



Ausgabe 50 – Dezember 2015

Liebe Leserinnen und Leser,

wir freuen uns, Ihnen die neueste Ausgabe unserer Corporate Treasury News präsentieren zu können.

Wenn Sie Fragen oder Anregungen zu Themen haben, die künftig in unserem Newsletter kurz behandelt werden sollen, dann schreiben Sie uns:
de-corporate-treasury@kpmg.com

Aktuelle Meldungen rund um das Finanz- & Treasury-Management finden Sie auf unserer [Internetseite](#) oder über Twitter: www.twitter.com/KPMG_DE_FTM

Mit besten Grüßen,

Prof. Dr. Christian Debus

Carsten Jäkel

In dieser Ausgabe

Erfahrungsbericht zum Setup einer Treasury-Organisation

Seite 2

Business Continuity im Treasury - was tun, wenn das TMS streikt?

Seite 4

Fallstricke bei der Ausgestaltung konzerninterner Sicherungen

Seite 6

Veranstaltungen und Termine

In unseren kostenfreien *Webinaren* nehmen wir zu aktuellen Themen aus dem Bereich Finanz- & Treasury-Management Stellung und informieren Sie über Strategien und die konkrete Implementierung.

Wählen Sie sich online ein und nehmen Sie an unseren thematischen Expertenrunden teil:

28. Januar 2016, 16:00 h

[Währungsmanagement - Steuerung der bilanziellen Fremdwährungsrisikoposition](#)

Von jedem Webinar fertigen wir einen Mitschnitt des Vortrags an. Sie finden ihn in unserem [Webinar-Archiv](#).

Erfahrungsbericht zum Setup einer Treasury-Organisation

Im Frühjahr/Sommer 2014 wurde durch die Siemens AG entschieden, die österreichische Anlagensbau-Tochter VAI Metals Technologies in ein Joint Venture mit der Mitsubishi Heavy Industries-Tochter (MHI) Mitsubishi Hitachi Metals Machinery einzubringen. Im Rahmen dieses Projekt erhielten Miljenko Solje als zukünftiger Leiter Finance und Jeremy Hamon als zukünftiger Leiter Treasury den Auftrag, eine neue Treasury-Organisation für das zukünftige Joint Venture mit dem Namen Primetals aufzubauen. Im Interview berichten beide von den Herausforderungen und Erfolgsfaktoren:



Welcher Zeitrahmen stand Ihnen für den Aufbau des Treasury zur Verfügung?

Miljenko Solje:

Das Ausgründen der Gesellschaften aus der bestehenden Organisationsstruktur startete im Frühjahr/Sommer 2014. Zeitgleich begannen wir mit der Bankkonteneröffnung und somit der Sicherstellung der Zahlungsfähigkeit.

Jeremy Hamon:

Für den eigentlichen Aufbau der Treasury-Organisation war ein sehr enger Zeitplan von nur 2,5 Monaten vorgegeben.

Was waren die größten Herausforderungen auf dem Weg zur selbstständigen Treasury-Organisation?

Miljenko Solje:

Die größte Herausforderung war sicherlich die mangelnde interne Personalausstattung. Das komplette Treasury Team musste zunächst definiert und anschließend rekrutiert werden. Folglich bestand das Projektteam seitens Primetals für die ersten zwei Monate nur aus Jeremy Hamon und mir.

Jeremy Hamon:

Ein nicht zu unterschätzender Punkt war die Verankerung des Themas „Treasury“ in die neue Organisation. Hintergrund ist, dass alle wesentlichen Treasury-Aufgaben in der alten Organisation von Siemens Financial Services bzw. MHI übernommen wurden. Herausfordernd war dabei insbesondere die Schnittstellen zu angrenzenden Abteilungen zu definieren und die Treasury-Sichtweise in den Köpfen zu verankern.

Was waren die wesentlichen Herausforderungen bei der Sicherstellung der Zahlungs- und Finanzierungsfähigkeit?

