlungsverkehrsplattformen sind im Einsatz bzw. kommen in Frage?
- ▲ Sollen flexibel unterschiedliche Systeme an SWIFT angebunden werden?
- ▲ Wie ist die hauseigene IT aufgestellt?
- ▲ Sollen alle Zahlungen über SWIFT gehen oder parallel mehrere Kommunikationskanäle (EBICS, Host-to-Host) angesprochen werden?
- ▲ Sollen unterschiedliche Kommunikationskanäle über einen einheitlichen Weg genutzt werden oder ist auch ein intern gemanagter Parallelbetrieb denkbar?
- ▲ Reicht die eine Durchleitung von selbst erstellten Zahlungsformaten aus oder wird eine Formatkonvertierungen benötigt?
- ▲ Gibt es einen Bedarf an zusätzlichen Services, wie beispielsweise Sanction Screening oder „Reparatur“ eingehender Kontoauszüge?

Die komplexen Zusammenhänge und Details, die bei der Auswahl der passenden Architektur zu berücksichtigen sind, stellen für Treasurer eine große Herausforderung dar. Ein solches Projekt ist mit beträchtlichen Kosten verbunden und mit ambitionierten Zielen: Für das eigene Unternehmen soll eine passgenaue und kosteneffiziente Lösung gefunden und – noch viel wichtiger – ein

störungsfreier Ablauf im laufenden Betrieb mit überschaubarem Aufwand sichergestellt werden.

### Was ist im laufenden SWIFT-Betrieb eigentlich zu tun?

Sind die Hürden der Implementierung erst einmal überwunden, verbleiben im Rahmen der Betreuung des SWIFT-Kanals neben dem Monitoring der relevanten Schnittstellen im Wesentlichen die folgenden Aufgaben:

- ▲ Erfüllung der Anforderungen aus dem Customer Security Programme und jährliche Bestätigung dieser an SWIFT
- ▲ Verwahrung der Token und regelmäßig (alle zwei Jahre) Aktualisierung der Zertifikate

### SWIFT-Token und Zertifikate – wozu?

Jede SWIFT-Anbindung geht mit der Festlegung von zwei zu benennenden Administratoren, dem Right und dem Left Security Officer (meist abhängig vom SWIFT-Setup in der IT oder im Treasury), einher. Diese erhalten die für die Nutzung des SWIFT-Netzwerkes notwendigen Zertifikate, die sie alle zwei Jahre auf SWIFTnet verlängern müssen. Die einzige „Gefahr“ hier: Eine solche Verlängerung wird allzu gerne übersehen, und sind die Zertifikate erst einmal abgelaufen, müssen sie neu beantragt werden. Abgelaufene Zertifikate haben keine Konsequenzen für den Betrieb „as-is“, sind aber natürlich mit zusätzlichen Kosten verbunden.

Die Zertifikate selbst werden im Rahmen der Implementierung einmalig auf den persönlichen hardwaregeschützten Token (kein USB!) der Security Officers hinterlegt. Die Token werden für die User-Au-

thentifizierung für die unterschiedlichen SWIFT-Services benötigt.

Die SWIFT Security Officer sind auch gefragt, wenn neue Banken angebunden werden sollen: Sie hinterlegen die entsprechenden RMAs (Relationship Management Application) der Banken, mit denen über SWIFT Nachrichten ausgetauscht werden sollen, auf SWIFTnet. Für eine solche Anpassung sind gültige Zertifikate natürlich die Voraussetzung.

Bei einer SWIFT-Anbindung über ein SSB sind diese Tätigkeiten in der Regel an das SSB ausgelagert, vom Kunden selbst sind keine Security Officers gegenüber SWIFT zu benennen. Auch einzelne L2BA-Provider bieten die Übernahme dieser Aufgaben an – bzw. einzelne haben sie sogar fix vorgesehen. Bei einer AL2-Anbindung liegt die Verantwortung immer direkt beim Kunden selbst.

Das Token-Management ist übrigens eine der verpflichtenden Kontrollen, die im Rahmen des SWIFT Customer Security Programme (CSP) zu bestätigen sind: Token müssen hinsichtlich Ausgabe, Verwendung und Aufbewahrung ordnungsgemäß und nachverfolgbar verwaltet werden (z. B. durch Einsatz eines passenden Tools).

### **SWIFT Sicherheitsprogramm für den Kampf gegen Cyberattacken**

Das CSP wurde 2016 als Reaktion auf den Angriff auf die Zentralbank von Bangladesch ins Leben gerufen, um ein hohes einheitliches Sicherheitsniveau bei allen SWIFT-Nutzern zu gewährleisten. Spätestens seit 2018 müssen sämtliche SWIFT-Teilnehmer die Einhaltung der im SWIFT Customer Security Controls Framework (CSCF) vorgegebenen verpflichtenden Kontrollen über das SWIFT KYC-Portal bestätigen. Für Neukunden heißt das, dass ihr SWIFT BIC erst nach Abgabe des CSP live geschaltet wird.

2019 wurde mit dem „Independent Assessment Framework“ die Möglichkeit einer Selbstbescheinigung durch die operativ verantwortlichen Bereiche gestrichen. Seither ist die Durchführung durch eine unabhängige Stelle vorgesehen. Ursprünglich bereits für 2020 geplant, wurde die verpflichtende Attestation aufgrund von COVID-19 auf 2021 verschoben. Ab heuer ist die Compliance mit dem CSCF durch geeignete interne Einheiten der 2nd oder 3rd Line of Defense (z. B. Risiko-Management, Compliance oder Interne Revision) oder durch qualifizierte externe Prüfer zu bestätigen.

Der Umfang der von einem Unternehmen zu bestätigenden Kontrollen hängt vom „lokalen Footprint“ der gewählten SWIFT-Lösung ab. Am kleinsten ist dieser naturgemäß bei einer L2BA-Anbindung, gefolgt von der SSB-Anbindung, AL2 erfordert im direkten Vergleich die meisten Kontrollen.

Gerade L2BA-Provider und SWIFT Service Bureaus werden von SWIFT selbst auf Herz und Nieren geprüft, in Zusammenarbeit mit diesen muss ein Unternehmenskunde daher nur noch für den in der eigenen Umgebung verbleibenden Rest attestieren. Darüber hinaus bieten mehr und mehr L2BA- und SSB-Provider als Zusatzservice umfassende bis Rund-um-sorglos-Pakete zur CSP-Unterstützung an.

### **Übertriebener Arbeitsaufwand oder doch eine Selbstverständlichkeit?**

Die von SWIFT vorgegebene Liste der im Rahmen des CSP durchzuführenden verpflichtenden (22) und empfohlenen Kontrollen (9) ist erst einmal recht lang. Viele Punkte sind für den nicht Technikaffinen auch nicht sofort „griffig“.

Ein zweiter, genauerer Blick zeigt aber: Viele der Anforderungen würde jeder Treasurer in ähnlicher Form an seine Zahlungsverkehrslösung stellen. Token sollen vor fremdem Zugriff geschützt werden, der physische Zugang zu sensiblen Umgebungen beschränkt und protokolliert und eine Passwort-Policy einheitliche Qualitätsvorgaben festlegen. Richtlinien, die Funktionentrennung, 4-Augen-Prinzip und ein Least-Privilege-Prinzip für Rechtevergabe und Systemzugriff definieren, sind für viele eine Selbstverständlichkeit. Multifaktor Authentifizierung – gerade im Zahlungsverkehr – ist inzwischen ohnehin eine Mindestanforderung. Auch eine schriftliche Regelung für den Fernzugriff, die auch das Risiko des unbefugten Zugangs durch Familienmitglieder oder Freunde berücksichtigt, ist im aktuellen Home-Office-Alltag aus Unternehmenssicht unverzichtbar. Nichts Anderes erwartet auch SWIFT.

Darüber hinaus wird im Rahmen des CSP sehr genau vorgegeben, welche Qualitätsansprüche an Themen wie Update-Management, Virus-Scanning und Sicherheitsschulungen gestellt werden. Beispielsweise sollten die mit SWIFT-Themen betrauten Mitarbeiter regelmäßig (zumindest einmal jährlich) über bestehende Cyber-Risiken geschult werden. Für die, die die Zahlungsanwendungen betreiben gelten dabei andere Maßstäbe als für jene, die für die Wartung der Infrastruktur zuständig sind.

Für die IT zeigt das CSCF detailliert auf, wie kritische Systeme durch klare Trennung von der restlichen IT-Umgebung und Beschränkung des Internet-Zugangs geschützt, Angriffsflächen reduziert und Schwachstellen ausgemerzt werden können. Zusätzlich müssen SWIFT-Teilnehmer über einen dokumentierten Plan verfügen, wie auf Cyber-Vorfälle zu reagieren ist.

All das ist im ersten Schritt sehr viel Arbeit – aber sollten diese Punkte angesichts der immer ausgeklügelten Einfallsstrategien von Cyber-Kriminellen nicht ohnehin auf der To-Do-Liste stehen? ▲

# Champions League statt Kreisklasse

Erfahrungen mit der Einrichtung und der laufenden Arbeit mit SWIFT. Ein Interview mit Nils Ostendorf, Director Global Treasury bei IFCO.

IFCO ist ein weltweit führender Anbieter von Mehrwegverpackungslösungen für Frischprodukte und betreut Kunden in über 50 Ländern. Das Unternehmen verfügt weltweit über einen Pool von mehr als 314 Millionen Mehrwegbehältern (Reusable Plastic Containers – RPCs), die jährlich für über 1,7 Milliarden Auslieferungen von frischem Obst und Gemüse, Fleisch, Geflügel, Fischereierzeugnissen, Eiern, Brot und anderen Produkten von den Produzenten zum Einzelhandel eingesetzt werden. IFCO hat seinen Sitz in Pullach bei München. Seit 2019 gehört das Unternehmen zu gleichen Teilen der Beteiligungsfirma Triton und ADIA, einem Staatsfonds des Emirats Abu Dhabi.

**TreasuryLog:** Seit dem Demerger von Brambles im Mai 2019 nutzt IFCO das SWIFT-Netzwerk über einen eigenen Alliance Lite2 Zugang. Wie ist es im Treasury zur Entscheidung für AL2 gekommen?

**Nils Ostendorf:** Mit SWIFT hatten wir bereits im Konzernverbund von Brambles gute Erfahrungen gemacht. Nachdem im Zuge des Unternehmensverkaufs alles sehr rasch gehen und IFCO schnell auf eigenen Beinen stehen musste, haben wir uns entschieden, auf diesen bewährten Kanal zu setzen. Aufgrund des zeitlichen Drucks haben wir uns auch auf eine einheitliche Kommunikationslösung fokussiert und bewusst keinen Parallelbetrieb mit EBICS aufgesetzt.

