Segregation of Duties Concepts

Chris Doxey, CAPP, CCSA, CICA,CPC

chris@chrisdoxey.com

President, Doxey, Inc.

Speakers

Chris Doxey
President

Doxey, Inc.

(Author, Speaker, P2P “Guru” and Internal Controls Expert)

Stephen Williams
Vice President of Marketing

MineralTree

Our Sponsor: MineralTree

Accounts Payable and Payment Automation from Invoice-to-Payment

Founded
in 2010

Based in
Cambridge, MA

Founder/CEO
BC Krishna, MIT Alumni

Trusted by
+1500 companies

Processed +$4B
in annual payments

Backed by Fidelity
Investments, First Data &
.406 Ventures

Resold as a private label
solution through over a
dozen banks

Agenda

- Introduction to the Segregation of Duties (SoD) Controls
- Defining SoD Conflicts
  - Corporate Level
  - AP Process Level
- About System Access Controls
- When to Consider Compensating Controls
- The Specifics of a SoD Policy
- Case Study
- Q&A

Segregation of Duties (SoD)

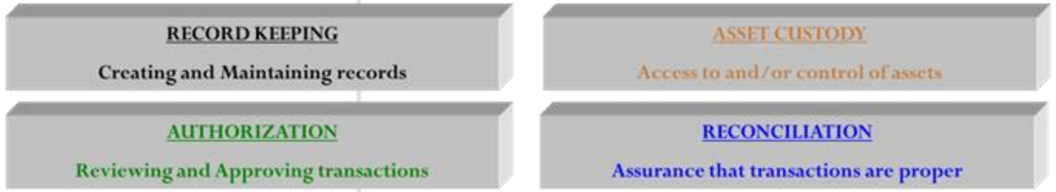
Key Segregation of Duties (SoD) Concepts

RECORD KEEPING **Creating and Maintaining records**	**ASSET CUSTODY** **Access to and/or control of assets**
AUTHORIZATION **Reviewing and Approving transactions**	**RECONCILIATION** **Assurance that transactions are proper**

Examples of SoD Conflicts

- Authorizing purchases and receiving goods purchased from the transaction
- Setting up a vendor and executing the payments

Segregation of Duties (SoD)

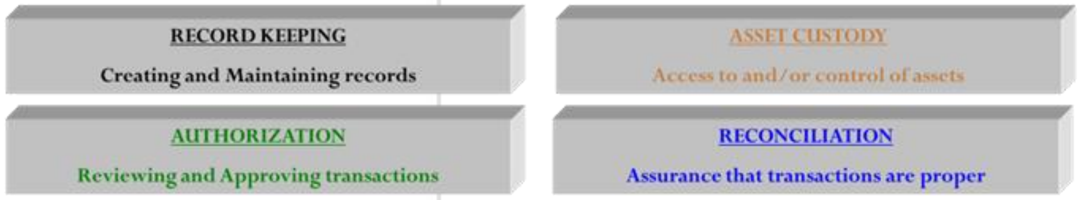


- The Segregation of Duties (SoD) control is the most important set of controls that your organization can have.

- It is the cornerstone of any formal internal controls framework and is essential to the detection and prevention of fraud.

- Effective segregation of duties reduces the risk that fraud error (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.

Segregation of Duties (SoD) (Continued)



SoD controls provide four specific 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 due to additional review(s) of the transaction.
3. The cost of corrective actions is reduced as errors are generally detected relatively early in their lifecycle
4. The organization’s reputation for integrity and quality is safeguarded through a system of checks and balances.

Segregation of Duties (SoD) (Continued)

RECORD KEEPING Creating and Maintaining records	ASSET CUSTODY Access to and/or control of assets
AUTHORIZATION Reviewing and Approving transactions	RECONCILIATION Assurance that transactions are proper

- Despite its indispensability as a fraud-mitigation measure, SoD is one of the most difficult to implement and maintain often due to limited headcount with broadly defined responsibilities, and constantly changing responsibilities.

- Even under challenging personnel circumstances, it is important to ensure that key duties are adequately segregated or consider compensating controls.

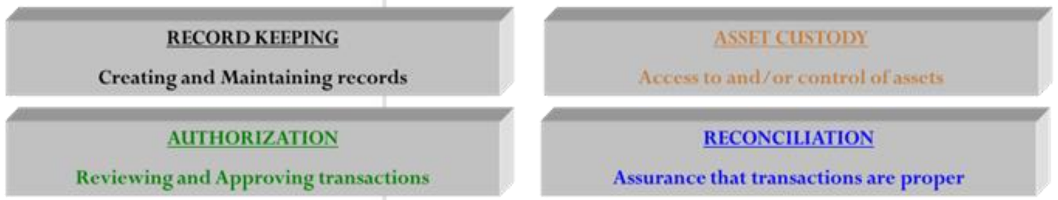
Segregation of Duties (SoD) (Continued)

RECORD KEEPING Creating and Maintaining records	ASSET CUSTODY Access to and/or control of assets
AUTHORIZATION Reviewing and Approving transactions	RECONCILIATION Assurance that transactions are proper

- **Planning/Initiation:** An organization should consider roles and responsibilities when establishing the structure of a department focusing on the review and approval process.