Jeremy Hamon:

Neben der zeitgerechten Konteneröffnung war die Bereitstellung von Finanzierungslinien seitens der Banken die wesentliche Herausforderung. Dies war insbesondere dadurch begründet, dass nur sehr begrenzte „Financials“ für das neu zu gründende Joint Venture vorlagen und die Zeit für vertragliche Verhandlungen äußerst begrenzt war.

Miljenko Solje:

Ich erinnere mich hierzu noch sehr gut, dass die letzten Linienverträge auf den Punkt kurz vor Weihnachten unterzeichnet wurden und der Go-Live damit sichergestellt wurde.

Wie konnte die Implementierung einer Treasury IT-Lösung in dieser kurzen Frist sichergestellt werden?

Miljenko Solje:

Aufgrund der sehr kurzen Projektdauer wurde sehr schnell deutlich, dass man dieses ehrgeizige Ziel nur mit einer

SaaS-Lösung erreichen konnte. Dies ermöglichte einen schnellen Projektstart also auch einen unkomplizierten und zügigen Rollout der Lösung bei den weltweiten Tochtergesellschaften.

Jeremy Hamon:

Ein weiterer Faktor war es, eine Lösung und IT-Infrastruktur aufzusetzen, die den hohen internen Anforderungen an die IT-Sicherheit gewachsen war. Durch die SaaS-Lösung konnte beispielsweise sichergestellt werden, dass Schnittstellen zu Marktdaten oder Handelsplattformen direkt vom IT-Anbieter umgesetzt wurden.

Miljenko Solje:

Im Rahmen der Auswahl und Implementierung ist sicherlich die sehr gute Unterstützung des externen Beraters zu nennen. Dies spiegelte sich zum einen in einem sehr effizienten und schnellen RfP-Prozess als auch in der Rolle des Implementierers und Kümmerers im Rahmen des gesamten Projekts wider.

Liquidität spielt insbesondere in neu gegründeten Unternehmen eine wesentliche Rolle. Welche Maßnahmen haben Sie ergriffen, um Transparenz über die Liquidität zu erhalten und diese zu verbessern?

Jeremy Hamon:

Vom ersten Tag des Projekts stand das Thema Liquiditätsplanung sehr weit oben auf der Agenda. Innerhalb nur einer Woche wurde ein provisorisches und Excel-basiertes Tool zur Liquiditätsplanung auf die Tochtergesellschaften ausgerollt, um erste Indikationen hinsichtlich der benötigten Liquidität zu erhalten. Parallel wurde eine robuste Systemlösung im ausgewählten Treasury-Management-System (TMS) implementiert.

Miljenko Solje:

Dieser sehr schnelle Start trug maßgeblich dazu bei, das gruppenweite Bewusstsein für das Thema Liquidität von Anfang an zu prägen. Neben der Planung selbst wurde das Thema Liquidität und Cash durch verschiedene Kommunikationskanäle regelmäßig als Prio-1-Thema in die Organisation getragen. Ein sehr wirkungsvolles und wichtiges Instrument war dabei der Treasury-Projekt-Newsletter. Dieser wurde alle 2-3 Wochen an die weltweite Finance Community versendet und enthielt wertvolle Informationen über aktuelle und anstehende Themen.

Mit Blick auf die sehr kurze Projektdauer mussten sicherlich gewisse Themen priorisiert werden und andere wiederum in eine Zeit nach dem „Day 1“ geschoben werden. Können Sie uns hierzu passende Beispiele nennen?

Miljenko Solje:

Oberste Priorität hatte die Sicherstellung der Zahlungsfähigkeit sowie die Bereitstellung der Finanzierungslinien. Ähnliche Priorität hatte die Absicherung der weltweiten Fremdwährungsrisiken zu dem Zeitpunkt, als die bestehenden internen Sicherungen mit Siemens terminiert wurden. In diesem Zusammenhang steht auch die Implementierung des TMS also Prio-1-Thema.

Jeremy Hamon:

Nachgelagerte Priorität hatten hingegen Themen wie Cash-Pooling, Garantiemanagement, Kreditrisikomanagement, zentralisierter Zahlungsverkehr oder Hedge Accounting. Diese Themen wurden alle nach dem „Day 1“ ab Januar dieses Jahres umgesetzt.

