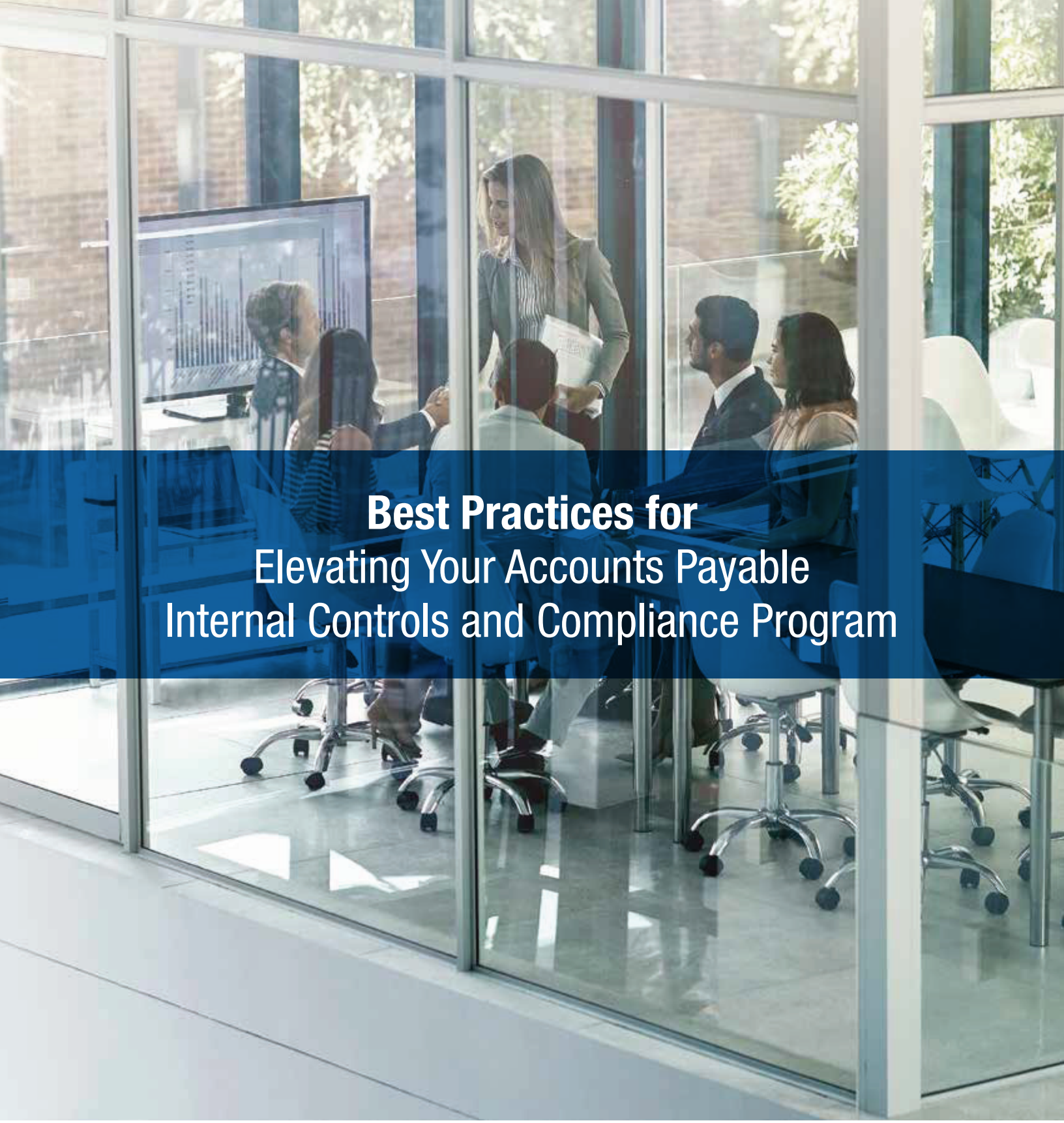

Best Practices for
Elevating Your Accounts Payable Internal Controls and Compliance Program

An AP & P2P white paper

ACCOUNTS PAYABLE & PROCURE-TO-PAY
APP2PNetwork
Payables • P2P • Shared Services

Sponsored by

Tipalti

TABLE OF CONTENTS

Introduction

The AP Department plays a critical role within an organization. As a governing entity in the supplier sourcing process, it ensures that each supplier is properly screened prior to onboarding, thereby protecting the company from risk due to fraud, fines, audits, and investigations. Once a supplier relationship is established, the AP Department continues to protect the company's financial interests by ensuring timely invoice processing, verifying that payments are made according to agreed-upon terms, and providing a high level of customer service.

Last but not least, accounts payable also serves as the last point of control before a payment is sent to a supplier. Once money is sent to a supplier, your chances of retrieving these funds at a later date due to an unintended data entry error or due to fraud by an employee or supplier are extremely low. The right approval workflows, signatory rights, and processes must be proactively established to minimize the likelihood of this occurring.

