eftsure

AN 8-STEP PAYMENT CONTROLS GUIDE

Procure-to-Pay

An 8-Step Payment Controls Guide for Accounts Payable Managers

The goal of the Accounts Payable (AP) function in any organisation is simple:

To ONLY pay invoices that are legitimate and accurate.

At first glance this goal seems straight forward. However, any AP function can quickly become overwhelmed when processing large numbers of invoices from hundreds, if not thousands, of suppliers. Without rigorous Payment Controls in place, your organisation may find itself facing major losses due to fraud and error throughout the Procure-to-Pay cycle.

Following this 8-Step Guide will ensure your AP function follows best-practice principles that mitigate the risk of incorrect payments.

At the end of the Guide, print and retain our handy Checklist so you can ensure you're ticking all the right boxes every time an invoice needs paying.

eftsure

eftsure allows you to process EFT payments to suppliers without the risk of irretrievably sending the funds to the incorrect payee due to fraud or error.

The Procure-to-Pay cycle involves many steps. Ensuring your AP team always adheres to all your payment controls can be challenging for any AP Manager. However, with eftsure integrated into your accounting systems, you can rest assured that the correct payments are being sent to the correct recipients

Step 1

Requisition Request

The first step to ensuring your AP function runs effectively and efficiently, is having clear requisition policies and procedures set down by your organisation's Board or Senior Management.

These rules must clearly stipulate the types of requisition requests, including values, that require managerial authorisation. When managerial authorisation is necessary, the rules must specify which specific managers in each function or department are tasked with approving or denying requisition requests. Budgetary parameters must also be clearly stipulated in advance.

Quality assurance controls may also need to be mandated by the Board or Senior Management for certain types of goods or services. These may necessitate managers obtaining approval from other individuals with specific expertise. For example, prior to purchasing third-party software, the manager of a department may need to seek the approval of an IT manager, to ensure the software meets minimum security standards.

All staff need to be aware of the requisition policies and procedures, which typically include:

Requisition Request Form:

An employee (requisitioner) requests the purchase of a good or service by completing a Requisition Request Form. Depending on the type and value of the purchase, the requisitioner may need to obtain quotes and product specifications from multiple prospective suppliers. Numerous internal stakeholders may be involved in deliberations to ensure appropriate goods or services are being requisitioned. Additionally, contractual negotiations may be required between authorised representatives of your organisation and the supplier. These details may need to be included with the Requisition Request Form.

Requisition Request Screening:

The Requisition Request Form is submitted to a purchasing agent, who screens it to ensure all necessary information is included. If information is missing or inadequate, it may be returned to the requisitioner pending additional details. If sufficient information is included and the purchase amount is considered small, the purchasing agent may be authorised to approve it. Alternatively, the purchasing agent may escalate the request to an appropriate manager for authorisation.

Requisition Request Authorisation:

The Requisition Request Form is escalated to the relevant manager in the requisitioner's department for authorisation. The manager will determine whether the purchase is necessary, is within established budgetary parameters and meets quality assurance controls. If authorised by the manager, it will be forwarded to the finance team to issue a Purchase Order.

Step 2

Purchase Order

Once your organisation has agreed internally to purchase a particular good or service, it is necessary to advise the supplier of your decision. This is done through the issuance of a Purchase Order (PO).

Typically, a PO is used for the purchase of a single good or service, whereas a contract is negotiated with a supplier for ongoing commercial arrangements. The PO may outline specific details about the purchase including price, quantity, quality specifications and fulfillment times.

The process for issuing a PO includes:

Purchase Order Creation:

A PO should be drafted by the finance team once a requisition request has been authorised. At this point, best-practice requires the finance team to determine whether the supplier is new or already exists in the Vendor Master File. If the supplier already exists in the Vendor Master File, their supplier code number should be included on the PO. If the supplier does not yet exist in the Vendor Master File, they need to be onboarded before dispatching the PO (see Step 3). Importantly, the PO should also include a unique Purchase Order number. This is essential so your AP team will be able to match the invoice that the supplier will send with the correct PO. Failing to have a structured numbering convention in place will result in significant challenges and delays when it comes to efficiently processing invoices.

