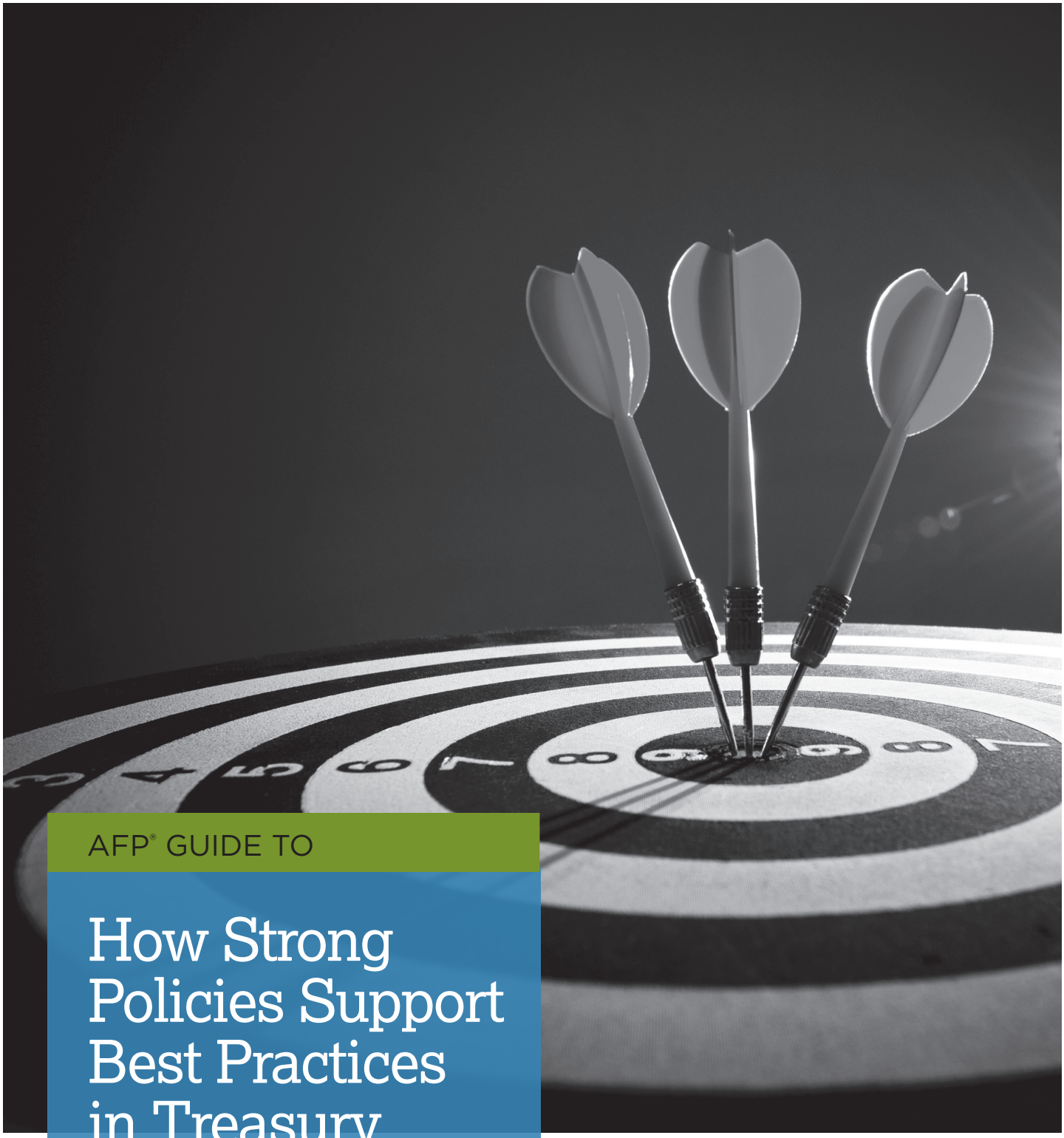
ASSOCIATION FOR FINANCIAL PROFESSIONALS



AFP® GUIDE TO

How Strong Policies Support Best Practices in Treasury

TREASURY IN PRACTICE SERIES

Underwritten by:

kyriba™

TREASURY IN PRACTICE SERIES

How Strong Policies Support Best Practices in Treasury

CONTENTS

AFP® GUIDE TO:
HOW STRONG POLICIES SUPPORT BEST PRACTICES IN TREASURY

TREASURY IN PRACTICE SERIES

Kyriba is excited to be a continued supporter of AFP's Treasury in Practice series, including the most recent publication, *How Strong Policies Support Best Practices in Treasury*.

Establishing effective treasury policies, while executing sound, consistent operational procedures is one of the most understated responsibilities that treasury teams have today. With the increasing threat of fraud and cybercrime alongside growing workloads and strategic responsibilities for treasury teams to balance, the need has never been higher to formally document what treasury should be accomplishing, what guidelines it should operate within, how exceptions should be managed, and how operational activities should be conducted.

Yet many treasurers report that treasury polices are an afterthought, sometimes documented over a decade ago without review to determine if outlined procedures are at all congruent with today's treasury realities. Further, with the majority of treasury teams relying on a combination of treasury systems and ERP platforms to manage daily operations, the opportunities for treasury technology to drive and enforce treasury procedures offer additional value, likely not seen when treasury policies were initially drafted.