- **Transaction Authorization:** Compensating controls are critical to a process with limited headcount. However when implementing compensating controls, the organization should risk the cost of the reduction of risk to implement the control.
  - **Custody of assets such as financial assets and inventory.**
  - **Recording or reporting of transactions.**
  - **Control tasks such as review, audit, and reconciliation should not be performed by the same individual responsible for recording or reporting the transaction.**

Segregation of Duties (SoD) - Best Practice



- **As a best practice, many organizations review their SoD controls on a quarterly basis as part of their controls self-assessment (CSA) and continuous controls monitoring (CCM) processes.**
  - 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.
  - 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.

Polling Question 1

On average, how many payments do you process each month?

- 0-50
- 51-100
- 101-200
- 200+

Defining SoD Conflicts

Corporate Level SoD Concepts

- In an ideal system, different employees would perform each of these major functions.
- Segregation of duties would imply that no one would have control of two or more of these responsibilities within a given sub-cycle or process.
- As a matter of degree of application, the more negotiable the asset is in the marketplace, typically the greater the need for proper segregation of duties -- especially when dealing with cash, negotiable checks and inventories.

Corporate Level SoD Concepts

- It may be possible for one person to perform multiple responsibilities as long as they are across separate or segregated processes, activities, transactions and other business matters.

- For example, a customer account representative may have responsibilities for obtaining credit information, updating customer profile information, verifying contract terms, and posting equipment changes

Polling Question 2

How much do you think its costs to process and pay one invoice??

- Less than $1
- $1.01 - $5.00
- $5.01 - $10.00
- More than $10

Example SoD Conflicts Matrix – Accounts Payable

PROCESS	GROUP NAME	GROUP	01 CHECK DISBURSEMENT MANAGEMENT	02 PROCESS AND PRINT PAYMENTS	03 A/P ENTRY	04 A/P PAYMENTS	05 PURCHASE REQUISITIONS	06 RELEASE PURCHASE REQUISITIONS	07 PURCHASE ORDERS	08 RELEASE PURCHASE ORDERS	09 VENDOR MASTER DATA	10 RELEASE VENDOR INVOICES	11 VENDOR PRICING AGREEMENTS	12 CHECK ADJUSTMENTS	13 POST A/P PAYMENTS
AP & PROCUREMENT	CHECK DISBURSEMENT MANAGEMENT	01			×	×					×	×		×	×
	PROCESS AND PRINT PAYMENTS	02			×	×	×	×	×	×	×	×		×	×
	A/P ENTRY	03	×	×		×	×	×	×	×	×	×	×	×	×
	A/P PAYMENTS	04	×	×	×		×	×	×	×	×	×	×	×	
	PURCHASE REQUISITIONS	05		×	×	×		×		×	×	×		×	
	RELEASE PURCHASE REQUISITIONS	06		×	×	×	×				×	×	×	×	
	PURCHASE ORDERS	07		×	×	×				×	×	×	×	×	×
	RELEASE PURCHASE ORDERS	08		×	×	×	×		×		×	×	×	×	×
	VENDOR MASTER DATA	09	×	×	×	×	×	×	×	×		×	×	×	×
	RELEASE VENDOR INVOICES	10	×	×	×	×	×	×	×	×	×		×	×	×
	VENDOR PRICING AGREEMENTS	11			×	×		×	×	×	×	×		×	×
	CHECK ADJUSTMENTS	12	×	×	×	×	×	×	×	×	×	×	×		×
	POST A/P PAYMENTS	13	×	×	×				×	×	×	×	×	×	

About Systems Access

Systems Access

- The principle of segregation of duties in an information systems environment is also critical as it ensures the separation of different functions such as transaction entry, on-line approval of transactions, vendor master file initiation, master file maintenance, system access rights, and the review of transactions.

- In the context of application level controls, this means that one individual should not have access rights which permit him or her to enter, approve and review transactions.

Systems Access (Continued)

- Assigning different security profiles to various individuals supports the principle of segregation of duties.

- As an example, operational or process segregation of duties and determines to whom varying system access rights that should be granted.