Purchase Order Approval:

Even though the requisition has already received authorisation, before a PO is sent to a supplier, it requires one final approval. This is so any final amendments to the purchase requisition can be included. Depending on your organisation, this final approval may be the authorising manager or a finance manager.

Purchase Order Dispatch:

Once the PO is approved, it is ready to be sent to the supplier. The PO should stipulate a date by which time the supplier needs to sign and return the document. It only becomes legally binding once signed by the supplier.

Copies of the PO should be supplied to:

- The requisitioner.
- The receiving department.
- The AP team for filing under the supplier's account in the ERP/Vendor Master File.

Step 3

Vendor Master File

Maintaining an accurate and up-to-date Vendor Master File is critical. Data anomalies increase the risk of payment errors. Furthermore, lax internal controls can result in cases of internal fraud.

When considering that the average Vendor Master Files contain 25% anomalous data, this is a significant risk that all organisations should be addressing.

When onboarding new suppliers into your Vendor Master File, follow these steps:

Compliance Checking:

At both initial onboarding, and prior to release of payments, always check the supplier's Registered Name/Trading Name, Contact Details, ABN and GST Registration Status. These details should be independently sourced and verified, rather than taken directly from invoices.

Credit Worthiness:

Obtain credit scores or credit worthiness reports on third party vendors to deliver goods and services. This is of particular importance if you are pre-paying for goods and services and want to be confident of delivery.

Naming Conventions:

Establish strong supplier naming conventions to avoid creating multiple entries for each supplier within your Vendor Master File. The key here is to be consistent. Rigorously adhering to naming conventions will help you avoid duplicate payments.

Data Hygiene:

Having one member of your AP function responsible for inputting data into your Vendor Master File, and another member responsible for checking that data on a continual basis, is an effective way to ensure that the data in your file remains clean, accurate and up-to-date. Never have the same individual inputting data into the system, checking the data and processing payments. Segregation of duties is an essential internal control that should be embedded throughout the payment process. It will enable your organisation to mitigate fraud and reduce error.

Call Backs:

Conducting manual call backs is one of the most important, yet time consuming, tasks the AP team undertakes in order to ensure payment accuracy. With increased risk of invoice manipulation, call-back controls must not be avoided. There are numerous risks when conducting call backs. If the invoice has been manipulated, it is possible that the contact details on the invoice were also altered. Therefore, it is essential to source supplier contact details from an independent source, such as the payee's official website. Furthermore, your AP team should never blindly trust information from inbound calls or voicemail messages. Such information could be part of the fraudster's tactics. Your AP team should be trained to detect the latest fraud schemes. Social Engineering scams such as Business Email Compromise have reasserted the need for rigorous verification and best practice call-back controls.

Step 3

Matching Bank Data:

One of the most significant risks organisations face when processing invoice payments via EFT, is that banks do not match the Account Name with either the BSB or Account Number. This poses a significant risk as it opens the way for fraudsters to manipulate communications, deceiving AP teams into changing records in ERP systems, Vendor Master Files or the text-based ABA files that are used to process EFT payments in online banking portals. This may result in funds being transferred irretrievably to the fraudster's bank account. Internal fraud and error are additional risks that can result from this verification gap. AP teams need to be vigilant in ensuring that Account Names align with BSB and Account Numbers to reduce the risk of transferring funds to incorrect recipients.

Step 4

Receiving and Inspection Reports

In an ideal world, every supplier would fulfil every PO accurately and on time. However, in reality, this is often not the case. All too often suppliers do not fulfil their obligations. Every organisation's AP function has a responsibility to ensure payments are not processed to a supplier unless they have fulfilled their obligations as outlined in the PO.

Some of the common problems organisations experience with suppliers of goods include:

- Invoice terms not aligning with the PO.
- Partial shipments.
- Damaged goods.
- Price discrepancies between the invoice and the PO.
- Inclusion of additional charges such as freight, insurance etc.
- GST or other taxes added on when they should be included in the sale price.

Best-practice mandates that the following steps should be followed when suppliers fulfil orders:

Centralised Receiving:

Goods should be delivered centrally to a receiving department. This is to ensure that accurate records can be kept and all relevant functions in the organisation maintain visibility over procurement.