Was waren die wesentlichen Change- bzw. Project Management-Herausforderungen?

Jeremy Hamon:

Die Schaffung des Bewusstseins für die Notwendigkeit einer zentralen Treasury-Funktion war sicherlich eine der größten Herausforderung im Change Management-Prozess.

Miljenko Solje:

Ein weiterer wesentlicher Punkt war das „Rightsizing“ der Prozesse und Systeme auf die neue Unternehmensgruppe. Dies beinhaltete das Aufbrechen bestehender Strukturen, Abschalten überdimensionierter Systemlösungen sowie kontinuierliches Change Management auf personeller Ebene.

Rückblickend betrachtet, was waren die wesentlichen Erfolgsfaktoren für dieses ambitionierte Projekt?

Miljenko Solje:

Wesentlich für den Erfolg war die vertrauensvolle Zusammenarbeit zwischen allen Beteiligten, sprich neuem

Treasury, Accounting, Controlling, Beschaffung, IT, der Leitungsebene mit CFO und den externen Beratern. Die gute Projektstruktur und Methodik, bereitgestellt durch die externen Berater, verhalf uns, zielgerichtet die zu bewältigenden Aufgaben abzuarbeiten.

Jeremy Hamon:

Darüber hinaus war es von hoher Bedeutung die lokalen Einheiten weltweit mit einzubeziehen. Die interne Kommunikation war maßgeblich für den Projekterfolg.

Autor: Harald Fritsche, Senior Manager, hfritsche@kpmg.com

Business Continuity im Treasury - was tun, wenn das TMS streikt?

Freitag, 15.30 Uhr im Backoffice der Treasury-Abteilung eines internationalen deutschen Industrieunternehmens: das Einlagekapital für die neue Tochtergesellschaft in den USA muss heute noch überwiesen werden. Alle Unterschriften sind eingeholt, die US Dollar-Zahlung im Treasury-Management-System erfasst und der Leiter Treasury hat vor wenigen Minuten die abschließende Freigabe im System für den Transfer der Zahlung an die Bank erteilt.



Doch kurz vor Ende der Cutoff-Zeit der Hausbank treten dem zuständigen Backoffice-Mitarbeiter langsam die Schweißperlen auf die Stirn. Anstatt, wie üblich, einige Sekunden nach Zahlungsfreigabe eine Ausführungsbestätigung der Bank in Form einer grünen Ampel neben der Zahlung auf dem Bildschirm zu sehen, steht dort – nichts. Ein technisches Problem? Hat das Treasury-Management-System die Zahlung überhaupt an das firmeneigene SWIFT-Gateway transportiert? Ist dieses möglicherweise derzeit nicht verfügbar? Gibt es am Ende ein Verarbeitungsproblem bei der Bank? Und falls wirklich ein Problem gefunden wird, ist dieses schnell genug lösbar oder muss kurzfristig eine alternative Zahlungsmöglichkeit per E-Banking oder Fax gefunden werden?

Wohl dem, der in dieser Situation die Nerven behält und über einen kompetenten und schnell handelnden technischen Support verfügt, der Transparenz über mögliche Fehlerquellen entlang der gesamten Treasury-Prozesskette und entsprechende Anweisungen und Dokumentationen in der Schublade hat, wie in solchen Notfällen vorzugehen ist. Denn nicht immer sind es nur kleinere Vorfälle im Umfeld eines Treasury-Management-Systems wie eine Zahlung, die nicht verschickt wird, ein Kontoauszug, der nicht eingespielt wird, oder ein FX-Geschäft, das in der externen Handelsplattform zwar abgeschlossen wurde, im hauseigenen System aber nicht erscheint. Was also tun, wenn wirklich mal ein umfangreicheres Szenario eintritt, ganze Systeme in Rechenzentren ausfallen oder schlichtweg die Arbeitsplätze für das Treasury nicht zugänglich sind? Existieren Pläne für diese Situationen, sind sie allen Mitarbeitern bewusst und – ebenso wichtig – werden sie regelmäßig überprüft und aktualisiert?