This Treasury in Practice guide offers excellent tips to optimize the creation and update of treasury policies and procedures, including:

1) How to build effective treasury policies
2) Evolving treasury policies to align with new treasury realities
3) Leveraging treasury technology to enforce treasury procedures
4) Considerations when updating treasury policies and procedures to build resilience to new threats such as fraud and cybercrime
5) Templates and examples of documented policies and procedures.

Kyriba is a proud sponsor of the AFP Treasury in Practice series. We embrace our role to help CFOs and treasurers become better informed about how to maintain updated and effective treasury policies and procedures, including leveraging their technology to ensure consistency and standardization. Please enjoy this guide.

Best regards,

Bob Stark
Vice President, Strategy
Kyriba

1 INTRODUCTION

A treasury department is only as good as the policies and procedures it has in place. Whether they are formal, specific policies or just general guidelines, treasury needs to have a cohesive framework to execute on key strategies. Policies may differ greatly depending on company size, structure, location, and industry, but they are undoubtedly a key resource for treasury.

This Treasury in Practice Guide, underwritten by Kyriba, looks at how policies around cash management, payments and risk support best practices in treasury.

2 THE NEED FOR TREASURY POLICIES

In 2004, AFP released the *AFP Manual of Treasury Policies: Guidelines for Developing Effective Control*, in response to requests from members for sample policies they could adopt for their organizations. In its research, AFP ultimately found that many organizations lacked formal written policies, or had not updated their policies in years.

Since that time, as the corporate treasury function has risen in prominence within most organizations, formal policies have become much more prevalent, and are updated more frequently. Indeed, with recent advancements in technology, as well as rapidly escalating threats like data breaches and payments fraud, it is imperative that treasury policies need to be kept current. However, treasury departments must also take into consideration that policies need to be broad enough so that updating is limited to only major needs.

"You want to write your policies and guidelines to help protect the company and provide people with the basis of interpretation and how to handle situations—how to handle what to do and what not to do," said John Nielsen, treasurer for Henniges Automotive. "Given that we're in an environment now where technology is rapidly changing, the perspective that I would take is that when you write a policy, if you go into the nth detail, it can open you up to new risk."

Jennifer Dale, CTP, assistant treasurer for Sprint, noted that many companies of similar size to hers still don't have formal policies. But for perspective, having a policy is very helpful. "I don't think it's 100% necessary, but from a control perspective, it's nice to have that document to fall back on," she said. "If anything, you have no gray area when you have a policy."

3 ESTABLISHING AND WRITING POLICIES

Nielsen cautions against being too specific when creating policies because that can result in people looking for loopholes to work around certain standards. And again, with technology advancing, there could be big changes that are coming—though not necessary in all aspects of treasury. "For example, policies around payment systems are the types of policies that you should be looking at yearly," he said. "But maybe you don't have to look so much at your cash management policy or an overall treasury policy so often. Still, you should be at least looking through it and making sure that there's nothing in there that needs to be updated."

When crafting policies, one of the biggest challenges that treasury teams can face is trying to determine how much needs to be ironed out at the start. Many treasury organizations try to capture everything at the outset so that they don't have to frequently refresh their policies. The problem is that there's only so much you can predict about the future. "One of the hardest things that people have in writing policies is you think, 'Well, okay, if I write this policy now, what happens when we get a better handle on Same Day ACH? Should I start to write some stuff in there now? No… I'm just going to wait another two months to do this until I find out a little more,'" Nielsen said.

All too often, however, that day never comes because treasury practitioners either get busy with other tasks or don't want to acknowledge that policies may need to change over time. "I think that is part of the problem; people get scared of just moving forward and putting a marker in the sand and saying, 'You know what? I'm okay with having to update and refresh my policies,'" Nielsen said.