Aktuell nutzen wir SWIFT für den Zahlungsverkehr – inkl. Kontoauszüge und Statusnachrichten – mit acht Bankengruppen in Europa und Kanada und damit für über 50 Konten. Wir wollen SWIFT zukünftig in der ganzen Gruppe nutzen und werden dabei durch die globale Abdeckung von SWIFT optimal unterstützt.

Im Unterschied zu früher, als wir eine umfangreichere Lösung nutzten, haben wir unserem Bedarf entsprechend auf die Kombination von SAP BCM und SWIFT Alliance Lite2 (AL2) gesetzt. Weitere für uns wesentliche Entscheidungsfaktoren waren das hohe Sicherheitsniveau von SWIFT und der reiche Erfahrungsschatz der ehemaligen Kollegen, die uns gerade in der Anfangsphase mit Rat und Tat zur Seite standen. Wer einmal Champions League gespielt hat, mag nicht mehr in die Kreisklasse zurück, des-



© IFCO

Nils Ostendorf zeichnet bei IFCO verantwortlich für das globale Treasury.

halb waren viele vereinzelte und dadurch arbeitsaufwändige, bankspezifische Electronic Banking-Lösungen keine Alternative für uns.

**TreasuryLog:** Wie waren Ihre Erfahrungen in der IT bei der technischen Einrichtung von SWIFT und der Anbindung an Ihr SAP?

**Ostendorf:** IFCO selbst hat kein eigenes Rechenzentrum und hostet bei externen Partnern. Im Fall von SWIFT stellte dies eine Herausforderung dar, nachdem die für die Anbindung notwendigen VPN-Boxen physisch im Rechenzentrum platziert werden mussten. Unser Hosting-Partner war am Anfang sehr skeptisch, da musste einiges an Aufklärungsarbeit geleistet werden. Auch die Einrichtung selbst war anspruchsvoll: Firewalls, Routing und schließlich die Verbindung des SWIFT AutoClients mit SAP waren große Themen. Mit punktueller Unterstützung von SWIFT und etwas „Trial and Error“ ist es uns aber gelungen, zeitnah die Kommunikation mit SWIFT in der benötigten Qualität einzurichten.

Sobald die Architektur dann stand, war alles Weitere, wie etwa die Anbindung der Banken, aus technischer Sicht kein relevanter Aufwand mehr.



Mehrweg statt Einweg. Reusable Plastic Container ist das Business von IFCO.

© IFCO

**TreasuryLog:** *Wie hoch ist der laufende Aufwand für Sie in der IT mit Themen wie Monitoring, Token- und Zertifikate-Management oder auch Updates?*

**Ostendorf:** Left und Right Security Officer sind bei uns in der IT angesiedelt, die für Zertifikate- und Token-Management anfallenden Aufgaben sind aber überschaubar. Das ist auch kein exklusives SWIFT-Thema und fällt bei anderen Softwarelösungen genauso an, da aber für jede Electronic Banking Lösung einzeln.

Insgesamt würden wir unseren IT-Aufwand für SWIFT auf zehn Tage pro Jahr beziffern. Wir profitieren jetzt davon, dass wir nah am Standard geblieben sind, uns am Anfang sehr intensiv mit der Materie auseinandergesetzt haben und ausgiebig Gebrauch von den in SWIFT.net verfügbaren, gut gemachten Trainingsunterlagen und Empfehlungen, wie z. B. zum Berechtigungsmanagement, gemacht haben. Das hat uns dabei geholfen, die notwendigen Schnittstellen optimiert aufzusetzen.

Wir nutzen auch viele Abonnements und die Newsletter aus dem SWIFT-Portal, um rechtzeitig von Upgrades und Neuerungen zu erfahren. Aktives Monitoring betreiben wir nicht. Für die relevanten Schnittstellen haben wir E-Mail-Meldungen bei Störungen eingerichtet. Bislang waren hier aber so gut wie keine Eingriffe nötig. Alles läuft stabil.

Auch unsere bisherige Erfahrung mit Upgrades war sehr gut. Verglichen mit anderen Schnittstellen fällt bei SWIFT der geringste Aufwand an. Im letzten Jahr stand beispielsweise ein Update des AutoClients an, bei dem nach dem Einspielen auf unserer Seite keinerlei Nacharbeiten mehr notwendig waren.

Was die IT-Kosten betrifft, finden wir SWIFT als Produkt, mit dem man global einheitlich agieren kann, sehr vorteilhaft. Gerade bei einer Gruppe mit Büros in mehr als 30 Ländern ist es viel wert, wenn nationale Unterschiede nur in Ausnahmefällen zu berücksichtigen sind. Wie viel Zeit und Geld wir im Zahlungsverkehr mit der Verwendung eines globalen Produktes sparen, das sehen wir aktuell bei der Einführung der elektronischen Rechnungsabwicklung. Hierzu gibt es in jedem Land andere Lösungen und separate Schnittstellen, die laufenden, kostenintensiven Betreuungsaufwand verursachen.

**TreasuryLog:** *Wie ging und geht es Ihnen mit dem umfassenden Anforderungskatalog des SWIFT Customer Security Programme (CSP)? Haben Sie schon festgelegt, wie Sie der für 2021 von SWIFT geforderten unabhängigen Attestierung nachkommen werden?*

**Ostendorf:** Zu Anfang ist das CSP gefühlt ein Gebirge, welches sich vor einem auftut, vor allem, weil man inhaltlich sehr viel durcharbeiten muss. Auf den zweiten Blick ist es aber eine sehr gute Sache. Die von SWIFT bereitgestellten Unterlagen sind detailliert und verständlich ausgearbeitet und stellen klar dar, wie Sicherheit und Segregation of Duty funktionieren. Das CSP selbst ist rasch beantwortet, die Hauptarbeit kommt danach, wenn man die erkannten Lücken schließen und die Prozesse anpassen muss. Der Aufwand fällt vor allem im ersten Jahr an, danach ist es wesentlich einfacher und unser Fazit nach dem ersten Schrecken ist eindeutig positiv.

IFCO plant die Etablierung einer neuen, unabhängigen, aber internen, Stelle für IT-Sicherheit. Das Stellenprofil umfasst auch künftig die unabhängige Bewertung für das SWIFT CSP vorzunehmen. Wir möchten das Know-how bewusst nicht extern vergeben, sondern bei uns im Haus belassen.

**TreasuryLog:** *Welches Resümee ziehen Sie im Treasury nach zweijähriger SWIFT-Mitgliedschaft? Welche Aspekte der AL2-Anbindung finden Sie besonders vorteilhaft für Ihre spezifischen Gegebenheiten und wie zufrieden sind Sie insgesamt?*

**Ostendorf:** Ein aus unserer Sicht besonders positiver Aspekt von SWIFT ist die Unabhängigkeit von Systemanbietern und Banken. Im Falle des Falles wären wir innerhalb von nur wenigen Wochen in der Lage, Bankverbindungen zu wechseln und neu aufzusetzen. Das ist durchaus ein Vorteil in Bankgesprächen.

In puncto Sicherheit fühlen wir uns mit SWIFT extrem gut aufgestellt, gerade im Hinblick auf die immer häufiger vorkommenden Angriffsversuche, denen auch wir uns fallweise ausgesetzt sehen. Das SWIFT CSP empfinden wir gerade vor diesem Hintergrund als ein wertvolles Werkzeug, das uns fundiert darin unterstützt hat, unsere Schwachstellen zu erkennen und zu beheben.

Verbesserungsbedarf sehen wir ganz klar bei der grafischen Oberfläche, der GUI von AL2, das wir zur manuellen Erfassung von Zahlungen nutzen. Praktisch ergibt sich für uns daraus aber kein Nachteil, weil wir SWIFT AL2 als reinen Kommunikations-

weg verwenden und das GUI im Tagesgeschäft selten nutzen (müssen).

Auch mit den Banken hat die Anbindung sehr gut und effizient funktioniert. Das Vertragswerk ist stark standardisiert, mit den Inhalten können wir gut leben und die technischen Aspekte sind mit wenigen Ausnahmen schnell geklärt. Allerdings sind die Preisunterschiede zwischen den Banken eklatant, da gibt es schon die eine oder andere negative Überraschung gerade bei etablierten Instituten, bei denen man das so nicht erwarten würde, da sie bestimmt mehr als einen Kunden haben, der SWIFT nutzt.

Unser Fazit: SWIFT ist keine kleine Investition, aber im professionell aufgesetzten Zahlungsverkehr kommt man kaum um SWIFT herum, wenn man unabhängig bleiben will. Am Anfang war die Umstellung mit einigem Aufwand verbunden, seit sich aber alles eingespielt hat, wollen wir es nicht mehr missen. ▲



## Betriebliche Altersvorsorge nach Maß

Zeit, Geld neu zu bewerten.

Mit den Vorsorgemodellen von Fidelity sind Sie und Ihre Mitarbeiter rundum gut für die Zukunft aufgestellt. Neben einem modern gestalteten Pensionsplan hilft das Zeitwertkonto die Zeit vor Renteneintritt ideal zu gestalten. Intelligente Kapitalanlagestrategien, eine einfache digitale Kontenverwaltung, stabile Treuhandlösungen sowie eine effiziente Mitarbeiterkommunikation sind elementare Bausteine. Nutzen Sie die Vorteile dieser zeitgemäßen Gesamtlösung – unser Maßstab sind Sie.

Mehr über die Vorsorgelösungen von Fidelity International erfahren Sie unter [www.fidelity.de/bav](http://www.fidelity.de/bav)





Oleksandr

## „Wir haben den Bedarf erkannt“

Mit Ralf Klein, Senior Account Director Corporates bei SWIFT, haben wir über Zukunftspläne, Usability und die Bedeutung von Sicherheit gesprochen. Kommunikation in einer geschützten Umgebung, fälschungssicher und frei von Übertragungsfehlern, ist seiner Ansicht nach die wesentliche Leistung der global agierenden Zahlungsverkehrsorganisation. Die vermehrte Verwendung von Cloud-Diensten und gestiegene Anforderungen an die Anwenderfreundlichkeit sind die zentralen Herausforderungen.



**TreasuryLog:** *Wie viele Corporates im DACH-Raum nutzen das SWIFT-Netzwerk direkt über einen eigenen BIC?*

**Ralf Klein:** Derzeit gibt es weltweit ca. 2.400 Corporate BICs, mehr als 15 Prozent davon in der DACH Region. Unser jährliches Wachstum liegt bei rund 10 Prozent. Qualität ist hierbei wichtiger als Quantität. Bei den Neukunden nutzen rund die Hälfte SWIFT über einen L2BA-Provider, ein knappes Drittel hat sich für ein SSB entschieden und 20 Prozent für ein eigenes AL2.