Vernetzte globale Organisationen sind einer geradezu unendlichen Anzahl an Bedrohungsszenarien ausgesetzt, die teilweise überwacht und eingeschränkt werden können, teilweise aber nicht vorhersehbar sind. Dummerweise wird die zweite Kategorie immer bedeutender, beginnend mit natürlichen Katastrophen, über technisches und menschliches Versagen bis hin zu bewussten Angriffen cyberkrimineller Natur. Planungen und Vorkehrungen zur Risikovorsorge sind daher sowohl auf fachlicher Ebene als auch in der technischen Infrastruktur erforderlich. Diese Maßnahmenpakete werden üblicherweise mit den übergeordneten Fachbegriffen „Business Continuity“ (für die Anwendersicht) oder „Disaster Recovery“ bzw. „Service Continuity“ (für die IT-Sicht) tituiert. Dabei geht es einerseits um die Vermeidung möglicher Katastrophen- oder Notfallsituationen und die Verringerung ihrer Eintrittswahrscheinlichkeiten im Sinne von risikominimierenden Maßnahmen. Andererseits aber auch insbesondere um eine angemessene Reaktion auf diese Ereignisse zur Fortführung der Kernprozesse durch eine gezielte Wiederherstellungsplanung.

Soweit die reine Theorie, wie sie auch im Rahmen IT-technischer Normen wie den ITIL-Verfahren oder den ISO- bzw. nationalen BSI-Standards beschrieben ist und noch keine Treasury-Spezifika berücksichtigt. Tatsache ist je-

doch, dass eine global aufgestellte Treasury-Organisation, deren Prozesse auf einer komplexen Systemlandschaft mit einer Vielzahl intern wie extern angebundener und vernetzter Systeme aufbauen, niemals umfänglich auf alle Eventualitäten vorbereitet werden kann. Denn dies wäre gleichbedeutend mit der Kontinuität im Katastrophenfall für alle Teilfunktionen, Einheiten und Länder. Ausfallsicherer Betrieb von der Anbindung externer Handelsplattformen bis hin zu den Schnittstellen in alle lokalen Accounting-Systeme – ein Ding der Unmöglichkeit. Daher sind aus Treasury-Perspektive zunächst einige grundlegende Überlegungen von Bedeutung, wenn es darum geht, einen Ansatz zu finden, der die Besonderheiten der Treasury-Prozesse und jeweiligen Systeme berücksichtigt:

- Wie ist die allgemeine Strategie des Unternehmens im Hinblick auf das Business Continuity Management? Hier fließen die Treasury-übergreifenden Planungen ein bis hin zu der Frage, unter welchen Ausfallszenarien überhaupt ein Treasury-Notbetrieb erforderlich ist.
- Welche Rahmenbedingungen setzt die IT bzw. der/die IT-Betreiber? Systeme im Treasury sind keine Inseln und eingebettet in eine komplexe Basis-Infrastruktur aus Hard- und Software in verschachtelten Netzwerktopologien. All dies muss aufeinander abgestimmt werden, wenn es darum geht, Ausfallsicherheit zu konzipieren. Hochverfügbarkeitsanforderungen an Handels- oder Zahlungssysteme sind völlig nutzlos, wenn der IT-Dienstleister nicht die gleichen Services für die zugrundeliegenden Netze garantiert.
- Eine bereits im Produktivbetrieb komplex verteilte und wenig überschaubare Systemlandschaft für das Treasury kann nicht effizient ausfallsicher gestaltet werden. Es sollte daher zunächst mit der Optimierung der „ersten“ Architektur begonnen werden. Das Stichwort lautet hier Zentralisierung in einer einheitlichen Plattform bis hin zur Nutzung von Cloud-Diensten, um den technischen Aufwand für die „zweite“ Umgebung – die für den Notbetrieb – zu minimieren.

Die Business-Impact-Analyse im Treasury: was soll abgesichert werden?

Zwei bestimmende Faktoren setzen die Leitplanken für die Erstellung eines Treasury-spezifischen Business Continuity-Plans (BCP): Verfügbarkeit und Wirtschaftlichkeit.