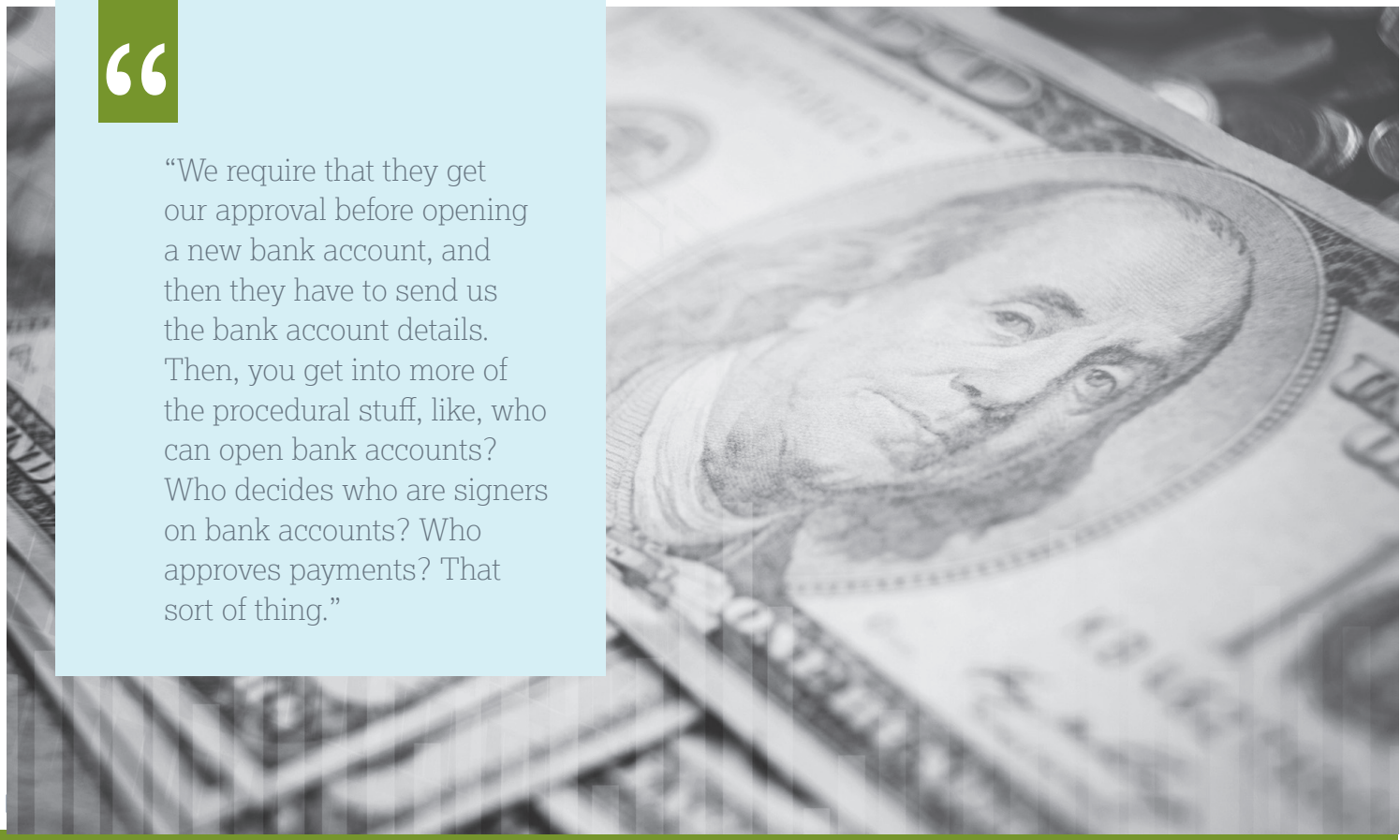
Establishing policies also depends largely on support from senior leadership and how the delegation of authority works within the organization. For example, at Henniges, both Nielsen and the corporate controller are responsible for a number of the policies, because they revolve around the controls of the organization. He noted that if both parties agree to a policy change, the CFO is highly likely to sign off on it. "If we get together and we're fine with things, the CFO will perceive it as, 'Go ahead; get it rewritten and put it out on our intranet. Send a message out to the people that need to know and say that we've got an updated policy, and here's the section that has changed,'" he said.

In contrast, some treasury organizations must go to the board of directors every time they make policy changes. Needing that kind of constant approval can be quite onerous. "And really, your board of directors isn't supposed to be your operational know-it-all," Nielsen said. "They're supposed to be strategic. Maybe it's appropriate for certain treasury policies like foreign exchange or risk hedging, because then you're dealing with the strategic direction of the company. But a lot of your other policies shouldn't have to go all the way to the board for approval."

4 COMMUNICATING POLICIES

Communicating your policy to your staff can also be a challenge. Unless you are part of a large, multinational company, treasury is generally a skeleton crew, and it may be difficult to build out time to talk to your team members about your policies. “We’re a $5 billion company, but I just literally have five people doing different things, including capital markets activity,” said Jim Gilligan, CTP, FP&A, assistant treasurer for Evergy Inc. “So it’s a challenge to find time to sit down and talk with people.”

However, communicating these policies is a necessity when you bring new people on board, because you need them to understand how treasury does things, and why. “You can’t just bring somebody in and expect them to know everything in a relatively short period of time,” Gilligan added. “This is a complicated world that we live in, and understanding treasury’s role is overwhelming for a lot of people, especially if they get turned over in a position quickly.”



> "We require that they get our approval before opening a new bank account, and then they have to send us the bank account details. Then, you get into more of the procedural stuff, like, who can open bank accounts? Who decides who are signers on bank accounts? Who approves payments? That sort of thing."

CASH MANAGEMENT AND PAYMENTS

Policies around cash management and payments can differ from company to company, depending on the structure and size of the organization. According to the *AFP Manual of Treasury Policies,* a formal policy should communicate treasury's objectives to the company and establish linkages between cash management practices and the company's overall business management objectives. It should define the roles, responsibilities and cross-functional relationships of various departments involved in cash activities and promote consistent, uniform practices throughout the organization.

For cash collection specifically, relationships with other departments is especially important; it can be influenced by factors outside of traditional treasury. Input is often needed from sales and marketing, billing and accounts receivable. Treasury must have input into policies and practices that "touch" the cash collection and concentration process but are not actually under treasury's control. The manual thus recommends appointing a "champion" to oversee the policy development process; this is typically the treasurer, assistant treasurer, cash manager or an appointed committee.

For Bob Whitaker, CTP, senior vice president of corporate finance for DHL and chairman of AFP's Board of Directors, policies around cash management are fairly high level. DHL has operations in many countries, so its policies are mainly around which banks the company's local operations should use. In most cases, they should be working with global banks in DHL's bank group, as opposed to smaller local banks.