Receiver Inspection:

Upon delivery, goods should be inspected immediately by the receiving department. This is to validate whether quantities of delivered goods align with the delivery receipt and PO. Any obvious problems, such as incorrect quantities or obviously damaged goods, should be detailed in a digital Receiving Report. At this point the receiving department can deliver the goods to the requisitioner's department.

Requisitioner Inspection:

The requisitioner conducts a more comprehensive inspection to validate quantity and quality of goods delivered. If the requisitioner determines that the quantity and quality of the goods are in alignment with the PO, they indicate 'acceptance' of the goods on the digital Receiving Report. If the quantity or quality of the goods do not align with the PO, then the requisitioner indicates 'non-acceptance' on the digital Receiving Report and the goods are returned to the receiving department, pending their return to the supplier.

Receiving Report:

The completed Receiving Report must be made available to the AP team. The AP team needs to ensure the completed digital Receiving Report is accurately filed under the correct supplier code number in the ERP/Vendor Master File.

In some organisations, the requisitioner will also complete a separate Inspection Report. This is a qualitative assessment to determine whether the goods procured meet expectations. This can also be a useful mechanism to determine whether services purchased align with the PO. If undertake, the Inspection Report should be made available to the AP team and filed under the correct supplier code number in the ERP/Vendor Master File.

Step 5

Invoice Handling

With the right systems and procedures in place, it is possible to efficiently determine whether an invoice is legitimate and accurate. This allows your AP team to efficiently process those invoices that need to be paid, whilst avoiding fraud or error.

The following steps represent best-practice when it comes to receiving and handling invoices:

Electronic Invoices:

Encourage all suppliers to send invoices electronically. In some cases, suppliers may use E-Invoicing software, or they may simply email through an invoice. Paper invoices should be avoided. Invoices should be sent to a dedicated AP email address that is accessible by a limited number of nominated individuals within the AP function. This is an important control to ensure that invoices are not lost and reduces the risk of internal manipulation. The personnel that access electronic invoices are your first line of defence in identifying potential phishing or Business Email Compromise attacks. They need comprehensive and ongoing training to be able to identify the warning signs of malicious email, such as suspicious 'From' addresses, incorrect domain names, suspicious or incorrect wording, etc. Any links or attachments in suspect communications must not be clicked and the incident needs to be reported to the IT help desk immediately.

Invoice Encoding:

Nominated individuals within the AP function should have responsibility for encoding invoice data into the Vendor Master File and ERP systems. Segregation of duties necessitates that these individuals should NOT be those who verify and process payments. By this stage, the supplier should be set up within your ERP/Vendor Master File. The encoder should categorise the invoice and verify that it is not a duplicate payment. Ensuring that a limited number of individuals are responsible for encoding data will help you maintain data hygiene and integrity in your systems, resulting in increased efficiencies and fewer opportunities for losses due to fraud or error. Some organisations have adopted AP Automation technologies to drive further efficiencies in this stage of the process. The information encoded should include:

- The Purchase Order number.
- The supplier code as per the ERP/Vendor Master File.
- The supplier name as per the ERP/Vendor Master File.
- An invoice number issued by the supplier to avoid duplicate payments.
- Payment amount.
- Payment date.
- EFT details.

Incomplete or Incorrect Invoices:

Not all suppliers send accurate invoices. Once the data from an invoice has been encoded into the Vendor Master File and ERP system, it may become apparent that the invoice is either incomplete or incorrect (*see Step 6*). This will require the AP team to revert back to the supplier with a request to update or amend the invoice.

Step 6

Invoice Challenges

As discussed above, some suppliers send invoices that do not align with the PO. They may be incomplete or incorrect invoices. This can result in significant inefficiencies and will require your AP team to liaise with both the supplier and the requisitioner.

Some of the common challenges found in invoices include:

Unidentified Invoices:

All too often, invoices turn up in the AP department with no PO number, nor any identification as to who the requisitioner is. In large organisations, it can be extremely time consuming, if not impossible, for AP staff to identify which employee or department procured the good or service. Unidentified invoices should NEVER be processed, as it may be an attempt to defraud your organisation. Unidentified invoices should be returned to the supplier pending further information.

Missing Invoice Numbers:

Suppliers should issue a unique invoice number for every invoice they send out. This is extremely important so you can avoid paying duplicate invoices. If any invoice arrives without a unique invoice number, return the invoice to the supplier so it can be amended.