Nicht die IT-technischen Möglichkeiten sollten entscheidend sein, sondern die Anforderungen an die Verfügbarkeit und die Ausfallsicherheit der zeitkritischen Geschäftsprozesse im Treasury wie etwa der Zahlungsverkehr oder der externe Handel mit Finanzinstrumenten. Die Identifikation genau dieser Prozesse (neudeutsch: „vital business functions“) und ihre Bewertung im Hinblick auf mögliche Schäden bei einem Ausfall bestimmt ihre Kritikalität und hat die Beantwortung einer entscheidenden Frage zum Ziel: wie lange kann maximal auf die Durchführung des Prozesses verzichtet werden? Höchstwahrscheinlich beginnen Sie schon zu überlegen, worauf Sie wie lange verzichten können: die Anlieferung von Cash-Forecasts der Töchter, auf Marktdaten, auf Kontoauszüge? Wie erzeugen Sie Zahlungen ohne System? Wie schließen Sie offene Future-Positionen ohne Handelsplattform?

Diese zugegebenermaßen vereinfachte Darstellung einer in der Praxis durchaus komplexen Business-Impact-Analyse der Prozesse im Treasury ist aber dennoch der entscheidende Schritt beim Aufbau eines umfassenden Vorsorgeplans: erstens, weil die Identifikation und Bewertung der kritischen Prozesse vornehmlich in der Verantwortung des Treasury selbst liegt, und zweitens, weil alle weiteren Schritte – insbesondere die IT-technischen – auf dieser Analyse aufbauen. Fragen nach möglichen Gefährdungen, Risikominimierung und Schutzbedarf führen bei besonders zeitkritischen Treasury-Prozessen logischerweise zu einem höheren Investitionsbedarf für die Sicherstellung der Verfügbarkeit. Hier kommt der zweite Leitplankenfaktor dann ins Spiel: die Wirtschaftlichkeit der Anforderungen muss sichergestellt sein, um möglichst ein Gleichgewicht zwischen Investitionen und Risikobereitschaft zu erreichen. Natürlich kann Ihre IT das Liquiditätsplanungstool so absichern, dass es bei einem Ausfall der Datenbank innerhalb von 60 Minuten wieder zur Verfügung steht. Nur: ist das wirtschaftlich sinnvoll im Hinblick auf die Zeitkritikalität des Prozesses? Und natürlich möchte Ihr Front-Office das Handelssystem gerne ohne Unterbrechung nutzen, damit keine ungeplanten P&L-Effekte eintreten. Nur: ist dies wirklich 24 Stunden erforderlich oder reduziert sich der Wunsch nicht eher auf die Spitzenzeiten eines Handelstages?

Nicht nur Papier erzeugen: regelmäßig testen und Mitarbeiter schulen

Glückwunsch. Sie haben es geschafft und einen umfangreichen Business Continuity-Plan für Ihre globale Treasury-Organisation erstellt. CFO und CIO haben Budget bereitgestellt, alle Notfallverfahren sind dokumentiert, das Treasury-Management-System wird von der IT redundant betrieben, Verantwortlichkeiten und Eskalationsschritte für bestimmte Szenarien sind definiert, für Ihre wichtigsten Ressourcen werden bei Bedarf Notfallarbeitsplätze bereitgestellt und falls doch einmal etwas passiert, haben Sie mit den wichtigsten Banken Vereinbarungen für den Notbetrieb.

Doch an dieser Stelle beginnt der Kardinalfehler vieler Unternehmen bei der praktischen Umsetzung. Einmal dokumentiert und technisch aufgebaut, verbleiben die meisten Business Continuity-Pläne mitsamt ihrer dazugehörigen technischen Disaster-Recovery-Umgebungen in den virtuellen Schubladen der Schreibtische der Verantwortlichen. Insbesondere für Treasury-Bereiche ist dieser Fehler fatal. Ihr Treasury Business Continuity-Plan enthält – im Idealfall – Szenarien, Prozesse, technische Verfahren und manuelle Workarounds, Meldewege, Eskalationsschritte und Ansprechpartner im Fachbereich, in der IT und bei Ihren externen Kontrahenten. Da liegt es in der Natur der Sache, dass diese regelmäßig aktualisiert werden müssen. Es wäre äußerst ärgerlich, wenn beispielsweise Ihr Swift-Servicebüro durch automatisches Monitoring der Verbindung zu Ihrem Rechenzentrum in der Nacht einen Ausfall feststellen würde, aber dann aufgrund eines geänderten Ansprechpartners dieses nicht erreicht und Sie am nächsten Morgen keine Kontoauszüge und keinen Finanzstatus in Ihrem Treasury-Management-System vorfinden würden.