AP also supports the integrity of the supplier master file within the Procure to Pay (P2P) process and the integrity of the financial transaction through the financial close or the Record to Report (R2R) process. Error-prone and delayed payment reconciliation processes raise red flags that can lead to financial reporting errors and audits.

Given their crucial role in the business, accounts payable processes are subject to compliance requirements and internal controls that can be complicated and overwhelming. Companies that operationalize best practices into their AP processes and monitor them with internal control systems can manage the complexity, prevent transactional or closing problems, and consistently maintain the integrity of their corporate transactions.

This whitepaper will put you on a path to establish a best-in-class compliance and internal controls program for your AP Department. It includes requirements and recommended best practices, along with roles and responsibilities for their implementation.

What are the Roles of the CFO and Controller?

The CFO and Controller play four vital roles in establishing a compliance and internal controls program. They are:

Stewards: CFOs and Controllers protect and preserve the assets of the organization by establishing strong controls, complying with regulations, and preventing risks.

Operators: They balance capabilities, costs, and service levels to fulfill the finance organization's responsibilities in a controlled environment.

Strategists: They provide financial leadership in determining strategic business direction and align financial strategies with minimal risk.

Catalysts: They stimulate behaviors across the organization to achieve strategic and financial objectives with strong controls.

Who is Responsible for Financial Compliance and Internal Controls?

A company's emphasis on internal financial control and compliance starts with its "tone at the top," the ethical atmosphere that is created in the workplace by the organization's leadership. The tone set by management has a trickle-down effect on both the employees and suppliers of the company. If managers emphasize ethics and integrity, employees and suppliers will be more inclined to uphold the same values.

The Best Practice (1 of 7):
Integrate ethics and compliance requirements into all business processes to ensure that the "tone at the top" is embedded throughout the organization. Specifically as it relates to accounts payable financial controls, fraud prevention, and tax and regulatory compliance, the office of the CFO is responsible for establishing these guardrails and expectations for that function. This approach establishes a corporate environment of internal controls and compliance that extends to the accounts payable organization, including supplier management. These initiatives typically include the deployment of ethical standards or a code of conduct for the organization. This is also a requirement for Sarbanes Oxley 404.

Who is Responsible: Financial Executive Staff and Ethics Officer for implementation and all Company Employees for adherence.

The Three Critical Corporate Controls to Achieve Best-in-Class AP Compliance

There are three critical corporate controls (a.k.a. "core controls"):

1. Segregation of Duties (SoD)
2. Systems Access (SA)
3. Delegation of Authority (DoA)

The Segregation of Duties (SoD)

The Segregation of Duties (SoD) control is one of the most important controls that your company can have. Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing for separate processing by different individuals at various stages of a transaction and for independent reviews of the work performed.

The SoD control provides four primary benefits:

1. the risk of a deliberate fraud is mitigated as the collusion of two or more persons would be required in order to circumvent controls
2. the risk of legitimate errors is mitigated as the likelihood of detection is increased
3. the cost of corrective actions is mitigated as errors are generally detected relatively earlier in their lifecycle
4. the organization's reputation for integrity and quality is enhanced through a system of checks and balances.

Although SoD is a basic key internal control, its often one of the most difficult to accomplish due to limited headcount, broadly defined responsibilities, and constantly changing responsibilities. Basically, the general duties to be segregated are: planning/initiation, authorization, custody of assets, and recording or reporting of transactions.

Additionally, control tasks such as review, audit, and reconcile should not be performed by the same individual responsible for recording or reporting the transaction.

Best Practice (2 of 7):
One of the most common "root causes" of fraud is the lack of SoD controls, weak SoD controls, inappropriate compensating controls, or failure to update SoD controls when responsibilities change. As a best practice, many organizations review their SoD controls on a quarterly basis as part of their control self-assessment (CSA) process. As a result of this review, the applicable SoD controls are updated appropriately.

Systems Access

Systems automation can play a crucial role in establishing, simplifying, and monitoring all three of the core controls, particularly role-based system access and activity logging. Many companies experience lapses in control due to their reliance on manual processes, or experience vulnerabilities in the transfer of data from one system to another. Human beings make mistakes, but a system of checks and balances can mitigate the risk of fraud or mismanagement.

The Best Practice (3 of 7):
Employ systems that provide flexibility and discrete configuration of controls around system access and critical accounts payable paths. Specifically, certain employees should have full ability to effect AP transactions, approval rights, and access to information, while some may only be able to affect certain processes, have "read only" visibility or only limited visibility. On a related note, account funding for supplier payments should have limited access and clear roles. This reduces the need to manually monitor every transaction.

Who is Responsible: Controller and Accounts Payable

Delegation of Authority

In an automated Delegation of Authority (DoA) process, supplier onboarding, invoice and payments approval are all linked to the company's DoA Policy and the employee Master file and is automated based on defined workflow rules. The workflow determines: (1) if a supplier / invoice / payment needs approval; (2) who the appropriate approvers are, and; (3) in what order payments should be approved according to established company rules. The workflow will then sequentially ask each approver via a generated email to electronically approve invoices and also payments. (For example, you can define a rule so that invoices over a certain threshold require CFO approval and then CEO approval.)