Historisch hatten sich einige wenige Kunden für die Implementierung einer eigenen SWIFT Infrastruktur entschieden. Diese prüfen derzeit alle einen Umstieg auf eine Cloud basierte Lösung, sodass die On-Premises Solution künftig keine Rolle mehr spielen dürfte.

**TreasuryLog:** *Das Customer Security Programme (CSP) ist ein Thema, das bei potenziellen SWIFT-Kunden – so unser Eindruck bislang – zuallererst Verunsicherung auslöst. Spricht man dann mit Kennern, wie IFCO, zeigt sich ein gänzlich anderes Bild. Was möchten Sie all jenen mitgeben, die über SWIFT nachdenken, sich von den CSP-Anforderungen aber erst einmal überrannt fühlen?*

**Klein:** Das Customer Security Programme ist aus unserer Sicht eigentlich ein Angebot an Corporates. Sie bekommen damit ein sehr dezidiertes Sicherheitsprotokoll an die Hand, das genau darstellt, wie eine solche Architektur betrieben werden muss, um sicher aufgestellt zu sein. Das ist per se einmal überhaupt nichts Schlechtes! Es ist ein zusätzliches Feature, das mit einer SWIFT-Anbindung kommt. Der Kunde kauft Sicherheit ein, zu dem Preis, dass er dafür auch bestimmte Dinge selbst tun muss.

Dass die Passwortlänge- und -komplexität für diesen Zweck keine ausreichenden Features sind, haben wir aus bitterer Erfahrung lernen müssen. Das Einfallsstor liegt im Umfeld der SWIFT-Infrastruktur, und genau da setzt das CSP an.

Klar, für den Treasurer ist das in dem Detail oft unbekanntes Terrain, aber IT- und Compliance-Experten, die regelmäßig mit diesen Themen zu tun haben, beurteilen die festgelegten Kontrollen als Standard-Cyberhygiene. Wir haben einige Kunden im DACH-Raum, die unser CSP auch auf ihre anderen Kommunikationskanäle ausgeweitet haben.

Aus unserer Sicht ist das CSP für Unternehmenskunden eine Empfehlung. SWIFT selbst steht bei Nichterfüllung nicht mit erhobenem Zeigefinger da, dazu ist uns eine wahrheitsgemäße Beantwortung viel wichtiger. Die Kontrolle der Einhaltung erfolgt vielmehr durch die Community: Counterparties (z. B.

Banken) können die Attestierung einsehen, um sich davon zu überzeugen, dass die Handelspartner gut aufgestellt sind. Im Gegensatz zu Geschäften zwischen Finanzkontrahenten, wo die CSP-Compliance von der Finanzaufsicht verlangt wird, gibt es für Unternehmenskunden keinen behördlichen Regulator.

Wir verstehen auch, dass das für das CSP 2021 geforderte „Independent Assessment“ Aufwand auslöst. Aus unserer Sicht war dies jedoch notwendig, um das Niveau des CSP qualitativ zu verbessern: Ein Assessor muss sich die gemachten Angaben ansehen und diese überprüfen. Das kann durchaus von einer neutralen Stelle im eigenen Haus übernommen werden, aber der Vorteil einer externen Überprüfung ist natürlich der frische Blick.

**TreasuryLog:** *Im Gegensatz zu L2BA-Lösungen gab es für AL2-Kunden, aufgrund der dafür notwendigen VPN-Boxen, bislang nicht die Möglichkeit, für ihre SWIFT-Installation die Public Cloud zu nutzen. Was hat SWIFT diesbezüglich vor, um am Puls der Zeit zu bleiben?*

**Klein:** Den Bedarf haben wir klar erkannt – viele unserer Kunden hosten nicht bei sich selbst, sondern nutzen gemietete Speicherkapazität und der Trend geht klar in Richtung Public Cloud. Unser Ziel ist es, dass wir für Anbieter, wie zum Beispiel Azure, AWS oder Google, eigene Frameworks, ähnlich denen für L2BA-Anbieter, schaffen. Hier gibt es schon erste Piloten, derzeit mit Banken, die mit Soft-Zertifikaten anstelle von VPN-Boxen auskommen. Herausfordernd sind die bislang definierten Standard-Anforderungen von SWIFT – wie verschlüsselte Kommunikation – die mit einer Public Cloud schwer umgesetzt werden kann. SWIFT muss seine Regelungen hier den aktuellen Gegebenheiten anpassen. Dabei steht für uns natürlich im Vordergrund, dass wir das gewohnte Sicherheitsniveau auch mit Public Cloud-Anbietern sicherstellen können.

Unsere Roadmap sieht vor, dass Unternehmenskunden spätestens in zwei Jahren voll umfänglich Public Cloud Services für Ihre SWIFT Kommunikation nutzen können.

**TreasuryLog:** *Ein Kritikpunkt, der von AL2-Kunden regelmäßig angebracht wird – so auch in unserem Gespräch mit IFCO – ist die Anwenderfreundlichkeit des GUI-User-Interface, das noch nicht ganz im 21. Jahrhundert angekommen ist. Sind hierzu Neuerungen geplant?*

**Klein:** Bei diesem Thema sind wir schon weit über die Planungsphase hinaus, mit der „Alliance Cloud“ (AC) ist der Nachfolger von AL2 bereits in der Pilotphase. Unser Anspruch dabei ist einfach erklärt: Das besser machen, was in der Vergangenheit nicht so gut gelaufen ist. Die wesentliche Neuerung ist also

nicht die Cloud-Komponente – auch AL2 ist ja eine Cloud-Lösung – sondern die deutliche Verbesserung in den Bereichen Datenaustausch und Handling.

Eines der prioritären Ziele war die Erhöhung der Nutzerfreundlichkeit unserer User-Interfaces. Damit möchten wir auch der Tatsache Rechnung tragen, dass die Fachabteilungen in ihrer täglichen Arbeit die Anwendung selbst kaum nutzen, sondern die Flows automatisiert abgewickelt werden. Im Ausnahmefall ist es daher umso wichtiger, dass alles intuitiv bedienbar ist und man sich auch ohne tiefere IT-Kenntnisse rasch orientieren kann. In der neuen Benutzeroberfläche von AC können Anwender sehr einfach Einzelzahlungen erfassen und auch Templates für den Zahlungsverkehr hinterlegen. Darüber hinaus gibt es komfortable User-Interfaces für Administration und Backup.

Die neue Alliance Cloud-Lösung erleichtert zukünftig auch eine Migration des SWIFT BIC. In der Vergangenheit war es technisch keineswegs trivial, wenn Kunden zwischen unterschiedlichen Anbietern wechseln wollten. Das Setup wird mit AC nun seitens SWIFT technisch so aufgesetzt, dass dies sehr einfach und flexibel möglich sein wird. Darüber hinaus stellen wir gerade konkrete Überlegungen zu einem erweiterten Service-Angebot an. Wir denken daran, zukünftig auch optionale Zusatzfeatures wie Screening, Bankdatenvalidierung oder Monitoring integriert anzubieten.

**TreasuryLog:** *Ab wann wird AC für Ihre Corporate-Kunden zur Verfügung stehen und was bedeuten diese Neuerungen für Ihre bestehenden AL2- und L2BA-Kunden?*

**Klein:** Für Neukunden im Corporate-Segment wird AC spätestens im vierten Quartal verfügbar sein. Praktisch bedeutet das, dass alle Neukunden, die ab diesem Zeitpunkt eine direkt von SWIFT angebotene Cloud-Lösung nutzen möchten, mittels AC und nicht mehr über AL2 angebunden werden.

Für unsere AL2-Bestandskunden ist keine verpflichtende Migration vorgesehen und AL2 kann weiterhin verwendet werden. Auf Wunsch ist ein Wechsel natürlich möglich.

Mit den L2BA-Providern sind wir bereits in Gesprächen, auf deren Seite besteht großes Interesse an einer Migration, da Ihnen die technische Plattform mehr Flexibilität bietet.

Für AC gibt es ein ähnliches Preismodell wie für AL2 bzw. L2BA: Die bekannten Bänder bleiben erhalten, zukünftig werden jedoch auch eingehende Nachrichten bepreist und dafür die bisher geltenden Bandbreiten stark erhöht. Damit stellen wir sicher, dass sich die monatlichen Kosten für den Einzelnen nicht wesentlich ändern. ▲

## Die „Großen“ geben den Takt vor

Die umsatzstärksten Unternehmen der DACH-Region unterzogen sich beim SLG-Treasury-Summit einem direkten Benchmarking. 2020 waren es 17 Teilnehmer, die ihre Entwicklungen im Treasury diskutierten und Innovationen vorstellten.

### Die Autoren:



**Georg Ehrhart**  
ist Geschäftsführer  
und Partner bei  
Schwabe, Ley &  
Greiner.



**Thomas Diernbauer**  
ist Senior-Berater bei  
Schwabe, Ley &  
Greiner

Bei einem Gesamtumsatz von fast einer Billion Euro und insgesamt über 800 Personen mit Treasury-Agenden überrascht es kaum, dass diese 17 bereits den Großteil ihrer Hausaufgaben erfüllt und beim Best-Practice-Vergleich sehr gut abgeschnitten haben. Getreu dem Motto „Stillstand ist Rückschritt“ ist es aber der Anspruch dieser Unternehmen, auch in den kommenden Jahren im Treasury zu den Besten zu gehören und sich regelmäßig zu messen. Im Fokus der letzten Summit-Runde stand der weitgefaste Begriff der „Digitalisierung“, der alle Treasury-Bereiche in unterschiedlicher Weise berührt.

### Auch der SLG-Treasury-Summit wurde „digitaler“

Den Umständen geschuldet und erstmalig fanden die Erhebungsinterviews und die Ergebnisworkshops online statt. Die SLG-Lounge wurde zu diesem Zweck in ein kleines Fernsehstudio mit professioneller Technik umgebaut. Vom positiven Feedback der Teilnehmer waren wir sehr angetan. Es hat sich gezeigt, dass auch in diesem Rahmen fachlicher Diskurs in der gewohnten Qualität möglich ist.

Vermisst wurden natürlich der Kaffeeplausch zwischendurch und der persönliche Austausch bei den gemeinsamen Abendveranstaltungen. Daher wird ein persönliches Treffen in dieser Runde, so bald wieder möglich, nachgeholt. Die Eindrücke aus der digitalen Durchführung decken sich mit den Erfahrungen der

Teilnehmer im vergangenen Jahr: Online-Meetings sind bereits sehr gut eingespielt und werden auch nach der Rückkehr zur Normalität weiterhin den Alltag prägen. Persönliche Treffen von Zeit zu Zeit bzw. bei besonderen Themen ersetzen diese aber nicht.