Discrepant Invoices:

In cases where there is a discrepancy between an invoice and the PO, Receiving Report or Inspection Report (see Step 7), the AP team will need to liaise with the requisitioner and the supplier to resolve outstanding issues. Ideally, any discrepancies will be resolved by the due date, however in some cases this may not be possible. As a result, the supplier may send a second invoice. This creates a challenge as the AP team needs to identify it as a second invoice and have visibility over the cause of the delay in processing the payment. Detailed information and records of communication with the supplier are necessary to ensure second invoices are not inadvertently paid.

Short-Paying Invoices:

An organisation may decide to short-pay a supplier due to a range of reasons. These may include negotiated discounts for early payment, incomplete shipments, damaged goods, prior credits, etc. However, whenever an invoice is not paid in full, it is important to maintain detailed records in the ERP/Vendor Master File and to communicate the reasons to the supplier. Failure to do this will result in accounting discrepancies between records in the ERP/Vendor Master File and bank statements at audit time.

Step 7

Invoice Matching

Determining whether or not an invoice should be paid is one of the most important responsibilities of the AP team.

Once an invoice is received, the AP team needs a system to check the validity of the invoice. This is achieved through either 2, 3 or 4 Way Invoice Matching.

Invoice Matching

	2-Way	3-Way	4-Way
Invoice	▲	▲	▲
Purchase Order	▲	▲	▲
Receiving Report		▲	▲
Inspection Report			▲

Inadequate reporting and filing systems would make Invoice Matching impossible. Only when POs, Receiving Reports and Inspection Reports are created according to established procedures, will the AP team be able to efficiently access the information they require to conduct Invoice Matching.

If, for whatever reason, an invoice does not match with the PO, Receiving Report or Inspection Report, payment should be stopped pending further information. The AP team should seek further clarification from the requisitioner, who may need to liaise with the supplier to address certain issues.

Guidance for whether to opt for 2, 3 or 4 Way Invoice Matching is a determination of the Board or Senior Management. Typically, smaller invoices will only require 2 Way Invoice Matching. Larger invoices will require 3 or 4 Way Invoice Matching.

As stated previously, the purchase of services will not require a Receiving Report but may require an Inspection Report.

Step 8

Continuous Controls Monitoring (CCM)

Payment processing is a high-risk activity due to the possibility that supplier banking details can be fraudulently manipulated or erroneously changed at any stage of the Procure-to-Pay cycle.

As discussed previously, banks do not have the capacity to verify that an Account Name matches a BSB or Account Number when processing EFT payments. That verification gap means you cannot assume the details in your EFT/Vendor Master File are accurate.

Despite the fact that you undertook a range of verification checks, including call-backs, when you onboarded a supplier into your Vendor Master File (see Step 3), over time this data may have been compromised, either by malicious actors or due to staff error.

Every organisation should adopt Continuous Controls Monitoring (CCM) technology solutions to ensure payment data remains accurate right up to the point of payment processing.

Spot-checks:

Once a payment file is compiled, manual spot-checks need to be undertaken to validate the accuracy of the data in the file. Random line items should be checked against existing data in the ERP/Vendor Master File to verify that they match. Manual spot-checks are both time consuming and are not infallible as only a selection of payments are checked. It is preferable to have a technology solution in place that allows your organisation to embrace an effective CCM policy.

CCM Technology:

Continuous Controls Monitoring is an indispensable element in the Procure-to-Pay cycle. Between the time a supplier is onboarded into your Vendor Master File, through to the time when an EFT payment is processed, any number of events can occur that result in incorrect payments. Malicious actors may succeed in manipulating supplier banking details following breaches of your ERP/Vendor Master File. Internal threat actors may compromise data in the text-based ABA files that are used to upload payments to online banking portals. Alternatively, fraudsters may deceive your AP team into erroneously changing supplier banking details. Due to all these reasons, it is not enough to rely on the fact that you verified a supplier at the time they were onboarded into your Vendor Master File.

Whilst spot-checks can be useful to identify some invalid payments, they are not comprehensive. Inevitably, incorrect payments will slip through a system of manual spot-checks. A CCM technology solution will validate all payments in real-time, right before the payment is being processed, to identify any incorrect payments. A CCM technology solutions should also validate in real-time the payee's ABN and GST registrations to ensure they remain current.