The Best Practice (4 of 7):
Leading-practice companies link the DoA policy to the job levels within the employee master file. They then establish a DoA table to drive the approval workflow. If an approver moves to a different position or department or leaves the company, the approval tables are automatically updated.

Who is Responsible: Controller, Accounts Payable, and Procurement

The Supplier Onboarding Process

Supplier Data Collection

The supplier onboarding process involves validating the supplier and ensuring that there are no financial or compliance risks before adding them to the master file. This process requires appropriate and continuously enforced segregation of duties. Not enforcing a proper supplier data validation process exposes your company to potential fraud, supplier payment error fees and delays, tax compliance issues, and other regulatory problems. If your company pays suppliers outside of the US, the rules and requirements for data validation increase dramatically with thousands of different variations to check up against.

Ownership of the process usually resides in the accounts payable organization; however, some companies split the overall responsibility between the procurement and accounts payable departments.

In such cases, procurement may set up the supplier, but accounts payable is responsible for any changes made to the supplier master file. In most cases, accounts payable owns supplier payment and tax information collection and validation.

Lastly, many large Fortune 100 companies have established Shared Services Centers wherein the finance team takes responsibility for all master files, including the supplier master, the material master, and the customer master. This is an excellent way to avoid any potential segregation of duties issues.

The Best Practice (5 of 7):

- Validate supplier contact information, payment data, and tax information prior to supplier approval. This process should take into account the different requirements per each payment method and payee country.
- Employ TIN matching to ensure verification of supplied vendor data. TIN matching is a pre-filing service only offered to payers and/or their authorized agents who submit any of six information returns (Forms 1099-B, 1099-K, INT, DIV, OID, PATR, or MISC). It enables validation of TIN and name combinations prior to submission of the information return.
- Obtain a W-9 form for domestic suppliers, a W-8 form for foreign suppliers, and perform TIN matching prior to vendor setup and payment processing.

Who is Responsible: Accounts Payable (and sometimes procurement)

FATCA Tax Compliance

The Foreign Account Tax Compliance Act (FATCA) established a new regime under Chapter 4 of the Internal Revenue Code for documentation of foreign entity payees and withholding from payments in the absence of certain documentation. These requirements are in addition to the documentation, withholding and reporting required under Chapter 3 of the Code. FATCA compliance will be phased in, starting in 2013.

Some FATCA requirements will affect payers that make the types of payments reportable on Form 1099-MISC and Form 1042-S. Payers will need to update their procedures to ensure compliance with both sets of documentation and withholding requirements: the new rules for FATCA, and the previously existing rules for withholding at source on certain payments to nonresident alien individuals, foreign corporations and other foreign entities.

The IRS is employing the new FATCA requirements to ensure they collect all appropriate tax funds from payers and payees and, to ensure success of this program, have reportedly hired and training large teams of IRS agents to enforce compliance.

Payers / accounts payable teams are the primary party held responsible for non-compliance. Payers not properly collecting documentation identifying "US accounts" from overseas accounts will suffer a 30 percent withholding tax on all US withholdable payments. (Source: **www.kpmg.com/BB/en/IssuesAndInsights/ArticlesPublications/Documents/fatca-and-the-funds-industry-defining-the-path.pdf**)

The Best Practice (6 of 7):

- Collect and store tax forms prior to supplier onboarding
- Screen tax forms and tax data provided to ensure proper payee tax classification (US account or non-US account)
- Withhold necessary taxes prior to sending payment to supplier with non-US account classification
- Apply tax status and withholding rules into annual 1042-S tax reporting

Who is Responsible: Accounts Payable

Regulatory Compliance

Compliance requirements are complex, ever changing, and vary by industry and process. (Please reference Addendum 2 for a Comprehensive Compliance Guide). For these reasons, the initial screening of your supplier master file records should include validation with:

- OFAC: Office of Foreign Asset Control
- BIS: Bureau of Industry and Security
- SDNs: Specially Designated Nationals are considered enemies of the United States. They can be either organizations or individuals who are involved in drug trafficking, terrorism, or other illegal activities.

The OFAC, BIS, and SDN lists are updated regularly. This means that a supplier that was screened during the initial set-up may appear on a watch list during another phase of the lifecycle.

As a best practice, compliance screening should be performed on a quarterly basis or prior to payment. Some organizations have linked their compliance screening efforts to a "Quarterly Letter of Commitment" implemented at the CEO level. This is a great example of linking compliance efforts to the "Tone at the Top."

The Best Practice (7 of 7): Perform ongoing regulatory compliance screening on a regular basis vv vand/or prior to supplier payment.

Who is Responsible: Accounts Payable

Detecting and Preventing Accounts Payable Fraud

The below table describes 20 of the most frequently utilized internal controls at Fortune 100 companies. These practices have been found to detect fraud and strengthen compliance.