### Nutzen steht im Vordergrund

Digitalisierungsmaßnahmen stehen bei allen Teilnehmern auf der Agenda. Bei manchen ganz oben, bei anderen mit nicht ganz so hoher Priorität. Der unterschiedliche Zugang zeigt sich auch in der Erwartungshaltung zu einzelnen Einsatzgebieten (siehe Grafik). Doch bei einem sind sich alle einig: Nicht Digitalisierung der Digitalisierung wegen – der tatsächliche Nutzen (auch im Verhältnis zum Aufwand) steht im Vordergrund.

Einige interessante Lösungen stellten Teilnehmer im Bereich Robotic Process Automation vor. Dabei werden durch kleine „Bots“ aufwändige manuelle Tätigkeiten automatisiert. Ein Teilnehmer beispielsweise liest automatisiert Informationen aus E-Mails von Banken aus und speichert diese ebenso automatisiert in einem System ab. Ein anderer Teilnehmer verschickt mittels solcher Anwendungen regelmäßig vereinbarte Informationen an Banken.

Beim Thema automatisierte Ableitung von Sicherungsstrategien wurden zwei Ansätze diskutiert. Einerseits einer, bei dem auf Basis von Volatilitäten und Korrelationen und ausgehend von einem Zielrisiko eine optimale Sicherung angestrebt wird – beispielsweise die Minimierung der Sicherungskosten. Zum anderen ein Ansatz, der noch etwas weiter geht und mittels künstlicher Intelligenz versucht, den idealen Sicherungszeitpunkt vorherzusagen.

Künstliche Intelligenz wird bei einem Teilnehmer auch eingesetzt, um auf Basis historischer und makroökonomischer Daten zukünftige Cashflows vorherzusagen und so die Liquiditätsplanung fast gänzlich automatisiert zu erstellen. Auch bei der Kreditrisikoprüfung oder bei der „Fraud Detection“ kommt bereits künstliche Intelligenz zum Einsatz. Bei der automatisierten Betrugserkennung wird dabei nach auffälligen Mustern gesucht, mit deren Hilfe kriminelle Manipulationen im Zahlungsverkehr erkannt werden können.

Eine angemessene Datenbasis mit entsprechender Historie ist eine Voraussetzung für viele der genann-

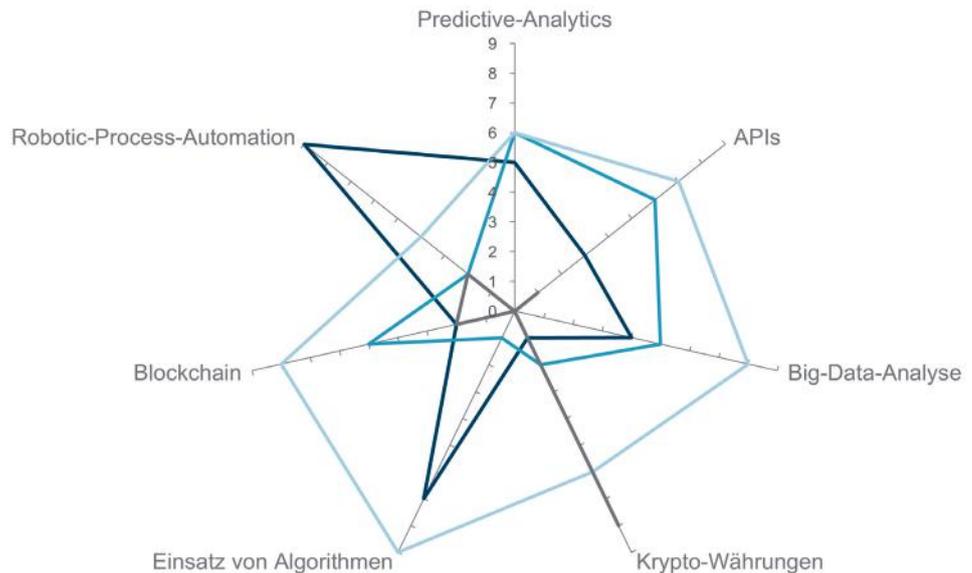


Abb. 1: SLG-Lounge zum Studio umfunktioniert

Der Autor bei der Präsentation in der zum Studio umfunktionierten SLG-Lounge.

**Abb. 2: Einschätzung von Anwendungsmöglichkeiten im Treasury**

Den Summit-Teilnehmern wurde die Frage gestellt, welche Anwendungsmöglichkeiten verschiedene Technologien im Treasury bieten: Lesehilfe: Robotic Process Automation ist bei neun Teilnehmern im Einsatz. Vier Teilnehmer sehen möglicherweise in der Zukunft Anwendungsmöglichkeiten. Jeweils zwei Teilnehmer untersuchen mögliche Anwendungen oder sehen keinen Anwendungsbereich.



ten Einsatzmöglichkeiten. Daher kann es sich lohnen, auch Daten zu sammeln, die zwar noch nicht heute, vielleicht aber in naher Zukunft verwendet werden können. Klingt zwar einfach, doch Erfahrungsberichte der Teilnehmer zeigen, dass die Plausibilisierung und Bereinigung der Daten teilweise mit hohem Aufwand verbunden sind.

**Krise befeuert den Wandel**

Während mit Digitalisierungsmaßnahmen versucht wird, bestehende Prozesse effizienter, sicherer und transparenter zu gestalten, führt nicht zuletzt die Krise auch zu neuen Treasury-Anforderungen. Hier tun sich insbesondere Omni-Channel-Payments hervor. Die Frage an die Summit-Teilnehmer, ob die damit einhergehenden Herausforderungen von Treasury behandelt werden sollen, hat ein Teilnehmer kurz und bündig so beantwortet: „Das ist der neue Zahlungsverkehr, und Zahlungsverkehr gehört ins Treasury“.

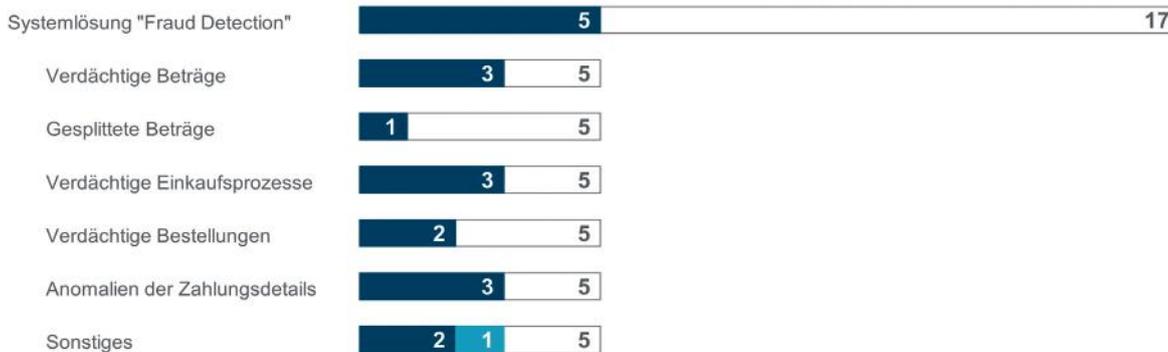
**Treasury-Summit: Tradition seit 1997**

Seit 1997 führt Schwabe, Ley & Greiner regelmäßig das Benchmarking-Projekt „SLG-Treasury-Summit“

durch, an dem bereits über 200 Unternehmen teilnahmen. Das Format stellt nicht etwa einen lockeren Gedankenaustausch dar, sondern ein Projekt, bei dem die Teilnehmer ihre Treasury-Funktionen einem professionell durchgeführten Vergleich unterziehen.

Die Datenerhebung basiert auf einem umfassenden Fragebogen und Interviews mit Akteuren der Treasury-Abteilung. Diese inkludiert alle relevanten Themenblöcke in Treasury. Die Antworten werden quantitativ ausgewertet und die Ergebnisse bei einem gemeinsamen zweitägigen Workshop präsentiert. Letzter Schritt sind bilaterale Termine, bei denen die Detailergebnisse des jeweiligen Unternehmens durchleuchtet und Handlungsempfehlungen abgegeben werden.

Unternehmensvertreter, die diese Form des Benchmarkings für sich nutzen möchten, können bereits jetzt die Gelegenheit nutzen, sich für 2022 anzumelden. Bei Interesse bitten wir um eine E-Mail an [info@slg.co.at](mailto:info@slg.co.at).



**Abb. 3: Systemunterstützung bei Fraud Detection noch wenig etabliert**

Fünf von 17 Teilnehmern verwenden eine Systemlösung zum Erkennen von Betrugsversuchen im Zahlungsverkehr. Diese und auch die anderen Unternehmen zeigten großes Interesse an der Erweiterung bzw. der Einführung einer solchen Lösung.



© Sébastien Bertrand

Durch ihre Regularien wird die EU zum Standardsetzer im Bereich nachhaltiger Finanzierungen.

## Sustainable Finance: Nicht „grün“ = „braun“?

Die „grüne“ Taxonomie der Europäischen Union und die begleitenden Verordnungen nehmen weiter Form an. Im Artikel „Grüne Finanzierungen: Gekommen, um zu bleiben“ (TLog Ausgabe 5/2019) haben wir zuletzt über die ersten Veröffentlichungen rund um die EU-Taxonomie berichtet. Rund ein Jahr später hat sich einiges getan, vor allem eine Debatte rund um eine Erweiterung um eine „braune“ Klassifizierung von Wirtschaftstätigkeiten beschäftigt den Finanzsektor.

### Der Autor:



**Johannes Asamer**  
ist Manager bei  
Schwabe, Ley &  
Greiner

„Europa ist im Kampf gegen den Klimawandel führend“, postete EU-Ratspräsident Charles Michel am 11. Dezember 2020 auf Twitter, nachdem man sich beim EU-Gipfel auf ein deutlich verschärftes Klimaziel bis 2030 einigen konnte. Mindestens 55 Prozent, statt der ursprünglich vereinbarten 40 Prozent, soll der Ausstoß von Treibhausgasen unter den Wert von 1990 sinken. Diese ambitionierte Marke erhöht nun auch den Druck auf den Finanzsektor, entsprechende Impulse zu setzen, und auf Unternehmen, vermehrt Maßnahmen in dieser Transformationsphase bis hin zur Klimaneutralität umzusetzen.

Viele Unternehmen sind sich ihrer Verantwortung durchaus bewusst und folgen auf freiwilliger Basis Richtlinien oder Nachhaltigkeitsprinzipien. Nur eines der vielen Positivbeispiele in Deutschland ist etwa das Rahmenwerk für klimaneutrale Gebäude der Deutschen Gesellschaft für Nachhaltiges Bauen (DGNB).