Treasury's role then is essentially governance over the company's operations in a whole host of countries, because it is not actually executing the local work, except the United States. Whitaker noted that cash management policies for those local operations can get pretty granular. "We require that they get our approval before opening a new bank account, and then they have to send us the bank account details," he said. "Then, you get into more of the procedural stuff, like, who can open bank accounts? Who decides who are signers on bank accounts? Who approves payments? That sort of thing."

When it comes to excess cash, many organizations use key performance indicators (KPIs) to measure the effectiveness of policies around the amount of total

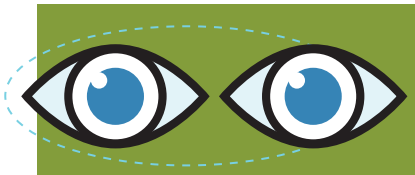
cash used for working capital. For example, the policy may be to use no more than 10%, and the KPI would reward treasury for getting below this number. Furthermore, a policy may specify what is an acceptable level of idle cash in accounts, perhaps distinguishing between remotely managed accounts by regional controllers, compared to operating accounts that treasury controls.

"We see many clients have policies around how to invest excess cash, with certain investment instruments or categories of instruments permitted," said Bob Stark, vice president of strategy for Kyriba. "Some industries, such as insurance, will also document how to invest operational cash differently than nonoperational cash, which can be provided to in-house investing teams to achieve a higher return on cash. A policy may state that treasury must have visibility and control of all corporate bank accounts, with approval rights on all openings and closings."

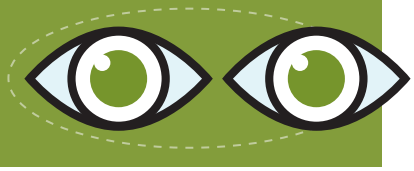
When it comes to payments, the goal of treasury policies are specifically focused on protecting against fraud. For a huge company like DHL, that means keeping a database of all its bank accounts around the world. "The goal is to prevent someone from stealing your money," Whitaker said. "So it's just really trying to put in all the controls you can."

As fraud threats have continued to escalate, CFOs and CIOs have begun to direct treasury to not only digitize payment policies, but also ensure their payment systems are setup to enforce those policies. Examples include real-time screening for duplicate payments, whether the right individuals have approved high dollar payments, or holding payments with modified delivery instructions for another level of validation.

DHL's guidelines include applying the four-eyes principle. This is essential with the epidemic of business email compromise (BEC) scams that has plagued treasury departments in recent years. Additionally, treasury at DHL doesn't allow anyone to direct debit its accounts, with a few notable exceptions. "Basically we try and secure our accounts, so we put debit blocks on them and positive pay," Whitaker said.



FOUR-EYES PRINCIPLE: A requirement that at least two individuals review an activity before an action is taken. The four-eyes principle is typically applied to payments to protect against fraudulent transactions.



> "We make sure that we impress upon our colleagues that you just can't take wire instructions over the phone."

John Dourdis, CTP, vice president and treasurer for Conair, agreed about the importance of having strong polices, particularly around wire payments. "We make sure that we impress upon our colleagues that, you just can't take wire instructions over the phone," he said.

He added that these policies need to be cross-departmental so that everyone is in lockstep with one another. "Those particular departments should have their own policies and procedures, but we certainly support that," he said. "Safeguarding the company's money is obviously an important role."

There are some policies where treasury will need to consult with the legal group, like determining how long to keep checks on hand, noted Tom Hunt, CTP, AFP's director of treasury services. "It's always good to consult internally with legal on policies that may have an impact on future operations that have a statute of limitations component," he said.

Another newer issue for treasury is that payment processing has transitioned to the customer service function at many organizations. This is a major challenge for a large biller like Evergy that has more than 1 million customers. "We get a lot of payments, and that processing of payments can be outsourced, or it can be done internally," Gilligan said. "But whether it's done internally or whether it's outsourced, you have exception processing, and that function is typically being done now by customer service people, who don't have a background in treasury or payments."

As more companies transition to this type of a model for payments, it will become imperative for them to work cross-functionally with customer service and make sure that they understand treasury policies around exceptions.

With the rise in fraud, Nielsen recommends reviewing policies around accounts receivable (AR) and accounts payable (AP) more frequently than standard treasury policies. Those policies, particularly ones for AP, should be reviewed at least once a year. "The head of that department should be reviewing policies on an annual basis and saying, 'Is everything in here still relevant? Are we missing things that we should be adding to this?' AP needs to be reviewed from a payment standpoint because fraud is rampant now," he said. Additionally, the internal audit group can also help to ensure that policies are enforced by each department.

Again, attending conference sessions can help treasury teams learn best practices. Webinars around fraud, like those hosted by AFP, Kyriba and others, can also be helpful. "Just about every webinar nowadays has to do with some sort of fraud and the changes to it," Nielsen added. "People are taking those learnings and going back and saying, 'You know what? These are great points. How do I update my policy in order to help protect against some of these new fraud techniques?'"

When it comes to fraud, it may be necessary to be very detailed; you may find that you need to establish policies around very specific threats. For example, while most treasury teams are aware of the telltale signs of the "CEO fraud" version of BEC scams, many large organizations are still being fooled by fraudsters impersonating routine vendors who send bogus payment instructions. If an organization has a policy in place that does not allow changes to vendor master data unless those changes are verified by a public source, the threat is more or less neutralized.