Neben der Pflicht zur Aktualität ist das Überprüfen und Testen der Notfallmaßnahmen oberstes Gebot für einen BCP. Nur somit kann sichergestellt werden, dass neben der Operabilität der technischen Notfallsysteme auch Ihre Mitarbeiter für den Ernstfall gewappnet sind und sich das Bewusstsein und das Verständnis für die etablierten Verfahren in den Köpfen verankert haben. Damit werden zwar nicht alle Ereignisse und Ausfälle vermieden werden können, der Leiter Treasury kann aber zumindest etwas ruhiger schlafen und kein Backoffice-Mitarbeiter muss mehr kurz vor Cutoff noch in Panik verfallen.

Autor: Michael Baum, Senior Manager, michaelbaum@kpmg.com

Fallstricke bei der Ausgestaltung konzerninterner Sicherungen

In den letzten Newsletter-Beiträgen haben wir bereits auf die aktuelle Bedeutung der Wechselkurs- und Rohstoffpreisentwicklungen hingewiesen. So hat die Kupfer-Quotierung ihr Allzeithoch in 2011 von über zehntausend US-Dollar/Tonne über deutliche Kurssprünge aktuell mehr als halbiert.



Vergleichbare Entwicklungen lassen sich auch bei den anderen Buntmetallen sowie vielen weiteren Rohstoffen, wie beispielsweise Öl oder Weizen, erkennen. Neben einer verlässlichen Exposure-Ermittlung und einer abgestimmten Sicherungsstrategie stellt sich immer auch die Frage, wie einzelne Sicherungsstrategien in den Einzelabschlüssen und sonstigen rechtlichen Rahmenbedingungen abgebildet werden sollen.

Einige Treasury-Abteilungen geben feste Wechselkurs- oder feste Preiszusagen für optional abrufbare Kontingente an die Konzernunternehmen aus. Die Steuerung über solche Zusagen sollte grundsätzlich auch im Hinblick auf verschiedene Fragestellungen überprüft werden, die sich nicht aus dem Konzernabschluss ergeben.

Existieren preis- und mengenmäßig fixierte Zusagen für die Zukunft, die physisch abgerufen werden müssen, handelt es sich bei Fremdwährungen in der Regel um Derivate. Dementgegen stellen Rohstoffkontingente in der Regel sowohl handelsrechtlich als auch nach IFRS Erfüllungsgeschäfte (executory contracts) dar. Diese schwebenden Geschäfte müssen in handelsrechtlichen Einzelabschlüssen auf drohende Verluste, bzw. unter IFRS auf eine provision for onerous contracts im Sinne des IAS 37.68, überprüft werden. Die genaue Bewertung solcher Zusagen unterscheidet sich zwischen beiden GAAPs.

Existieren jedoch preis- und mengenmäßig fixierte Zusagen, die auch über einen Barausgleich abgewickelt werden können, handelt es sich grundsätzlich um Derivate (IAS 39.9). Das gilt auch, wenn die abrufbare Menge bestimmt, der Abruf selbst allerdings im Ermessen einer Partei liegt (Option).

Manche Treasury-Abteilungen sagen Unternehmen des Konzernverbunds allerdings Wechselkurse oder Rohstoffpreise zu, die bis auf Widerruf gelten und mengenmäßig nicht bestimmt sind. Diese Wechselkurs- oder Preiszusagen können während ihrer Gültigkeit sowohl als Kassageschäft als auch für zukünftige Termine abgerufen werden. Das bedeutet, dass einzelne Abrufe auf diese Zusage auch dann noch gelten, wenn für neue Abrufe bereits ein anderer Konzernkurs gilt.