Die EU arbeitet schon länger an den Fundamenten einer einheitlichen Klimapolitik, denn nicht einmal die Fragen, was ist nun „grün“ bzw. ökologisch nach-

haltig und anhand welcher Kriterien kann man einen positiven Beitrag zur Zielerreichung messen, ließen sich bislang eindeutig beantworten. Ein Dschungel aus unterschiedlichsten Definitionen, Auslegungen und Klassifizierungen machte so manche Transaktion möglich, die nur dem Anschein nach „grün“ war. Einem Bericht des Guardians aus dem Jahr 2019 zufolge, erhielt beispielsweise die Industrie für fossile Brennstoffe jährlich Subventionen in Höhe von mehr als 370 Milliarden US-Dollar, wovon lediglich 10 bis 30 Prozent für den Übergang zu sauberer Energie verwendet wurden.

Mit der Veröffentlichung der Taxonomie im Jahr 2018 und dem Ziel, auf EU-Ebene einheitliche Kriterien zur Klassifizierung und Messung ökologisch nachhaltiger Wirtschaftstätigkeiten einzuführen (siehe Infobox 2), sollten diese Fragen beantwortet und gleichzeitig auch Anreize für Investitionen in bzw. Finanzierung von ebensolchen Wirtschaftstätigkeiten geschaffen werden.

**Klassifizierung für nachhaltiges Wirtschaften**  
Ursprüngliches Ziel der Kommission war es jeden-

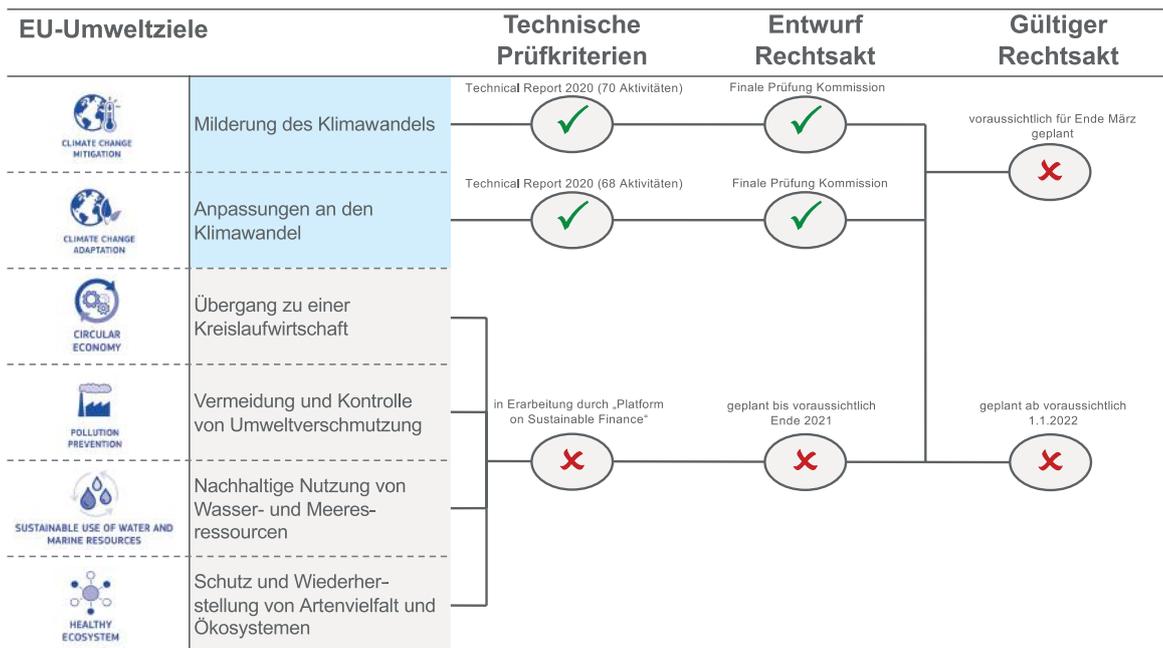


Abb. 1: EU-Umweltziele

falls, dass kein Wirtschaftszweig per se diskriminiert und auch Anpassungsleistungen brauner Sektoren honoriert werden sollten. Mit der Veröffentlichung des finalen Berichts („Technical Report“) der Technischen Expertengruppe für nachhaltige Finanzierungen (TEG) im März 2020 und der anschließenden Verordnung des Europäischen Parlaments und des Rates über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen, die am 12. Juli 2020 in Kraft getreten ist, existiert nun erstmals ein Klassifizierungssystem für nachhaltige Wirtschaftstätigkeiten. Dies soll eine gemeinsame Sprache für Investoren und Unternehmen schaffen.

Als Teil dieser Taxonomie-Verordnung wurde die Kommission damit beauftragt, technische Prüfkriterien („technical screening criteria“) zur Weiterentwicklung der Taxonomie vorzulegen. Die ersten beiden Sätze von Kriterien wurden im November 2020 in einem Entwurf veröffentlicht. In einem Zeitfenster von vier Wochen konnten Marktteilnehmer dazu Rückmeldung geben. Das Dokument betrifft vorerst jene Aktivitäten, die wesentlich zur Milderung des Klimawandels („climate change mitigation“) oder zur Anpassung an den Klimawandel („climate change adaptation“) beitragen und legt technische Prüfkriterien fest, um zu bestimmen, wann wirtschaftliche Aktivitäten einen wesentlichen Beitrag zur Erreichung eines dieser beiden Umweltziele leisten und gleichzeitig nicht gegen eines der fünf anderen Ziele (siehe Abbildung 1) wirken („do no significant harm“ bzw. DNSH).

Aktuell beinhaltet die Taxonomie Prüfkriterien für 70 Aktivitäten zur Milderung des Klimawandels und 68 zur Anpassung an den Klimawandel sowie jeweils Kriterien gemäß dem DNSH-Prinzip. Die Aktivitäten umfassen dabei u.a. die Bereiche Forst- und Landwirtschaft, verarbeitendes Gewerbe, Elektrizitäts- und Gasversorgung, Wasser, Kanalisation und Abfall, Transport und Lagerung, Information und Kommunikation, Baugewerbe, Grundstücks- und Wohnungswesen, Erbringung von Finanz- und Versicherungsdienstleistungen sowie Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen.

Die Kommission prüft aktuell die unzähligen erhaltenen Antworten (rund 47.000), bevor die Verabschiedung (in Form eines delegierten Rechtsakts) abgeschlossen wird. Dieser soll ab dem 1. Januar 2022 gelten. Bis dahin werden dann auch die weiteren Umweltziele durch Kriterien beschrieben bzw. soll ein Rechtsakt für diese vorliegen.

#### Debatte über Empfehlungen der TEG

Mit 1. Oktober 2020 wurde die „Platform on Sustainable Finance“ (PSF) ins Leben gerufen. Die 57 Mitglieder und 10 Beobachter („observers“) zählen dabei zu den weltweit führenden Nachhaltigkeitsexperten unter anderem aus dem Finanz- und Unternehmenssektor, NGOs, Wissenschaft, Think Tanks und der öffentlichen Hand. Die PSF löst damit die TEG (temporäres Mandat bis September 2020) ab und wurde von der Europäischen Kommission als dauerhaftes Organ eingesetzt, um die Entwicklung von Prüfkriterien für die vier verbleibenden Umweltziele voranzutreiben.

NAME	ERWÄRMUNGSPOTENTIAL	KAPITALGEWICHT
 SAP SE	1,3°	10,5 %
 Deutsche Post AG	1,3°	3,8 %
 E.ON SE	1,6°	2,2 %
 Allianz SE	1,8°	7,5 %
 Munich Reinsurance Company	1,9°	3,3 %
 BASF SE	8,6°	4,6 %
 Volkswagen AG Pref	8,4°	2,5 %
 Daimler AG	8,2°	3,6 %
 Linde plc	7,8°	10,6 %
 Continental AG	7,4°	1,0 %

Abb. 2: Top/Bottom 5 DAX-Unternehmen mit dem niedrigsten bzw. höchsten Erwärmungspotenzial laut Globalance-Segmentierung

Weiters wurde von der Kommission unter anderem die rechtliche Grundlage geschaffen, die Taxonomie um soziale Ziele und braune Aktivitäten erweitern zu können. Die noch von der TEG ausgesprochene Empfehlung, nach einer Erweiterung um eine Definition von braunen Wirtschaftsaktivitäten, birgt jedenfalls viel Diskussionsstoff.

Die Befürworter argumentieren, dass eine grüne Taxonomie allein nicht ausreichend sein wird, um die Finanzmärkte „2030-konform“ zu machen, weil Investoren und Unternehmen zwar dazu ermutigt werden, mehr in nachhaltige Wirtschaftstätigkeiten zu investieren und diese voranzutreiben, nicht jedoch, braune Wirtschaftstätigkeiten zu meiden oder gänzlich auszugrenzen. Zentralbanken, Aufsichtsbehörden und zahlreiche NGOs sind überzeugt, dass eine braune Taxonomie den Weg für strengere Kapitalanforderungen für umweltschädliche Aktivitäten ebnet und so einen deutlich größeren Beitrag zur Erreichung der Klimaziele leisten würde.

Die Gegner dieses Vorschlages, darunter vor allem Finanzinstitute und Industrieunternehmen, sehen dieses Thema bereits ausreichend in der Taxonomie durch das DNSH-Prinzip abgedeckt und befürchten weiters, dass braune Unternehmen völlig von der Vergabe von Finanzmitteln ausgeschlossen würden, die jedoch dringend für die Transformationsphase benötigt werden.

In der Empfehlung der TEG umfasst die Taxonomie drei Leistungsstufen:

- ▲ substanzialer Beitrag = grün
- ▲ signifikanter Schaden = braun
- ▲ Aktivitäten, die weder das eine noch das andere darstellen

#### Segmentierung am Markt findet bereits statt

Auch wenn es noch keinen rechtlichen Rahmen bzw. Kriterien gibt, beginnt der Markt bereits mit der Segmentierung in „grüne“ und „braune“ Wirtschaftstätigkeiten. Beispielsweise analysiert die Plattform Globalance (Globalance Bank, Schweiz) Unternehmen nach ihrem Erwärmungspotenzial und differenziert diese auch demgemäß.

Ähnliches zeigt sich auch in einer Umfrage von Fitch unter 182 globalen Banken Anfang 2020. Diese ergab, dass negatives Screening oder Ausschlusskriterien, die am häufigsten angewandten ESG-Strategien im Finanzsektor bleiben. Fitch's Umfrage belegte auch, eine weit verbreitete und zunehmende Nutzung von ESG-bezogenem Screening bei Finanzierungs- und Investitionsentscheidungen der Banken.