The Top 20 Accounts Payable Controls
Corporate Level Controls
1. Adherence to the company's "Tone at the Top"
2. Adherence to the company's Code of Conduct and ethics training
3. Performance of employee background checks
4. Performance of Delegation of Authority (DoA) controls
5. Assurance of Segregation of Duties (SoD) controls
6. Implementation of System Access (SA) controls
7. Assurance of Record to Report (R2R) controls
8. Implementation of Account Reconciliation controls
Managing the Supplier Master
9. Obtain W-9s and W-8s forms and validate tax form data
10. Perform TIN matching
11. Perform compliance screening (before onboarding and throughout the life of the supplier relationship)
12. Validate the supplier (Websites, scam suppliers, phone numbers, and address)
13. Perform supplier and employee master file matching process (annually)
Invoice Processing and Funds Disbursements
14. Implementation of a large dollar disbursement review process
15. Implementation of supplier payment data verification processes including Positive Pay, Positive Payee, and ACH Payment controls
16. Ensure Segregation of Duties (SoD) and approval controls for Supplier Master and invoice, processing, and bank funding
17. Implement and review AP operational metrics
18. Implementation of payee analytics to proactively flag suppliers with prior fraud history and/or fraudulent patterns
HR Controls
19. Implementation of a job rotation program (if feasible)

Managing the Risk: Internal Control Process for the Accounts Payable Record to Report (R2R) Process

The major obstacles to streamlined Record to Report (R2R) or closing processes are:

- Lag or latency of data related to payment status
- Un-normalized data (as reported by banks)
- Returned paper checks (e.g., bad addresses)
- Poor visibility or errors during the review process
- Unreconciled general ledger accounts

The Top Ten Internal Control Processes to Support the Accounts Payable Record to Report (R2R) Process

Process	Recommendations
1. **Policies and Procedures**	Implement standard policies and procedures for: 1. Accounting 2. Coordination 3. Communication 4. Checklists
2. **Accrued Expenses**	• At the close of each month, quarter, and fiscal year, accrual procedures are needed to ensure that all payments related to that month are properly included in the company's financial statements. Estimate where possible.
3. **Properly Recognizing Payments**	• Payments should be recorded in the period in which the goods or services are received or used. • Payments should also be recorded as the corresponding revenues are recorded.
4. **Roles and Responsibilities During the Fiscal Close**	• Define and communicate specific roles and responsibilities during each fiscal close – for everyone that impacts the process.
5. **The Review Process**	• Too many levels of review during the fiscal close can slow down the process by creating "bottlenecks".
6. **Internal Controls**	• To ensure proper valuation of the company's balance sheet at fiscal year-end, invoices must be charged in the fiscal period in which the goods are received and services are performed. • Internal controls can help validate the accuracy of general ledger accounts by performing ratio and trend analysis of account balances.

Table continued on next page.

Table continued from previous page.

The Top Ten Internal Control Processes to Support the Accounts Payable Record to Report (R2R) Process	
Process	**Recommendations**
7. Reconciling Accounts	• Significant balance fluctuations should be researched and explained. • Every bank transaction should be auditable and payment status must be ascertained as quickly as possible. • Ensure account reconciliations are appropriately approved and variances are properly explained. • Automation of process of merging and normalizing payment result data across different payment methods and countries.
8. Reporting Variances	• Variances should be aged and explained. • Action plans should be developed to address all variances. • Ensure account variances are appropriately approved.
9. Journal Entries	• Make greater use of importing tools or direct integrations to upload information into the accounting package. • Minimize the risk of duplicate and erroneous manual entries.
10. Financial Close Metrics	• Gross number of adjusting entries: Transaction errors must be corrected and their correction delays the closing process. • Review errors: This information can be used to track down and correct underlying problems that can be prevented during future closing processes. • Completion times and ending balances: • Cycle time to complete final accounts payable disbursement run • Cycle time to complete accrual process • Ending Clearing Account Balance • Outstanding Debit Account Balance

Addendum 1: Summary of Best Practices

Summary of Best Practices	
Best Practice 1: Integrate ethics and compliance requirements into all business processes to ensure that the "tone at the top" is embedded throughout the organization. Specifically as it relates to accounts payable financial controls, fraud prevention, and tax and regulatory compliance, the office of the CFO is responsible for establishing these guardrails and expectations for that function. This approach establishes a corporate environment of internal controls and compliance that extends to the accounts payable organization, including supplier management. These initiatives typically include the deployment of ethical standards or a code of conduct for the organization. This is also a requirement for Sarbanes Oxley 404.	**Best Practice 5:** • Validate supplier contact information, payment data, and tax information prior to supplier approval. This process should take into account the different requirements per each payment method and payee country. • Employ TIN matching to ensure verification of supplied vendor data. TIN matching is a pre-filing service only offered to payers and/or their authorized agents who submit any of six information returns (Forms 1099-B, 1099-K, INT, DIV, OID, PATR, or MISC). It enables validation of TIN and name combinations prior to submission of the information return. • Obtain a W-9 form for domestic suppliers, a W-8 form for foreign suppliers, and perform TIN matching prior to vendor setup and payment processing.
Best Practice 2: One of the most common "root causes" of fraud is the lack of SoD controls, weak SoD controls, inappropriate compensating controls, or failure to update SoD controls when responsibilities change. As a best practice, many organizations review their SoD controls on a quarterly basis as part of their control self-assessment (CSA) process. As a result of this review, the applicable SoD controls are updated appropriately.	**Best Practice 6:** • Collect and store tax forms prior to supplier onboarding • Screen tax forms and tax data provided to ensure proper payee tax classification (US account or non-US account) • Withhold necessary taxes prior to sending payment to supplier with non-US account classification • Apply tax status and withholding rules into annual 1042-S tax reporting
Best Practice 3: Employ systems that provide flexibility and discrete configuration of controls around system access and critical accounts payable paths. Specifically, certain employees should have full ability to effect AP transactions, approval rights, and access to information, while some may only be able to affect certain processes, have "read only" visibility or only limited visibility. On a related note, account funding for supplier payments should have limited access and clear roles. This reduces the need to manually monitor every transaction.	**Best Practice 7:** Perform ongoing regulatory compliance screening on a regular basis and/or prior to supplier payment.
Best Practice 4: Leading-practice companies link the DoA policy to the job levels within the employee master file. They then establish a DoA table to drive the approval workflow. If an approver moves to a different position or department or leaves the company, the approval tables are automatically updated.	