"When someone in our organization gets a request from a vendor that says 'Hey, we've changed banks and we are now using x. Please update your records,' we send that immediately off to purchasing, and purchasing is responsible then for actually Googling the company's main phone number," Nielsen said. "They call their corporate office and say, 'Can I speak to someone in treasury or accounts receivable in that organization?' When they reach that person in there, they ask, 'Have you guys updated your banking information recently?'"

"I think you can take controls to an unnecessary level that just drives unnecessary work. You have the proper controls—the ones that are really going to stop errors from occurring or stop fraud from happening—those are the ones that should be SOX controls. It's not just every single step of the process."

SOX COMPLIANCE

Treasury departments need to take care to implement policies around fraud, to stay in compliance with the Sarbanes-Oxley Act (SOX). Embedded within SOX processes are certain cash management requirements, noted Gilligan. "There's a SOX control that says that in order to do a wire, we must have two approvals, and it is written in conjunction with our software that we use from our cash management banks to validate that," he said.

As previously noted, with the constantly evolving threat of fraud, as well as advancements in technology like Same Day ACH and real-time payments, policies around cash management and payments may require more frequent updates. Evergy's treasury department hasn't found itself making constant changes to its policies, but it does review its policies every time it certifies its SOX controls. "We go through a review process to make sure that those controls adequately are described, and if they do not adequately describe it, because there is a change in process or technology, then we have another process where we have to go through our internal audit department to flag it, basically."

But in some cases, advancements in technology don't really come into play. For example, there is a SOX requirement that a company has a control in place to send a file to a bank, and that it gets a response back from the bank that the file was received. But whether the payment is made via Same Day ACH or standard ACH wouldn't matter. For Evergy, it would come down to internal treasury policies on whether something like Same Day ACH would be used. "We may say that our process is that we're not going to do Same Day ACH because it's not cost-effective unless it is in place of a wire," Gilligan said.

SOX compliance can be challenging, but it doesn't have to be. Some treasury departments may find compliance onerous if they are attempting to build controls around everything, but Sprint has been able to determine which areas need to be heavily scrutinized as it prepares for audits, and which ones don't.

Dale recommends actively reviewing controls to make sure that you aren't doing needless work. "I think you can take controls to an unnecessary level that just drives unnecessary work," she said. "If you have the proper controls—the ones that are really going to stop errors from occurring or stop fraud from happening—those are the ones that should be SOX controls. It's not just every single step of the process."

Dale's treasury organization actively works with its internal audit group, which oversees SOX controls, to make sure that they are in compliance but also aren't going overboard. They have changed certain controls over the years and in some cases, successfully negotiated out of other ones. "We've just been able to have the discussion with them that certain controls don't seem relevant, or seem to be too cumbersome to the group and are just not necessary," she said.

Private companies are not typically required to have policies at SOX compliance levels. Nevertheless, when you have auditors come in to review your financials, they want to know that you have good policies and procedures in place.

In Henniges' case, the company is private but aspires to go public at some point. Therefore, Nielsen is aiming to ensure that the company's policies are up to speed so that there is a smooth transition when that day comes. "I looked at these policies and procedures that we had here in the treasury department, and the policies are a solid backbone that tells you what you can and can't do," he said. "But in some cases, these policies are a little out of date."

Over the past year, Nielsen has been rewriting a number of policies within the company to make sure they are current. Many of the ones he has gone through are guidelines around treasury as a whole. He favors the term "guidelines" over "policies," because he feels they should be used to provide guidance towards what treasury is expected to do. "The reason why I like the word guideline over policy is because you can write a policy the best that you can, but some way, somehow, somebody's going to need to break that rule," he said. "Someone can come along and when you write a policy, a lot of times your auditors say, 'Well that doesn't follow your policy, so what's your mitigation?'"

At the end of each guideline, Nielsen includes an interpretation section, which names the individual that is responsible in case there's any question regarding the interpretation of policy itself. Additionally, the guideline specifies that any deviations from it need to have documented approval from the treasurer, and those deviations should be reviewed and reapproved annually. In this way, treasury at Henniges has protocols in place but they are not so strict that they don't allow for any exceptions.

Since DHL is a German company that is not publicly traded in the U.S., it doesn't have to worry about SOX compliance. However, it does have to comply with European regulations, as well as its own internal control structure. "We've given it a lot more attention in the last few years," Whitaker said. "We have autonomous divisions within the group, and we even have different accounting systems across divisions, so it becomes very difficult. But we've been really working on putting very strong internal control structures everywhere, including providing evidence that those controls are in place. So we do have a control framework and I'm sure it meets whatever the SOX requirements would be."

6 RISK MANAGEMENT

If there is one area where a policy is necessary, it probably risk management. Having formal policies for risk sets parameters around a company's exposures. The policy should outline treasury's role, as well as the responsibilities of senior management and other departments.

CYBERRISK MANAGEMENT

The *2019 AFP Cyberrisk Survey* found that 88% of organizations were targeted by attempted or actual cyberattacks between May 2018 and October 2019. While organizations across the board are adopting cybersecurity safeguards and implementing robust training programs, the survey results indicate that those committing the attacks are not discouraged by these protections.

Kyriba has observed much greater attention being paid by CFOs on policies around cyber over the past five years, which has coincided with the dramatic rise in the complexity of cyberattacks. As such, it's important to be specific in your procedures. "Many organizations have suffered from writing policies that lack sufficient detail about how to manage exceptional situations, such as management requiring one-off payments," Stark said. "In many payments fraud examples, it wasn't necessarily someone inside the organization not following policy; it's that the policy was too vague to be effective."