Sowohl handelsrechtlich als auch nach IFRS handelt es sich bei der Zusage selbst zunächst einmal um schwebend unwirksame bzw. aufschiebend bedingte Verträge, die grundsätzlich nicht bilanziert werden müssen. Sobald aber die Kurszusage für einen zukünftigen Termin preis- und mengenmäßig fixiert wird, etwa durch einen konkreten Abruf (beispielsweise +10 Millionen US-Dollar; -8 Millionen Euro am 15. Juni nächsten Jahres), entsteht formal ein internes Derivat. Darüber hinaus könnten die Abrufe auch als Kassageschäfte abgerufen werden. In diesem Fall entstehen keine internen Derivate.

Bei diesen Zusagen stellt sich nachfolgend die Frage, wie und ab wann das Treasury die für die Kurszusage benötigten externen Derivate auf die Tochterunternehmen weiterbelasten kann. Das gilt insbesondere, wenn Gesellschaften verschiedener steuerlicher Organe betroffen sind oder Hedge Accounting analog zu IFRS-Einzelabschlüssen (beispielsweise Dutch GAAP) angewendet werden soll.

Wenn die Weiterbelastung des Marktwerts bestehender externer Derivate erst zum Jahresende vertraglich begründet, entsteht formal ein nicht marktgerecht abgeschlossenes internes Derivat. Der Terminkurs dieses internen Derivats entspricht wahrscheinlich nicht dem aktuell marktgerechten Terminkurs. Die Gewährung eines solchen Derivats muss unter Umständen (in IFRS-Einzelabschlüssen) als Einlage oder Entnahme des Gesellschafters bilanziert werden. Eine vergleichbare Interpretation kann auch steuerlich geboten sein, sodass unter Umständen hier immaterielle Vermögensgegenstände ohne Anschaffungskosten zum Teilwert aktiviert werden müssen.

Dementgegen sollten die externen Derivate über die Anlage von internen Derivaten an die Tochterunternehmen weiter belastet werden, bevor die internen Derivate einen Marktwert aufweisen (das heißt zeitgleich mit den externen). Dieser Punkt ist vor allem hinsichtlich seiner Wechselwirkung mit der EMIR-Verordnung relevant. Aus dieser Regelung müssen interne Derivate innerhalb von zwei Arbeitstagen an ein Transaktionsregister gemeldet werden. Das bedeutet, dass interne Derivate nicht rückwirkend zum Monats- oder Jahresabschluss erstellt werden können, sondern einen Prozess in der täglichen Abwicklung voraussetzen.

Alternativ müssen die Ergebnisbeiträge der externen Derivate allerdings auch nicht an die entsprechenden Tochterunternehmen des Konzerns weiter belastet werden. Für Zwecke eines Einzelabschlusses fehlt es dem Unternehmen der Treasury-Abteilung dann allerdings in der Regel an einem Grundgeschäft. Daher müssen externe Derivate in diesem Fall ohne die Nutzung von Bewertungseinheiten bzw. Hedge Accounting abgebildet werden.

Die Ausgestaltung der Sicherungsstrategie sollte in regelmäßigen Intervallen sorgfältig auf ihre Auswirkungen auf den Konzernabschluss, aber auch auf die Einzelabschlüsse, die Steuerbilanz und weitere Compliance-Themen (EMIR) analysiert werden. Nur auf diese Weise lässt sich sicherstellen, dass die Rahmenbedingungen eingehalten und genutzt werden können.

Autor: Felix Wacker-Kijewski, Manager, fwackerkijewski@kpmg.com

Impressum

Herausgeber

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt am Main

www.kpmg.de

Redaktion

Prof. Dr. Christian Debus (V.i.S.d.P.)
Partner, Finance Advisory
T +49 69 9587-4264
cdebus@kpmg.com

Carsten Jäkel

Partner, Finance Advisory
T +49 221 2073-1522
cjaekel@kpmg.com

Newsletter kostenlos abonnieren

www.kpmg.de/newsletter