Addendum 2: Comprehensive Compliance Guide

Comprehensive Compliance Guide			
Compliance Area and Reference	**Specific Industry Focus**	**Process Areas Impacted**	**Summary**
1. Anti-Money Laundering (AML) www.finra.org/industry/aml	Anti-Money Laundering (AML)	Shared Service Centers Payroll Processing Benefits Providers Business Process Outsourcing (BPO) Organizations Loan Servicing Organizations that Process Client Data Data Center Co-Location/Network Monitoring Services Software as a Service (SaaS)	Firms must comply with the Bank Secrecy Act and its implementing regulations ("Anti-Money Laundering rules"). The purpose of the AML rules is to help detect and report suspicious activity including the predicate offenses to money laundering and terrorist financing, such as securities fraud and market manipulation. FINRA reviews a firm's compliance with AML rules under FINRA Rule 3310, which sets forth minimum standards for a firm's written AML compliance program. The basic tenets of an AML compliance program under FINRA 3310 include the following. 1. The program has to be approved in writing by a senior manager. 2. It must be reasonably designed to ensure the firm detects and reports suspicious activity. 3. It must be reasonably designed to achieve compliance with the AML Rules, including, among others, having a risk-based customer identification program (CIP) that enables the firm to form a reasonable belief that it knows the true identify of its customers. 4. It must be independently tested to ensure proper implementation of the program. 5. Each FINRA member firm must submit contact information for its AML Compliance Officer through the FINRA Contact System (FCS). 6. Ongoing training must be provided to appropriate personnel.
2. Standards for Attestation Engagements (SSAE-16) www.ssae-16.com/	All Global Service Providers	Shared Service Centers Payroll Processing Benefits Providers Business Process Outsourcing (BPO) Organizations Loan Servicing Organizations that Process Client Data Data Center Co-Location/Network Monitoring Services Software as a Service (SaaS) Medical Claims Processors	Statement on Standards for Attestation Engagements (SSAE) No. 16 is an attestation standard put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) that addresses engagements undertaken by a service auditor for reporting on controls at organizations (i.e., service organizations) that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entity's internal control over financial reporting (ICFR). SSAE 16 effectively replaces Statement on Auditing Standards No. 70 (SAS 70) for service auditor's reporting periods ending on or after June 15, 2011. Two (2) types of SSAE 16 reports are to be issued, a Type 1 and a Type 2. Additionally, SSAE 16 requires that the service organization provide a description of its "system" along with a written assertion by management. As an initial point of nomenclature, SSAE 16, unlike SAS 70, is an "attest" standard, falling under the attestation framework and not that of the "auditing" framework, which is the origination of the SAS 70 standard.

Addendum 2: Comprehensive Compliance Guide (Cont.)

3. The Sarbanes Oxley Act of 2002 www.soxlaw.com/ www.sec.gov	All Public Companies	All Financial Transactions	Congress reacted to corporate financial scandals, including those affecting Enron, Arthur Andersen, and WorldCom, by passing the Sarbanes Oxley Act of 2002. This Act, often referred to as SOX or Sarbox, is designed to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws." The act provides for new levels of auditor independence; personal accountability for CEOs and CFOs; additional accountability for corporate Boards; increased criminal and civil penalties for securities violations; increased disclosure regarding executive compensation, insider trading and financial statements; and certification of internal audit work by external auditors.
4. U.S. Sentencing Guidelines www.ussc.gov/guidelines/index.cfm	All U.S. Companies	All Financial Transactions	The US government would also appear to believe that a company's ethics and compliance culture are set by the very top levels of management because the U.S. Sentencing Guidelines states: "High-level personnel and substantial authority personnel of the organization shall be knowledgeable about the content and operation of the compliance and ethics program … and shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." While the Guidelines apply to all corporations, the larger the organization, the more formal the program should be and the greater the penalty for failure to comply. Formal policies and procedure and extensive communication programs are expected of a large publicly traded corporation. The expectations are not as extensive for a small business.
5. Foreign Corrupt Practices Act (FCPA) www.justice.gov/criminal/fraud/fcpa/	All U.S. Companies	Accounts Receivable Procurement Accounts Payable T&E Payroll	The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA"), was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. Specifically, the anti-bribery provisions of the FCPA prohibit the willful use of the mails or any means of instrumentality of interstate commerce corruptly in furtherance of any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person. The FCPA also requires companies whose securities are listed in the United States to meet its accounting provisions. See 15 U.S.C. § 78m. These accounting provisions, which were designed to operate in tandem with the anti-bribery provisions of the FCPA, require corporations covered by the provisions to (a) make and keep books and records that accurately and fairly reflect the transactions of the corporation and (b) devise and maintain an adequate system of internal accounting controls.