To be more precise, payments policy should dictate how to manage typical payment scenarios as well as unexpected scenarios such as the "real" CEO actually needing an emergency wire to be sent. The policy needs to also cover the exceptions to be effective.

For example, going back to payments fraud, does your CEO actually have the authority to email the treasurer and say, "I need a wire today. You actually can't tell people about it, because it is secret around a real acquisition." You might have a policy in place that says that treasury can't just wire the money, but does the CEO understand that? And does your staff have the confidence that you will back them up if they say no to the CEO when he tries to break the policy? These are the questions that need to be asked answered. "The policy should be that you have to follow it, every time," Stark said. "So it's that sort of thing that organizations will differ, but they used to be fairly vague around this or be silent on it."

Stark advises companies to digitalize their procedures wherever possible. "CFOs and Treasurers are asking for technology that helps enforce their controls, so they have confidence that cash, payments or bank account management procedures are following policy," he said. "Treasury and payments software can ensure the policy is being followed."

For example, again, your organization may apply the four-eyes principle as a policy. But that might not be specific enough, because who are the four eyes? More than two people will probably see the payment, so which two are the ones that count? You may need to delineate to a detailed level especially when the CFO or the treasurer need to be directly involved with a payment. "A payments policy should be scenario-driven, so that certain payments require 'four eyes,' while other scenarios require six or eight eyes," Stark said.

Some treasury policies require investing in cyber insurance, which in turn can help assess the overall threat level. "Insurance companies will conduct a thorough analysis of your systems to give you a good understanding of your risk as part of their premium determination," Hunt said.

“Corporate policy should determine how exposures are identified and how risk is to be managed. If a company chooses not to hedge their balance sheet exposures, for example, procedures should still be in place for situations like Brexit. A silent policy on currency risk scenarios can have significant impacts on earnings per share.”

FX RISK MANAGEMENT

For FX risk, the AFP Manual of Treasury Policies notes that a policy should establish key principles that will guide treasury in the company-wide communication and implementation of risk management activities. The policy should be split into two parts. The first section defines the importance of having an FX risk management strategy, recommends a policy development and approval process, provides guidance around monitoring compliance, and considers ways to manage exceptions. The second half identifies risk exposure and measurement, and comes up with hedging strategies and reporting guidelines.

Treasury should develop the policy, though it will require oversight and review from senior leadership, and input from other departments like tax, internal audit and accounting. The CFO should approve the policy; at some smaller organizations, this may be the final level of approval. Larger organizations may have a risk management committee and/or board of directors that provides the final approval.

According to the manual, a good policy should:

- Provide clear guidance and communication on the definition of risk
- Ensure linkage to the company’s overall business objectives
- Reduce the potential for miscommunication and errors in managing the FX program
- Ensure that the organization’s risk management objectives are met, and the hedging strategy is well-executed.

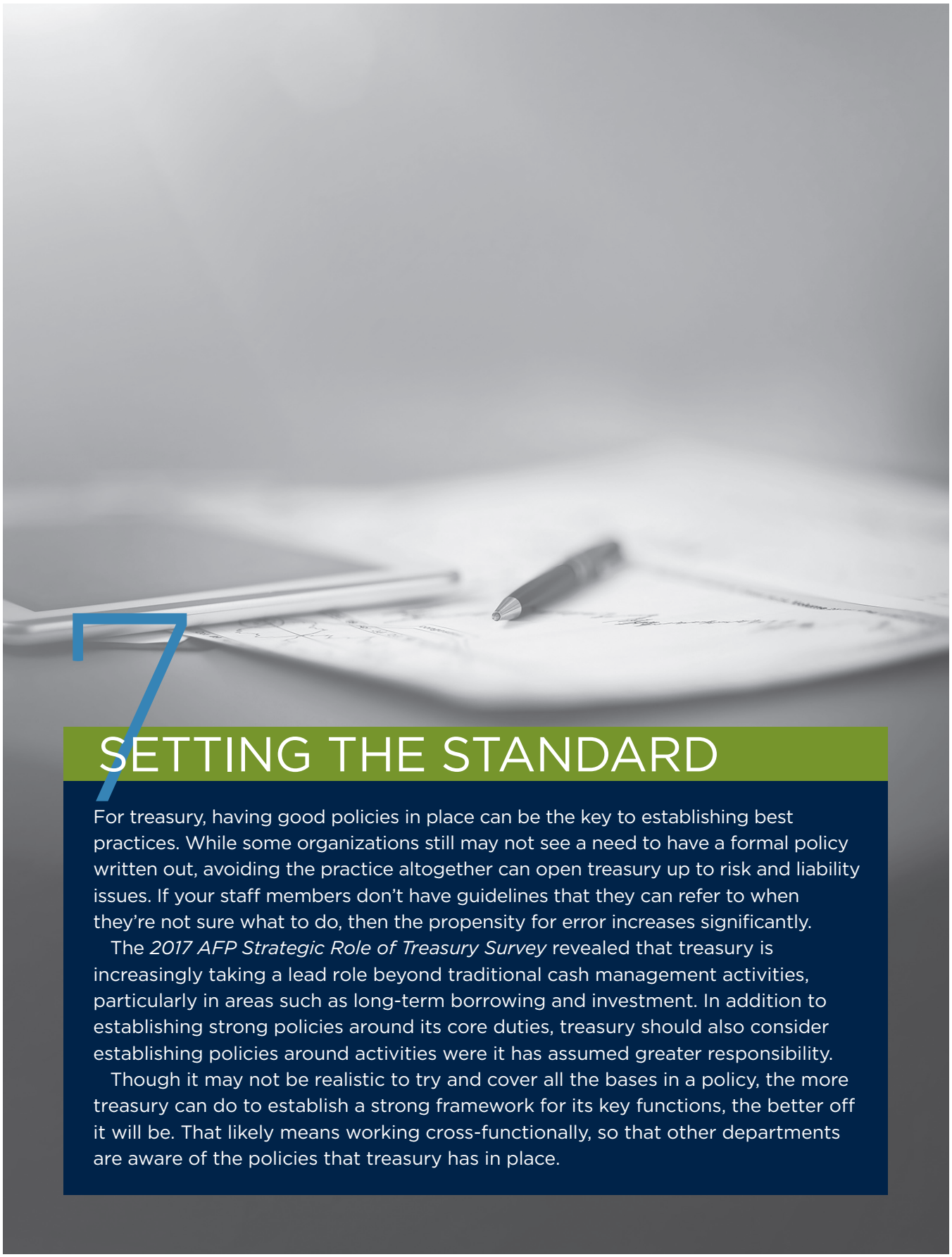
Just like payments fraud risk management, handling FX risk requires a lot of oversight. DHL has a policy that requires subsidiaries to hedge if there is a high amount of balance sheet risk. “And then you’re required to hedge with a parent, if it’s legally allowed,” Whitaker said. “If it’s not legally allowed, in a country such as Brazil, then you need our approval to set up a hedging program. Because when you get into hedge instruments, there are a lot of risks and you don’t want people off doing their own thing.”