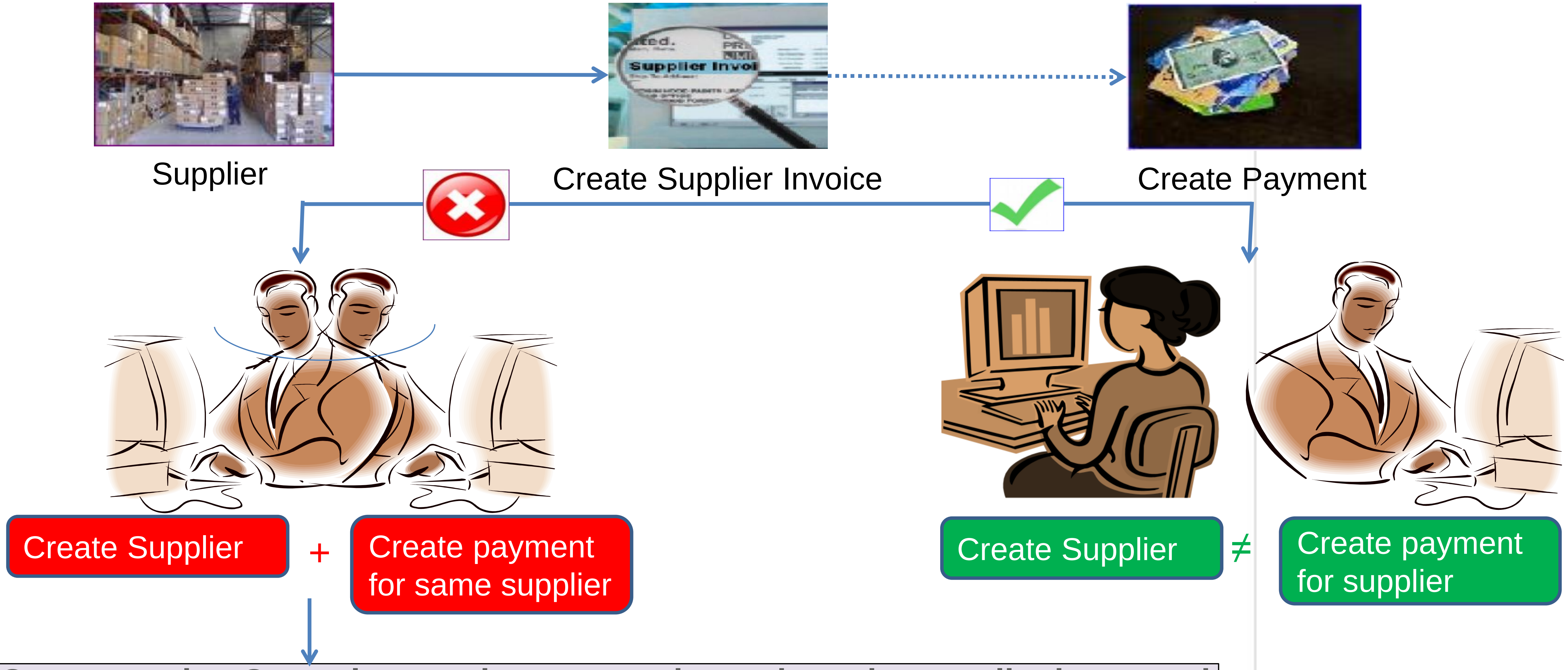
Systems Access (Continued)

- System access rights are reviewed on a periodic basis (usually monthly or quarterly) to ensure that system access capabilities are appropriate for current staff members and reflect any changes in responsibilities or movements to other departments.

System Access- Best Practices (AP Example)

- **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.
  - Account funding for supplier payments should have limited access and clear roles. This reduces the need to manually monitor every transaction.

Automating Systems Access Controls



Setup Compensating Control to monitor transactions where the supplier is created and paid by the same user

When to Consider Compensating Controls

Examples of Compensating Controls

1. Skim through detailed transactions report: A manager may consider performing a high level review of detailed report of transactions completed by an employee that performs incompatible duties. As an example, a manager may simply skim through the report sections that contain high risk transactions or account and may review specific payment types or amounts before the payment is made.

2. Review sample of transactions: In a quarterly control self-assessment process, a manager may select a few sample of transactions, request for the supporting documents and review the documents to ensure that they are complete, appropriate, and accurately processed. In addition to detecting errors, the knowledge of a periodic review could create a disincentive (that is, reduce the opportunity) for the person performing the incompatible duties to process unauthorized or fraudulent transactions. The self-assessment process can also reduce the risk of collusion.