Auch PWC hat in einer Studie („2022 – The growth opportunity of the century“) herausgefunden, dass bereits 2022 sieben von zehn Profi-Investoren in Europa auf Finanzprodukte verzichten wollen, sofern diese nicht den ESG-Kriterien entsprechen. Dabei zeigt sich jedoch, dass es noch keinen standardisier-

ten Ansatz für ESG-Ausschlüsse gibt. Kriterien und Klassifizierungssysteme variieren stark und auch die verwendeten Daten unterscheiden sich signifikant.

Eine braune Taxonomie könnte demnach zu einer stärkeren Standardisierung des Ansatzes von Investoren und Banken beim Screening von Sektoren führen, die als umweltschädlich gelten und dadurch erhebliche Verschiebungen der Finanzierungsbedingungen für betroffene Sektoren und Unternehmen mit sich bringen. Aus diesem Grund hat die PSF auch den Auftrag, eine Spezifizierung der möglichen Übergangsaktivitäten („transition activities“) für die Taxonomie zu entwickeln. Unternehmen und Investoren brauchen mehr Klarheit darüber, wie sie von Wirtschaftsaktivitäten, die erheblichen Schaden verursachen, zu weniger schädlichen und von weniger schädlichen zu letztlich nachhaltigen Wirtschaftstätigkeiten übergehen können. Die PSF soll daher auch die Frage beantworten, wie die Taxonomie die Finanzierung von Unternehmen unterstützen kann, die Kriterien für einen wesentlichen Beitrag noch nicht erfüllen oder möglicherweise nicht erfüllen können.

Der Vorsitzende der PSF Nathan Fabian stellte in einem Interview Mitte Januar bereits klar, dass die Taxonomie Unternehmen und Investoren helfen soll, Zugang zu Finanzmitteln für Übergangsaktivitäten zu bekommen. Transformationen, die vorgenommen werden müssen, damit alle ihren Teil zu einer CO<sub>2</sub>-Netto-Nullbilanz bis 2050 beitragen können.

### Berichtsansforderungen werden transparent

Auch Berichtsansforderungen wurden in der EU-Taxonomie und der dazugehörigen Verordnung behandelt. Um mehr Transparenz über substanzielle Beiträge oder (potenzielle) Schäden zu schaffen, hat die TEG Berichtsansforderungen zu den Grenzwerten unter der „Non-financial Reporting Directive“ (NFRD) definiert. Diese Grenzwerte müssen Unternehmen, die unter die NFDR fallen (siehe dazu Infobox 1), ab dem Finanzjahr 2021 öffentlich berichten. Dazu zählen etwa Umsatz, Investitionen und Betriebskosten. Auch Finanzprodukte, die als ökologisch nachhaltig vermarktet werden, müssen von Finanzinstituten zukünftig nach gewissen Transparenzanforderungen veröffentlicht werden.

Eine Gruppe aus fünf Organisationen (CDP, Climate Disclosure Standards Board, Global Reporting Initiative, International Integrated Reporting Council und Sustainability Accounting Standards Board) versucht hier sogar noch weiterzugehen und arbeitet an einem weltweit akzeptierten System der Unternehmensberichterstattung. Dazu wurde im Dezember 2020 der Prototyp eines Standards für die klimabezogene Finanzberichterstattung veröffentlicht. Diese Gruppe hat nun auch die EU und die „IFRS Foundation“ dazu eingeladen, sich an ihrer Arbeit zur Ver-

einheitlichung der klimabezogenen Berichterstattung zu beteiligen.

### Das Ziel: Klarheit und praktikable Standards

Auch wenn noch kein vollständiger und abschließender Standard vorliegt und viele wesentliche Fragestellungen unbeantwortet sind, macht die EU-Taxonomie die Nachhaltigkeit von Wirtschaftstätigkeiten und Finanzprodukten erstmals messbar und gibt Marktteilnehmern einheitliche und transparente Vorgaben. Auch die Initiativen rund um die Harmonisierung der Berichterstattung sind ein wichtiger Schritt, hin zu mehr Transparenz und Vergleichbarkeit. Die Diskussionen, vor allem rund um die braune Taxonomie zeigen, dass sich einerseits zunehmend mehr Organisationen, Behörden, Finanzinstitute und Unternehmen mit dem Thema „Sustainable Finance“ beschäftigen, aber andererseits auch, wie viel Ungewissheit und unterschiedliche Auslegungen unter den Marktteilnehmern noch vorherrschen.

Klares Ziel aller Beteiligten muss es daher sein, dass am Ende des gesamten Prozesses transparente, einheitliche und vor allem praktikable Vorgaben entstehen. Die EU ist hierbei zu einem weltweiten Vorreiter geworden. Erste positive Reaktionen auf die klare Positionierung Europas lassen sich bereits erkennen. So hat China im September letzten Jahres, noch vor den Wahlen in den USA, ein neues Klimaziel – CO<sub>2</sub>-Neutralität bis 2060 – verkündet. Es liegt nun an der EU, die ambitionierten Ziele und Zeitpläne auch mit Nachdruck weiterzuverfolgen, denn nur so kann Europa zum Standardsetzer im Bereich der nachhaltigen Finanzierungen werden. ▲

### Wer fällt unter die NFRD

- ▲ Unternehmen mit mehr als 500 Mitarbeitern,
- ▲ Unternehmen im öffentlichen Interesse,
- ▲ börsennotierte Unternehmen, sowie
- ▲ Banken & Versicherungen.

Damit eine ökonomische Tätigkeit als nachhaltig gelten kann, muss sie vier Kriterien erfüllen:

- ▲ Sie leistet einen substanziellen Beitrag zu mindestens einem der Umweltziele.
- ▲ Sie fügt keinem der anderen Umweltziele erheblichen Schaden zu.
- ▲ Sie ist im Einklang mit Mindestanforderungen in den Bereichen Arbeitsstandards und Menschenrechte.
- ▲ Sie erfüllt die durch die EU-Kommission vorgegebenen Technical Screening Criteria: Das sind quantitative und qualitative Kriterien wie etwa Schwellenwerte, anhand derer die ökologische Nachhaltigkeit von Aktivitäten festgelegt wird.



Wer sich gezielt vor Ransomware-Attacken schützt, erspart sich das Bezahlen von Lösegeld.

## Der Aufstieg von Ransomware

Früher kamen Fake-E-Mails von afrikanischen Prinzen oder angeblichen Lotto-Gewinnern und waren in einem furchtbaren Deutsch verfasst. Heute scheinen im Absenderfeld Banken, Zahlungsdienstleister oder der eigene CFO auf. Die E-Mails können dabei täuschend echt aussehen, im Hintergrund versteckt sich jedoch ein Angreifer, der es auf die Zugangsdaten oder auf interne Firmengeheimnisse abgesehen hat. Gelingt der Angriff mündet er nicht selten in einer Erpressung.

### Der Autor:



**Hannes Lorenz**  
ist Security Consultant bei Hackner Security Intelligence

**D**as Thema heißt Phishing und ist aktuell einer der weitverbreitetsten Wege, Unternehmen anzugreifen. Firmen haben in den letzten beiden Jahrzehnten viel gelernt und ihre IT-Infrastruktur gut abgesichert. Die Angreifer wenden sich daher zunehmend den Mitarbeitern zu. Tagtäglich werden tausende E-Mails verschickt, darunter auch solche, mit denen Zugriff auf Unternehmen erlangt werden soll.

### Hände hoch oder ich verschlüssele!

Im Mai 2017 ereignete sich ein weltweiter Cyberangriff von bis dahin ungeahnten Ausmaßen. Die Schadsoftware WannaCry befahl in etwa 150 Ländern über 230.000 Computer. Dabei wurden alle darauf befindlichen Daten verschlüsselt und die Benutzer aufgefordert, einen gewissen Geldbetrag in Bitcoin zu bezahlen, um wieder Zugriff zu erlangen. Viele Unternehmen standen vor der Situation, für ihre eigenen Daten Lösegeld – oder „Ransom“, wie es im Englischen heißt – bezahlen zu müssen. Aus diesem Grund wird Ransomware auch oft als Erpressungstrojaner bezeichnet. Besonders aggressive Ransomware-Varianten verbreiten sich zusätzlich im internen Netzwerk weiter, nutzen Schwachstellen in internen Systemen aus und machen Dateien unzu-

gänglich, auf welche der Benutzer oder der Rechner Zugriff besitzt – das betrifft dann auch Netzlaufwerke ganzer Abteilungen.

### Zunahme der Infektionen

Seit 2017 nimmt diese Art von Angriffen stetig zu. Europol veröffentlicht dazu einmal jährlich einen Bericht, in welchem die aktuelle Bedrohungslage analysiert und zusammengefasst wird: das Internet Organised Crime Threat Assessment (IOCTA). Dieser, auch für Laien interessante und sehr gut lesbare Bericht, dient als Zusammenfassung der aktuellsten IT-Risiken des Vorjahres. Ransomware ist darin seit einigen Jahren ein fixer Bestandteil. Neuerdings zeichnet sich leider ab, dass auch regelmäßige Backups oft nicht mehr vor den Folgen einer solchen Attacke bewahren können. Die neuesten Angriffsformen machen die Daten nicht nur unzugänglich für die Benutzer selbst, sondern schicken sie gleichzeitig zum Angreifer (sog. Double Extortion Ransomware). Wird das Lösegeld nicht bezahlt, werden die Daten im Darknet an den Höchstbietenden versteigert.

### Einen Angriff zum Mitnehmen bitte!

Besonders gefährlich ist der Trend, gezielte Attacken als Dienstleistung anzubieten. Ransomware-as-a-

## What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

## How to make money with Satan?

First of all, you'll need to **sign up**. Once you've sign up, you'll have to log in to your account, create a new virus and download it. Once you've downloaded your newly created virus, you're ready to start infecting people.

Now, the most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will keep a 30% fee of the income, so, if you specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the number of infections and payments you have.

Ransomware-as-a-Service bietet Ransomware-Funktionalität auf Knopfdruck.

Service (RaaS) heißt das Stichwort. Hierfür müssen Angreifer kein detailliertes technisches Know-How besitzen, um die Schadsoftware verbreiten zu können, sondern können den Angriff ganz einfach über einen RaaS-Anbieter im Darknet durchführen. Ein Beispiel hierfür ist die RaaS-Plattform „Satan“, bei welcher sich der Angreifer lediglich ein Konto erstellen muss und danach zielgerichtete, flexible Ransomware-Angriffe über das Satan-Portal starten kann. Die Plattformbetreiber erhalten am Ende etwa 30 Prozent des Gewinns.