Mitigating risk at a company the size of DHL is incredibly difficult; it isn’t really feasible to create a blanket policy for subsidiaries in 200 countries. But the treasury department’s overall rule is to restrict anything that is considered high risk. “You have to come to us to pick an open bank session, you have to come to us if you want to borrow money, and you have to come to us to do hedges,” Whitaker said.

At Conair, the purpose of its FX hedging framework is all around ensuring that the company is protective in nature. If there is anything unusual, treasury works cross-departmentally to keep everyone in the loop. “We go to accounting and say, ‘Hey guys, this is what we’re doing. We don’t see any issue here. Do you see any issue with we’re going to do?’ So that just helps everybody know that what we’re doing,” Dourdis said. “That way, there are no surprises, and people are aware of any financial swings of the currency. So part of our procedure is to ensure that we bring in our colleagues in our cross-departmental groups.”

Many FX policies are even more complex, as they often need to specify when exposures should be hedged, as well as when and how the treasury team should pursue organic reduction of net exposures. When an organization decides to hedge, it may have different policies for balance sheet hedges, which often settle within the quarter to avoid derivative and hedge accounting, and cash flow hedges, which are typically longer duration. Furthermore, an effective policy may also limit certain durations (e.g., not more than six months) with different percentages at different timing intervals—one month, three months, six months, etc. Finally, many FX policies need to be clear about what instruments are to be used. Many organizations only use forward contracts, while others will allow plain vanilla options or even more complex option strategies.

But it’s not a given that every organization hedges. Some of the largest companies in the world do not hedge, instead choosing to organically reduce net currency exposures. “Corporate policy should determine how exposures are identified and how risk is to be managed,” Stark said. “If a company chooses not to hedge their balance sheet exposures, for example, procedures should still be in place for situations like Brexit. A silent policy on currency risk scenarios can have significant impacts on earnings per share.”



7

SETTING THE STANDARD

For treasury, having good policies in place can be the key to establishing best practices. While some organizations still may not see a need to have a formal policy written out, avoiding the practice altogether can open treasury up to risk and liability issues. If your staff members don't have guidelines that they can refer to when they're not sure what to do, then the propensity for error increases significantly.

The *2017 AFP Strategic Role of Treasury Survey* revealed that treasury is increasingly taking a lead role beyond traditional cash management activities, particularly in areas such as long-term borrowing and investment. In addition to establishing strong policies around its core duties, treasury should also consider establishing policies around activities were it has assumed greater responsibility.

Though it may not be realistic to try and cover all the bases in a policy, the more treasury can do to establish a strong framework for its key functions, the better off it will be. That likely means working cross-functionally, so that other departments are aware of the policies that treasury has in place.

SAMPLE POLICIES

The following examples were submitted by a corporate practitioner to give readers an idea of what the structure of a policy could look like. The first part is a financial policy manual, which acts an overall guide to policies and procedures. The second part is a detailed policy for remote deposit capture.

SUBJECT: Financial Policies

APPROVED BY:

TITLE:

EFFECTIVE DATE:

REVISED DATE:

SECTION: Governance

SUBSECTION:

OVERVIEW

The purpose of this Financial Policy Manual is to standardize controls, processes, and accountabilities to ensure the assets of the Company are safeguarded and financial reports are prepared in accordance with Generally Accepted Accounting Principles [GAAP] and regulations of the Securities and Exchange Commission [SEC].

Each policy includes an OVERVIEW, POLICY, and PROCEDURE section.