Addendum 2: Comprehensive Compliance Guide (Cont.)

6. The Foreign Account Tax Compliance Act (FATCA) www.irs.gov/businesses/corporations/article/0,,id=236667,00.html	U.S. Companies Making Payments to Foreign Payees	Foreign Entity Payees	The Foreign Account Tax Compliance Act (FATCA) established a new regime under Chapter 4 of the Internal Revenue Code for documentation of foreign entity payees and withholding from payments in the absence of certain documentation. These requirements are in addition to the documentation, withholding and reporting required under Chapter 3 of the Code. FATCA compliance will be phased in, starting in 2013. Some FATCA requirements will affect payers that make the types of payments reportable on Form 1099-MISC and Form 1042-S. Payers will need to update their procedures to ensure compliance with both sets of documentation and withholding requirements: the new rules for FATCA, and the previously existing rules for withholding at source on certain payments to nonresident alien individuals, foreign corporations and other foreign entities
7. Office of Foreign Asset Control (OFAC) www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx	All U.S. Industries	Accounts Receivable Procurement Accounts Payable T&E Payroll	The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments. Various sanctions programs administered by OFAC prohibit U.S. citizens, permanent residents of the U.S. and U.S.-based businesses, including U.S. branches of foreign companies, from engaging in business or financial transactions with any party included on OFAC's Specially Designated Nationals List (SDN List). The SDN List, which contains thousands of names, includes individuals, banks, businesses, vessels and other organizations that have been targeted and blocked by the U.S. Government for various policy reasons, such as terrorism, drug trafficking and weapons of mass destruction proliferators. Because of the ever-changing foreign policy landscape, OFAC frequently makes changes to the SDN List.

Addendum 2: Comprehensive Compliance Guide (Cont.)

8. Bureau of Industry and Security (BIS) www.bis.doc.gov/	All Industries	Accounts Receivable Logistics	The United States Department of Commerce's Bureau of Industry and Security (BIS), formerly known as the Bureau of Export Administration, is responsible for administering and enforcing export controls on U.S. commercial products, software and technology. BIS is also responsible for overseeing export controls on "dual-use" items that can be used in weapons of mass destruction applications, terrorist activities or human rights abuses. In addition to enforcing the Export Administration Regulations (EAR), BIS is responsible for issuing and administering several restricted party lists that apply to export and re-export transactions for which the agency has jurisdiction. These lists, which change frequently, include the following: • Denied Persons List – Includes the names of individuals and companies that have been denied export privileges by BIS, usually due to a violation of U.S. export control laws. U.S. persons and companies are generally prohibited from engaging in export transactions with parties named on the Denied Persons List. • Entity List – Identifies the names of companies, individuals, government agencies and research institutions that trigger export and re-export license requirements. U.S. companies need to ensure that the appropriate export licenses are in place before proceeding with transactions with parties on the Entity List. • Unverified List – Includes the names of foreign parties that BIS have been unable to conduct a pre-license check or post-shipment verification. Potential transactions with parties on the Unverified List are a "red flag" that must be addressed and resolved before proceeding with the export. • Significant civil and criminal fines and other penalties can be imposed on persons or companies engaging in prohibited transactions with parties included on the Denied Persons and Entity Lists. Civil penalties can also be imposed on export transactions with such parties even if such activity occurred inadvertently.
9. Foreign Terrorist Organization (FTO) www.state.gov/j/ct/rls/other/des/123085.htm	All U.S. Industries	Accounts Receivable Procurement Accounts Payable T&E Payroll	FTOs are foreign organizations that are designated by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended. FTO designations play a critical role in our fight against terrorism and are an effective means of curtailing support for terrorist activities and pressuring groups to get out of the terrorism business.

Addendum 2: Comprehensive Compliance Guide (Cont.)