Final Authorisation:

Once all necessary steps have been followed to ensure that payment should proceed, final authorisation is usually required from an executive within the finance function. This final authoriser should ensure that all payment files have been validated in line with CCM best-practices.

Conclusion

Adhering to these 8 Steps will help ensure your organisation's AP function operates effectively, whilst reducing the risks you face of fraud and error throughout the Procure-to-Pay cycle.

Whilst many of these steps may be manual, resource intensive and time consuming, they are essential to ensuring only legitimate and accurate invoices are paid by the AP function.

The good news is that technologies now exist that can help automate a range of these essential steps. Platforms, such as eftsure, drive efficiencies throughout the Procure-to-Pay process. Whether it's onboarding and maintaining a clean Vendor Master File, checking supplier credentials for compliance purposes, or ensuring that EFT payment details are accurate, eftsure is a tool that allows you to operate your AP function effectively and efficiently.

Print and retain the checklist that follows to ensure your AP team is always following best-practices.

Procure-to-Pay Checklist

1 Requisition Request

- [ ] Has a Requisition Request Form been submitted by the employee who is requesting the procurement of the good or service?
- [ ] Has the Requisition Request Form been screened by the purchasing agent to ensure all relevant information is included?
- [ ] Has the Requisition Request Form been authorised by the relevant manager inline with company policies and procedures?

2 Purchase Order

- [ ] Has a PO been created and filed correctly under the supplier's account in the ERP/Vendor Master File?
- [ ] Has the PO been approved by the relevant manager inline with company policies and procedures?
- [ ] Has the PO been dispatched to the supplier so they can begin fulfilling the order?

3 Vendor Master File

- [ ] Is the order being placed with a pre-existing supplier?
- [ ] If not, has this new supplier been onboarded in the Vendor Master File in line with established Naming Conventions?
- [ ] Has the supplier's ABN and GST status been checked for compliance purposes?
- [ ] Has the supplier's credit worthiness been checked?
- [ ] Have you matched the Account Name against the BSB and the Account Number to ensure the bank details are accurate?
- [ ] Have you independently sourced the supplier's contact details and conducted a Call-Back to verify payment details?

4 Receiving and Inspection Reports

- [ ] Have the procured goods or services been fulfilled by the supplier in line with the PO?
- [ ] Has a Receiving Report been completed by the receiving department and filed correctly under the supplier's entry in the ERP/Vendor Master File?
- [ ] Has an Inspection Report been obtained from the requisitioner?

5 Invoice Handling

- [ ] Has an electronic invoice been sent to the dedicated email address?
- [ ] Has the email been scanned for malware and examined for any evidence of attempted Social Engineering?
- [ ] Has the data in the invoice been encoded into your ERP system and double checked for accuracy by a different member of your AP team?

6 Invoice Challenges

- [ ] Have you thoroughly checked for any duplicate payments?
- [ ] Is the invoice complete and, if not, has it been returned to the supplier to provide complete details?
- [ ] Will you be short-paying the invoice and, if so, have you documented the reasons and communicated these to the supplier?

7 Invoice Matching

- [ ] 2-Way Matching: Have you matched the invoice to the PO?
- [ ] 3-Way Matching: Have you matched the invoice to the PO and the Receiving Report?
- [ ] 4-Way Matching: Have you matched the invoice to the PO, the Receiving Report and the Inspection Report?

8 Continuous Controls Monitoring

- [ ] Have you undertaken random spot-checks to ensure the data in the payment file is still accurate?
- [ ] Have you embraced a CCM technology solution which allows you to check all payment details in real-time, immediately prior to processing?
- [ ] Have you received final authorisation for the payment from a finance manager?

Don't yet have a CCM technology solution? Visit: **eftsure.com.au/check**

This free tool allows you to verify the supplier's banking data against eftsure's database comprising over 2 million Australian organisations. It allows you to ensure, in real-time, that the supplier's Account Name aligns with their BSB and Account Number.

CONGRATULATIONS – You are now ready to process the payment!

eftsure

eftsure

Contact us

1300 985 976
sales@eftsure.com.au

eftsure.com.au