- The OVERVIEW contains a brief description of the objective of the policy and other necessary information.
- The POLICY communicates expectations for financial governance, accounting and reporting. The scope of the Policy is the company and all business units/entities.
- The PROCEDURE sets specific direction/instruction for the application and execution of the policy. The scope of the procedure includes the Company and all business units/entities unless specific procedures are noted for separate entities.

POLICY

A Financial Policy establishes principles and guidelines for conducting business activities.

PROCEDURE

A new or revised Financial Policy Draft will be submitted to the Senior Manager, Process Design and Documentation. The draft will be sent to the Financial Policy Committee for review and comment with a five-day turnaround request.

The Financial Policy Review Committee includes the following positions:

- Chief Financial Officer
- Chief Accounting Officer
- Vice President, Tax
- Vice President, Internal Audit
- Vice President, Commercial & Ops
- Vice President, Global Shared Services
- Directors Finance: U.S., Americas, and Asia
- Controllers: U.S., Americas, and Asia
- Treasurer
- Senior Director, Global Supply Chain
- Senior Manager, Process Design and Documentation

The Financial Policy approval rests with the CFO and CAO.

Any request for discussion will be subject to approval by the Chief Accounting Officer, who will determine if a meeting is necessary. Following circulation, review and approval, the new policy will be posted on the Financial Policy Manual site.

Critical policies [those determined to be of top priority] will be reviewed and updated annually. All other policies will be reviewed biannually.

REMOTE CHECK DEPOSIT SCANNING POLICY/PROCEDURE

OVERVIEW

In order to electronically deposit checks, our banks offer a scanning and e-deposit tool.

Checks are scanned, electronically endorsed and deposited into our bank account. The scanned check must be retained for 75 days in a secure location in case it is needed for research and/or verification. After 75 days, checks must be destroyed. Check destruction must be done under a dual control environment and both witnesses must sign a destruction control sheet.

PROCEDURE OVERVIEW

Day 1:

- Scan checks
- Transmit scanned checks
- Retain scanned checks in locked cabinet
- Organize scanned checks by date

Day 2:

- Verify electronic deposit using Bank Remote Check web tool

Day 75:

- Determine all checks that may be destroyed
- Prepare Check Destruction Report
- Using Bank Remote Check web tool, print check report for all checks deposited 75 days or greater
- Under dual control, locate all checks eligible for destruction, and shred
- Both shredder and witness must sign check destruction report
- Retain report for audit control purposes

DETAILED PROCEDURE

Day 1:

1. Prepare for check scanning
   - 1.1. For deposit control purposes, total the number of checks to be scanned and the total dollar amount of the checks.
   - 1.2. Log onto the Bank Remote Check Deposit website.
   - 1.3. From the Home page, click "Checks and Deposits" button, and then click the "Check Scan" button.
   - 1.4. Enter the total number of checks and the total dollar amount of the checks.
   - 1.5. Enter a deposit description to aid in identifying deposit activity.
   - 1.6. Click Start Scan to scan checks for electronic deposit.

2. Review Deposit
   - 2.1. Ensure all checks scan properly.
   - 2.2. If a repair is needed, the item will be identified and the status will reflect the rejection. Checks may need to be repaired for missing dollar amount, missing or incorrect MICR information.

3. Repair Checks/Rescan Checks
   - 3.1. Checks that are missing dollar amounts can be easily corrected within the deposit process. Key the amount and complete the deposit.
   - 3.2. Checks with missing or incorrect MICR information may be rescanned. Delete the image and rescan to complete the deposit. (If after three scanning attempts, the check image fails to be captured, manually repair the MICR line. See below.)

4. Image Quality
   - 4.1. The image failed on three scanning attempts. You may repair the MICR line if you can clearly see this information and if you have sufficient permissions to do so in the web tool.

5. Save Deposit
   - 5.1. The deposit is balanced based on the total number of checks and the total amount of the all the checks in the deposit.
   - 5.2. Once the deposit is balanced, it will be created and saved. The deposit will then appear in the Pending Items section.

6. Pending Items
   - 6.1. Click the Pending Items button to view all deposits eligible for approval.
   - 6.2. Next, click the check box next to the deposit and click "Approve".
   - 6.3. Finally, click the check box next to the deposit and click "Submit" to transmit the deposit to the bank. Transmit checks are endorsed with electronic deposit information and deposit date.

7. Reporting

8. Check Destruction

ABOUT THE AUTHOR

Andrew Deichler is the multimedia content manager for the Association for Financial Professionals (AFP). He produces content for a number of media outlets, including AFP Exchange, Inside Treasury, and Treasury & Finance Week. Deichler regularly reports on a variety of complex topics, including payments fraud, emerging technologies and financial regulation.

ASSOCIATION FOR FINANCIAL PROFESSIONALS

ABOUT AFP®

Headquartered outside of Washington, D.C. and located regionally in Singapore, the Association for Financial Professionals (AFP) is the professional society committed to advancing the success of treasury and finance members and their organizations. AFP established and administers the Certified Treasury Professional and Certified Corporate FP&A Professional credentials, which set standards of excellence in treasury and finance. Each year, AFP hosts the largest networking conference worldwide for more than 7,000 corporate financial professionals.

4520 East-West Highway, Suite 800
Bethesda, MD 20814
T: +1 301.907.2862 | F: +1 301.907.2864

www.AFPonline.org