10. Financial Crimes Enforcement Network (FinCEN) www.fincen.gov/	Financial Institutions	ACH, Wires, Checks, and Deposits	When the USA PATRIOT Act of 2001 was enacted, the act's Section 314(a) became a critical tool for investigating persons suspected of terrorism and/or money l aundering. With the Financial Crimes Enforcement Network (FinCEN) as the conduit, 314(a) enables law enforcement to solicit information from financial institutions related to such investigations through what is known as the FinCEN 314 list. The highly confidential and involved FinCEN compliance process depends upon the cooperation of three critical groups: 1. Federal, state, local and foreign law enforcement agencies send FinCEN their requests for information regarding subjects suspected of terrorism or money laundering. 2. FinCEN reviews these requests and, every two weeks, sends its FinCEN list via a secure internet site to financial institutions across the country. 3. Financial institutions must promptly search their entire customer database for any accounts maintained within the last 12 months and any transactions conducted within the last 6 months by named subjects on the FinCEN list.
11. Gramm-Leach-Bliley Act (GLBA) www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act	Per GLBA, the term financial institution covers many parallel sectors such as tax preparers, credit counselors, debt collectors, automobile dealers and much more. In general, if a business collects and shares personal information about consumers to whom they extend or arrange credit, they have an obligation to GLBA.	Transactions dealing with consumers' personal financial information	Three integral pieces of the 1999 Gramm-Leach-Bliley Act (GLBA) focus on the information security of consumers' personal financial information. The Financial Privacy Rule, the Safeguards Rule, and the Pre-texting Provisions together determine how financial institutions can collect this information and how they must ensure the security and confidentiality of it. To fulfill their GLBA compliance, all financial institutions must: • Provide notice to customers about its privacy requirements regarding their personal financial information (Financial Privacy) • Establish, implement, and maintain an Information Security Program that secures and protects consumers' personal financial information from anticipated threats and/or unauthorized access (Safeguards) • Ensure that consumers' personal financial information is not being collected under false pretenses (Pretexting)

Addendum 2: Comprehensive Compliance Guide (Cont.)

12. The Federal Financial Institutions Examination Council (FFIEC) www.ffiec.gov/	Financial Institutions	Business Continuity Planning Development and Acquisition Electronic Banking Fedline® Information Security IT Audit IT Management Operations Outsourcing Technology Services Retail Payment Systems Supervision of Technology Service Providers Wholesale Payment Systems	The Federal Financial Institutions Examination Council (FFIEC) is a five-member agency responsible for establishing consistent guidelines and uniform practices and principals for financial institutions. The member agencies include the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS). In 2004, the FFIEC updated its information technology examination manual to account for the ever-quickening pace of changes and advancements in technology occurring at financial institutions and technology service providers. The result is the FFIEC IT Examination Handbook, a compilation of twelve booklets that can be updated individually, as needed, by the Council.
13. Bank Secrecy Act (BSA) www.fincen.gov/statutes_regs/bsa	Financial Institutions	Bank Secrecy Act regulations require financial institutions to strictly record and/or report on cash purchases of negotiable instruments and cash transactions exceeding $10,000	The Financial Crimes Enforcement Network (FinCEN) is the administrator of the BSA. Over the years, the BSA has been strengthened through subsequent anti-money laundering (AML) laws. This includes parts of the USA PATRIOT Act that focus on money laundering in the form of terrorist financing. Financial Institution BSA/AML Compliance demands strong risk assessment and control of activities typically associated with money laundering and suspicious activities that might indicate money laundering, tax evasion or other crimes.
14. Reg CC www.federalreserve.gov/pubs/regcc/regcc.htm	Financial Institutions	Deposits to Financial Institutions	In response to consumer complaints about lengthy deposit hold times, Congress passed the Expedited Funds Availability (EFA) Act in 1987, ushering in Regulation CC (Reg CC). Reg CC sets fair and uniform guidelines and required disclosures for how deposited funds are handled and credited to customers' accounts. It also gives financial institutions the right to delay availability in situations that pose a high risk of fraud. Sub part B of Regulation CC \Compliance deals specifically with this Funds Availability, and therefore presents the most challenges for financial institutions. It stipulates, by deposit type, the amount of time that institutions can hold a deposit either under normal availability or, if specific criteria are met, under an extension of normal availability.

Addendum 2: Comprehensive Compliance Guide (Cont.)

15. Reg E www.fdic.gov/regulations/laws/rules/6500-3100.html	Financial Institutions	All EFT Transactions	Since 1978, when Congress passed the Electronic Fund Transfers Act (EFTA), better known as Regulation E (Reg E), financial institutions have been responsible for properly investigating consumer claims of electronic fund transfer (EFT) errors. Those investigations must follow very specific error resolution procedures. At the time that Reg E was enacted, paper-based payments far outnumbered electronic fund transfer payments. Today, the exact opposite is true with electronic payments representing over 66% of all payments. The rise in EFTs has been accompanied by a parallel rise in EFT error claims, making Reg E compliance that much more difficult for financial institutions to follow. Accurately complying with Reg E error resolution procedures requires financial institutions and their employees to recognize the following milestones and proceed accordingly with each claim: • When the official notice of a claim has occurred so that it can be investigated and resolved within the Reg E specified time period • When to issue provisional credit to the customer during an investigation • When to debit the customer's account if the investigation shows that no error occurred • When and how the customer should be notified throughout the investigation
16. U.S. Patriot Act and Consumer Identification Program (CIP) www.fincen.gov/statutes_regs/patriot/	Financial Institutions	Consumer Bank Account Information	Section 326 compliance requires that CIP procedures should: • Verify the identity of any person seeking to open an account using documentary and non-documentary verification • Maintain records of that CIP verification process for five years after the account is closed • Compare the customer's name against the government's list of known or suspected terrorists • Provide customers with adequate notice of the requirements for customer identification The U.S. Treasury Department considers Section 326's customer identification and record keeping requirements as vital tools in its fight against criminal enterprises such as terrorism and the growing threat from identity theft. Financial institutions play a significant role in that fight through their CIP compliance.