### Was tun?

Die technische Absicherung von IT-Systemen geht immer einher mit der Schaffung eines Sicherheitsbewusstseins unter den Mitarbeitern. In der täglichen Arbeit sollten dabei die folgenden Vorgaben zur Routine werden:

- ▲ Hinterfragen Sie die Legitimität von E-Mails, Anrufen und SMS.

- ▲ Verwenden Sie unterschiedliche Passwörter und nutzen Sie einen Passwort-Manager.
- ▲ Setzen Sie, wo immer möglich, 2-Faktor-Authentifizierung ein.
- ▲ Verwenden Sie aktuelle Software und Antiviren-Software.
- ▲ Melden Sie auffälliges Verhalten an Ihre Sicherheitsabteilung.

Da das Angreiferverhalten in den letzten Jahren immer besser und konkreter auf die Unternehmensmitarbeiter abgestimmt wurde, trägt jeder Einzelne dazu bei, den Level der IT-Sicherheit eines Unternehmens zu stärken und zu verbessern. Nur durch die Zusammenarbeit der Unternehmens-IT-Abteilung und der Mitarbeiter kann eine robuste Abwehr gegenüber Cybersecurity-Risiken gelingen. Die steigende Vernetzung und Digitalisierung wird auch weiterhin dazu führen, dass neue Sicherheitsrisiken auftreten und einer gemeinsamen, gesamtheitlichen Lösung bedürfen. ▲

## Sicherheitscheck statt Ransom-Blues

HACKNER Security führt gemeinsam mit Schwabe, Ley und Greiner gezielte IT-Sicherheitschecks durch. Dabei werden die Zahlungsverkehrsprozesse von Unternehmen vollumfänglich auf die Probe gestellt: Wo besteht Angriffspotenzial? Was passiert, wenn ein Phishing-Angriff erfolgreich war? Könnte ein Angreifer aktiv in Zahlungsprozesse

eingreifen und Zahlungen manipulieren? Welche Backup-Verfahren gibt es im Fall einer Verschlüsselung? Unserer Erfahrung nach gibt es hier häufig Optimierungspotential – eine Überprüfung durch unser Team verschafft Ihnen Einsicht in technische und organisatorische Sicherheitsmängel, sowie deren Behebung.

Contains accounting documents, and accounts, plus a lot of important information that may be of value to competitors or interested parties. All files of actual information. Also in the archive you will get several databases that are no less interesting.

Archive in zip format

1. Files pdf,docx,xlsx - 22328
2. Database - 3

When the auction is over, you will be provided with a download link from the cloud with the following deletion.

Minimum deposit:	\$5,000	Top bet:	--
Start price:	\$50,000	Blitz price:	\$100,000

**Opened** Time left: **6 days, 18 hours, 33 minutes and 12 seconds**

Mittels Ransomware gestohlene Daten werden im Darknet versteigert.

## Voll digitalisiertes Garantiegeschäft

Wenn man in späterer Zeit an das Jahr 2020 zurückdenkt, werden zumindest zwei Dinge im Gedächtnis bleiben: zum einen natürlich ein Virus, das uns gezwungen hat, unser soziales Leben auf ein Minimum zu reduzieren und zum anderen der durch Social Distancing beschleunigte Trend zur Digitalisierung. Vieles, was zuvor papierhaft abgewickelt wurde, wanderte in die virtuelle Sphäre und ermöglichte dadurch entsprechende Effizienzgewinne.



Ludgar Janßen  
ist Geschäftsführer  
bei Digital Vault  
Services

**E**in Beispiel dafür ist das Geschäft mit Garantien. Nach wie vor ist die Fehleinschätzung weit verbreitet, dass Bürgschaften immer papierhaft ausgestellt und mit einer Unterschrift versehen sein müssen. Tatsächlich können solche in Deutschland und Österreich immer auch digital ausgestellt und abgewickelt werden, es wurde halt kaum praktiziert.

In dieses Vakuum ist die Digital Vault Services GmbH (DVS) gestoßen und hat ein Geschäftsmodell zur vollständigen Digitalisierung des gesamten

Aval-Managements etabliert. Das Trade-Finance-Fin-Tech hat in Zusammenarbeit mit dem bayerischen Bauunternehmen Lindner Group KG, dem kanadische IT-Provider GlobalTrade Corporation, 16 Unternehmen verschiedener Branchen mit intensivem Avalgeschäft, sowie Kreditversicherern und Banken das SaaS-Produkt „Guarantee Vault“ entwickelt.

Der Guarantee Vault ist das zentrale Register für die Erstellung und sichere Aufbewahrung digitaler Avale. Zudem ermöglicht es den jeweiligen Beteiligten Avisierung, Freigabe, Änderung und Rückgabe ihrer Garantien. Eine nahtlose, digitale Anbindung bestehender Bank- oder Versicherungsportale sowie von Multi-bank-Plattformen oder ERP-Systemen ist über APIs möglich. Über API oder Webbrowser kann auch der Begünstigte Zugriff auf das Zentralregister erhalten.

**TreasuryLog sprach mit Ludger Janßen, dem Geschäftsführer der DVS.**

**TreasuryLog:** *FinTechs sind ja in aller Munde. Mit Ihnen haben Sie jetzt das Aval-Geschäft im Visier.*

**Janßen:** Der Fokus unserer Aktivitäten liegt nicht auf „Tech“. Es geht nicht um die Umsetzung einer technischen Idee, sondern um die Lösung eines konkreten Problems des täglichen Geschäftslebens: Wie wickle ich Garantien so effizient und transparent wie möglich ab, während alle Transaktionsbeteiligten gleichzeitig eingebunden sind?

**TreasuryLog:** *Stoßen Sie dabei nicht auf Vorbehalte? Sind Unternehmen wirklich bereit, die papierhafte Abwicklung aufzugeben?*

**Janßen:** Wichtig war die juristisch eindeutige Aufarbeitung. Der Zwang zum papierhaften Ausstellen und Unterschreiben ist in vielen Ländern bereits vor Jahren für den Wirtschaftsverkehr zwischen Unternehmen eingeschränkt oder abgeschafft worden. So können in Deutschland und Österreich Bürgschaften und Garantien für Unternehmen immer auch digital ausgestellt und abgewickelt werden. Bevor wir unsere Dienstleistungen in einem Land anbieten, führen wir immer eine gründliche juristische Analyse durch, wobei wir durch internationale Großkanzleien unterstützt werden.

**TreasuryLog:** *Wie sieht der typische Kunde von Digital Vault Services aus?*

**Janßen:** Ganz grundsätzlich steht der Guarantee Vault allen interessierten Unternehmen jeglicher Größe und Branchen offen, richtet sich aber naturgemäß an Firmen mit nennenswertem Avalgeschäft. Als Avalbegünstigter bietet die Nutzung des Vaults schon ab einigen wenigen Avalen im Jahr erhebliche Vorteile. Wichtig ist mir auch zu betonen, dass es sich dabei neben Bankavalen und Kautionsversicherungen der Kreditversicherer insbesondere auch um Konzernavale handeln kann.

**TreasuryLog:** *Sie sprachen von Vorteilen. Welche sind das im Wesentlichen?*

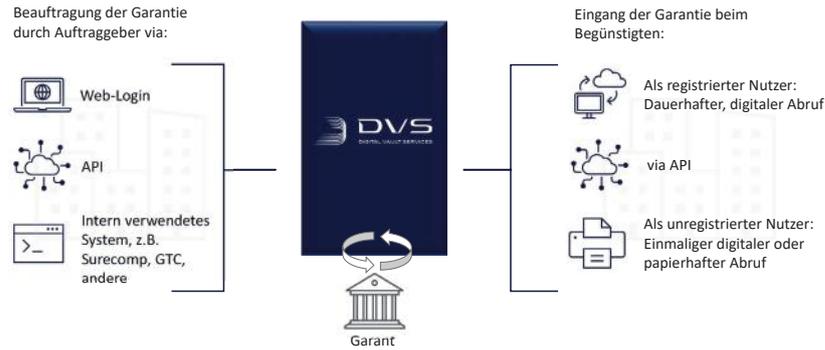
**Janßen:** Zunächst sind ganz erhebliche Effizienzgewinne und Kosteneinspareffekte zu nennen. Niemand beschäftigt sich gerne mit Papierkrieg. Wir gehen gegenüber dem Papierprozess von einem Gesamteffekt von durchschnittlich 35 Prozent für jeden der Beteiligten aus. Zusätzlich werden durch die nahtlose Datenübermittlung Fehlerquellen minimiert, die Prozesstransparenz erhöht und die Abwicklung insgesamt signifikant beschleunigt.

**TreasuryLog:** *Welche Voraussetzungen muss ein Unternehmen erfüllen, um bei DVS anzudocken?*

**Janßen:** Es gibt grundsätzlich für keinen der Avalbeteiligten technische Mindeststandards. Zugang zum Guarantee Vault und die Nutzung verschiedener digitaler Vorteile sind für jeden bereits mittels der gängigen Webbrowser möglich. Zur Nutzung aller Vorteile des Vaults sollte sich ein Avalauftraggeber jedoch digital an den Vault anbinden. Dazu kann er sich direkt an uns wenden oder an seine Kreditversicherer oder Banken – hier sind wir mit vielen hinsichtlich Anbin-

## Ein- und Ausgangskanäle der Plattform

DVS bietet verschiedene Ein- und Ausgangskanäle auf und von ihrer Aval-Plattform.



derung an den Garantie Vault im Gespräch bzw. bereits in Umsetzung und live. Ein Avalbegünstigter braucht zunächst grundsätzlich nichts unternehmen. Er erhält vom Garantie Vault aufgrund der vom Auftraggeber bereitgestellten Informationen automatisch den digitalen Zugang zu seinem Aval.

**TreasuryLog:** Können Sie bereits Angaben zu den Kosten machen, die durch die Auslagerung auf DVS entstehen?

**Janßen:** Die Zusammenarbeit ist für die bei kleinen und mittelgroßen Begünstigten zu erwartenden Avalmengen grundsätzlich kostenlos. Ehrlicherweise profitiert er von der digitalen Umstellung sofort und ganz erheblich. Avalauftraggeber haben die Möglichkeit, zwischen einem Starterpaket und drei unterschiedlichen, mengenabhängig gestaffelten, sogenannten Bundles, zu wählen. Beim Starterpaket erfolgt der Zugang zunächst per Webbrowser, eine API kann problemlos über ein Bundle zugebucht werden. Beim Starterpaket fällt je Aval eine einmalige Transaktionsgebühr von 14 Euro an, die sämtliche Services beinhaltet, inklusive künftiger Änderungen, Verlängerungen oder Rückgabe des Avals. Alle Bundles beinhalten in ihrem Paketpreis neben einem professionellen Onboarding auch die kostenlose API-Anbindung an den Vault, inklusive kostenloser Abwicklung einer fest vereinbarten Avalmenge. Lediglich die Kosten der internen API-Erstellung auf Seiten des Auftraggebers kommen noch hinzu.

**TreasuryLog:** Welche Garantieinstrumente und welche Märkte bedienen Sie – weltweit oder im deutschsprachigen Raum?

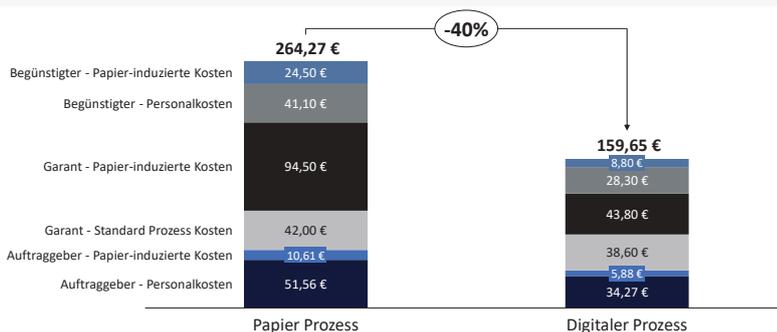
**Janßen:** Wir decken alle direkten Bürgschaften und Garantien ab, das heißt Bankavale, Kautionsversicherungen und Konzernbürgschaften. Die deutlich komplexeren und juristisch anspruchsvolleren indirekten Avale sowie Standby Letters of Credit werden zu einem späteren Zeitpunkt folgen. Nach erfolgreicher Einführung im deutschsprachigen Raum wird die Plattform weltweit auf andere dafür geeignete Regionen ausgeweitet werden. Die erste Expansion nach Frankreich und in die Schweiz ist bereits beschlossen und für das vierte Quartal 2021 in Vorbereitung.

**TreasuryLog:** Welche Sicherheits- und Verfügbarkeitsstandards darf man von Ihrer Plattform erwarten?

**Janßen:** Der Garantie Vault entspricht höchsten technischen Sicherheitsstandards. Dabei garantieren wir die auch von Banken und Kreditversicherungen bekannte permanente Verfügbarkeit von mindestens 99,5 Prozent. Ohne Gewährleistung dieses Levels würden wir von den mit uns zusammenarbeitenden nationalen und internationalen Banken und Kreditversicherungen auch gar nicht als Partner akzeptiert. Darüber hinaus läuft zurzeit auch unsere Zertifizierung nach ISO 27001, was wiederum die Einhaltung diverser Qualitäts- und Prozessstandards sicherstellt.

## 40% Kosteneinsparung durch Digitalisierung der Avale

Auftraggeber - Garant\* - Begünstigter\*



Durch die Digitalisierung von Avalen sollen Effizienzgewinne von rund 40 Prozent realisierbar sein.

## Neuer Partner, neue Fachabteilung

Gerüstet für die Zukunft: SLG stärkt seine Partnerbasis und gründet ein neues Kompetenzfeld für strukturierte Finanzierungen.



Florian Maak: Neuer Partner im Team von SLG.

In den letzten Jahren hat unser Spezialteam „Treasury mit SAP“ eine sehr erfreuliche Entwicklung genommen. Einem steilen Wachstumspfad folgend konnten viele interessante und herausfordernde Projekte gewonnen werden.

Florian Maak ist „Employee No.2“ im SAP-Team von Schwabe, Ley & Greiner: 2013, kurz nach der Team-Gründung, stieg er – nach sechs Jahren im Bereich SAP Treasury bei IBM Global Business Consulting – bei uns ein. Unter unermüdlichem Ein-

satz gelang es ihm, nicht nur eine ganze Reihe von neuen Kunden zu gewinnen, sondern auch ein schlagkräftiges Team aufzubauen.

Heute ist das SAP-Team aus dem SLG-Beratungsportfolio nicht mehr wegzudenken. Florians Verantwortungsbereich umfasst dabei die Bereiche Finanzgeschäfte und Accounting sowie Risiko- und Liquiditäts-Management, wobei er und sein Team stets die neuesten SAP-Weiterentwicklungen angehen, sei es in SAP S/4HANA oder in SAP Analytics Cloud. Und, wie wir sagen dürfen, mit durchschlagendem Erfolg. Florians Kunden schätzen seine freundliche Art und sein Verständnis ihrer individuellen Bedürfnisse. Das schätzt auch unsere Geschäftsführung: Per 1. November 2020 wurde Florian Maak zum Partner bei Schwabe, Ley & Greiner ernannt.



Benedikt Millauer: Verantwortet die Abteilung „Structured Finance & Risk Management“.

### Neue Kompetenzgruppe im Bereich Finanzierung

Unser Corporate-Finance-Bereich wächst und wächst! Von der Erstellung von nachhaltigen Finanzierungskonzepten bis zur Transaktionsbegleitung, Verhandlung und Implementierung von maßgeschneiderten Finanzierungsbausteinen – Schwabe, Ley und Greiner bietet Kunden in der DACH-Region seit Jahren umfassende und kompetente Beratung im Bereich Corporate Finance aus einer Hand.

Seit November 2020 verantwortet Benedikt Millauer die neu geschaffene Abteilung „Structured Finance & Risk Management“. Die Abteilung wird sich schwerpunktmäßig mit Corporate Finance, strukturierten Finanzierungen im Projekt- oder Akquisitions-Kontext und Risiko-Management beschäftigen. Benedikt

Millauer ist seit über neun Jahren in der Unternehmensberatung tätig und hat weitreichende Projekt- und Transaktionserfahrung im Bereich M&A, Unternehmens- und Projektfinanzierung und Financial Modeling.

Gestartet ist Benedikt bei Ernst & Young in der Wirtschaftsprüfung. Unsere Kunden schätzen seine Beratung aus einer Hand: Finanzierungs- und Transaktionserfahrung wird verknüpft mit Controlling, Accounting und Treasury Expertise. Bonitätseinschätzungen und Finanzierungskonzepte werden mit Risiko-Management Themen verknüpft und umgekehrt.

Die Mitglieder seines Teams sind die Berater der bisherigen Kompetenzgruppe „Marktrisiko-Management“. Diese verfügen über ausgeprägte technische Kenntnisse, die sie neben der Risikoberechnung auch bei Finanzmodellierungen einsetzen und Erfahrungen in der Unterstützung von Finanzierungsprojekten haben. Wir freuen uns, im nachgefragten Segment der strukturierten Finanzierungen nun eine zusätzliche schlagkräftige Truppe an die Seite unserer Kunden stellen zu können. ▲



# Treasury leben. Ziele erreichen.

Besuchen Sie unsere Seminare vor Ort oder seien Sie online „live“ dabei!

Über 30 Jahre Erfahrung in der Treasury-Beratung und mehr als 1.000 veranstaltete Seminare und Lehrgänge machen Schwabe, Ley & Greiner zu Ihrem kompetenten Partner in der Treasury-Ausbildung.

## Weiterbildung auch online im Homeoffice

### Seminare

#### Cash-Management

- ▲ Cash- und Liquiditäts-Management
- ▲ Die neue Welt des Zahlungsverkehrs
- ▲ Sicherheit im Zahlungsverkehr: Prozesse und Technik sicher gestalten
- ▲ Cash-Pooling aus rechtlicher Perspektive
- ▲ Payments im Point-of-Sale und E-Commerce als Erfolgsfaktoren

#### Corporate Finance

- ▲ Finanzstrategie, Rating und Kreditverträge
- ▲ Liquiditätsplanung: einfach, systemgestützt, zukunftsfähig
- ▲ Kreditverträge aus finanzwirtschaftlicher Perspektive
- ▲ Financial Modeling für die Finanzabteilung
- ▲ Financial Modeling Vertiefung: M&A und Akquisitionsfinanzierung

#### Risiko-Management

- ▲ Währungs- und Zinsrisiko-Management
- ▲ Finanzmathematik und Zinsrechnung
- ▲ Portfolio-Management für Anleger und Schuldner
- ▲ Hedge Accounting und Bilanzierung für Treasurer
- ▲ Risiko-Management für Fortgeschrittene

#### Systeme

- ▲ Digitalisierung im Treasury: Technologien und Systemfunktionalitäten
- ▲ Treasury-Management-Systeme: Nutzen, Funktion und Integration
- ▲ SAP: S/4HANA – was Sie im Treasury wissen müssen
- ▲ SAP: Cash-Management und Zahlungsverkehr
- ▲ SAP: Risiko- und Liquiditäts-Management

### Lehrgänge

- ▲ Einsteiger-Lehrgang: Treasury-Kick-Off
- ▲ Grundlagen-Lehrgang: Treasury-Management
- ▲ Führungskräfte-Lehrgang: Treasury-Express



21.-23. April 2021 | Virtuelle Fachkonferenz

# 32. FINANZSYMPOSIUM

Die digitale Networking-Plattform für alle Treasury- & Finanzthemen

## Virtueller Kongress auf höchstem Niveau

Die Treasury-Gemeinde trifft sich endlich wieder – aufgrund der aktuellen Lage nur virtuell, dafür aber mit einer Fülle an neuen Networking-Möglichkeiten und Formaten. Unser „Matchmaking Tool“ vernetzt Sie mit relevanten Personen, die Ihre Interessen teilen, neue Formate wie „Virtual Event Bag“, „Studio Interview“ oder „Treasury Café“ ermöglichen einen ungezwungenen Austausch der Teilnehmer, und auf der „Virtual Happy Hour“ und am „Virtuellen Gala-Abend“ werden Sie nicht nur unterhalten, sondern auch überrascht. Kreieren Sie gemeinsam mit uns ein spannendes 32. Finanzsymposium, vollgepackt mit aktuellen Themen und Herausforderungen.



**Sigmar Gabriel**

Bundesaußenminister a. D.

**Das europäisch-amerikanische Verhältnis – von der Luftbrücke zur Zugbrücke?**

**Uli Hoeneß**

Ehrenpräsident FC Bayern München eV

**Auf ein Wort mit Uli Hoeneß – Strategie und Führung im Profisport und Unternehmertum**



## Werden Sie Partner!

Profitieren Sie von unserem starken Besuchernetzwerk. Durch unser Matchmaking-Tool werden die richtigen Menschen, Ideen und Ressourcen gezielt zusammengebracht. Der perfekte Gesprächspartner hat sich ganz sicher für unseren Kongress registriert und unser Tool hilft Ihnen dabei ihn zu finden. Nutzen Sie diese Chance sich mit Führungskräften aus dem DACH-Raum zu vernetzen und präsentieren Sie Ihre Produkte und Lösungen.

[www.finanzsymposium.com](http://www.finanzsymposium.com)