Addendum 2: Comprehensive Compliance Guide (Cont.)

17. Office of Inspector General (OIG) www.oig.hhs.gov/	Hospitals, Healthcare Systems, and Healthcare Insurance Companies.	Accounts Receivable Patient Billing	Office of Inspector General's (OIG) mission is to protect the integrity of Department of Health & Human Services (HHS) programs as well as the health and welfare of program beneficiaries. Since its 1976 establishment, OIG has been at the forefront of the Nation's efforts to fight waste, fraud and abuse in Medicare, Medicaid and more than 300 other HHS programs. HHS OIG is the largest inspector general's office in the Federal Government, with more than 1,700 employees dedicated to combating fraud, waste and abuse and to improving the efficiency of HHS programs. A majority of OIG's resources goes toward the oversight of Medicare and Medicaid — programs that represent a significant part of the Federal budget and that affect this country's most vulnerable citizens. OIG's oversight extends to programs under other HHS institutions, including the Centers for Disease Control and Prevention, National Institutes of Health, and the Food and Drug Administration.
18. Accountable T&E Plans and Employee Expenses www.irs.gov/	All Industries	T&E	The IRS has several publications that provide guidance with respect to employee expenses and expense reimbursement. Publication 463 - Travel, Entertainment, Gift and Car Expenses is the primary document that provides information about the types of expenditures that are allowable, as well as recordkeeping and reporting requirements. Section 11 of Publication 535 – Business Expenses provides similar material. On the IRS website, www.irs.gov, there are short documents that draw from Publication 463 and other IRS publications that provide overviews. These short documents are: • IRS Topic 305 – Record Keeping; • IRS Topic 510 - Business Use of Car; • IRS Topic 511 – Business Travel Expenses; • IRS Topic 512 – Business Entertainment Expenses; and • IRS Topic 514 – Employee Business Expenses. The concept of an accountability plan is critical to the controlling and managing of employee expense reimbursements. An accountable plan must have three elements: • Expenses must have a business connection, and the connection and purpose must be documented; • Expense substantiation must be done within a reasonable period of time; and • Excess reimbursement or allowances must be returned within a reasonable period of time.

About the Sponsor

Tipalti is the only supplier payments management solution to automate all phases of the global payment lifecycle in one unified cloud platform. Tipalti makes it painless for finance departments to pay any supplier in a range of payment methods across the world while ensuring all tax and regulatory requirements are met and enhancing the partner payment experience. Fast-growing companies like Twitter, GoPro, Disqus, Touch of Modern, and Vimeo use Tipalti to eliminate up to 80% of their workload spent managing payments to partners, so they can scale their business rapidly and efficiently with global growth. Learn more at **www.Tipalti.com.**

About the AP & P2P Network

The AP & P2P Network is the leading provider of training, education and certification programs specifically for Accounts Payable, Procure-to-Pay, Global and Shared Services professionals as well as Controllers and their F&A teams.

Membership to the AP & P2P Network **(www.app2p.com)** provides comprehensive tools and resources to financial operations professionals who manage or are deeply involved in the Accounts Payable and Procure-to-Pay process.

Focus areas include best practices for every AP & P2P function; AP & P2P metrics and benchmarking data; tax and regulatory compliance (e.g. 1099, 1042-S, W-9, W-8, Sales & Use Tax, Escheatment, VAT, Canadian Tax, Internal Controls); solutions to real-world problems challenging your department; AP & P2P automation case studies; member Q&A networking forums, Ask the Experts, calculators, and more than 300 downloadable, customizable AP & P2P policies, flowcharts, templates and internal control checklists.

A membership to the AP & P2P Network provides tangible ROI to any organization – saving your organization time, money and keeping you compliant.

Over 10,000 professionals have been certified as an Accredited Payables Specialist or Manager (available in English, Simple Chinese and Spanish), and Certified Professional Controller through the AP & P2P Network and its parent company, the Institute of Finance & Management.

AP & P2P Network also hosts the Accounts Payable and Procure-to-Pay Conference and Expo (Spring and Fall), designed to facilitate education and peer networking.

The AP & P2P Network is produced by the Institute of Finance and Management (IOFM), which is the leading organization providing training, education and certification programs specifically for professionals in Accounts Payable, Procure-to-Pay, Accounts Receivable and Orderto-Cash, as well as key tax and compliance resources for Global and Shared Services professionals, Controllers and their F&A teams. With a universe of over 100,000 financial operations professionals, IOFM is the trusted source of information in the rapidly evolving field of financial operations.