Examples of Compensating Controls (Continued)

3. Review System Reports: Applications that support business or office operations have embedded reporting capabilities that enable the generation of reports based on pre-determined or user defined criteria. A review of relevant system exception reports can provide good compensating controls for an environment that lacks adequate segregation of duties. As an example, perform a review of report of deleted or duplicated transactions, report of changes to data sets and report of transactions exceeding a specific dollar amount on a quarterly basis.

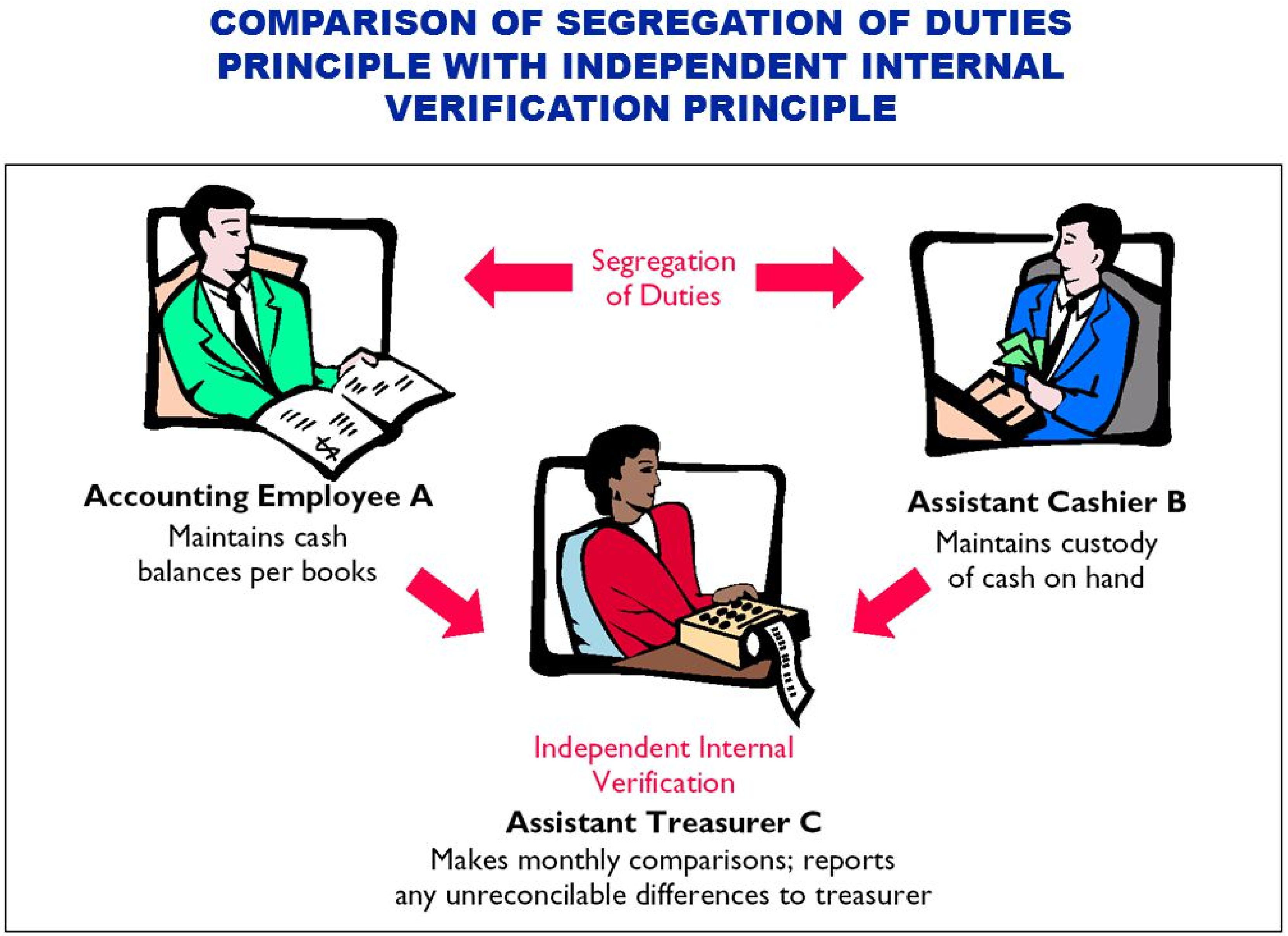
4. Perform Analytical Reviews: Another example of compensating control is the comparison of different records with predictable relationships and the analysis of identified unusual trends. For example, a budget vs. actual expenditure comparison or current year vs. prior year subscription fees analysis or comparison of selected asset records to actual physical count of asset might indicate unusual variances or discrepancies that may need to be investigated. In this review, an analytical review should occur on a monthly basis.

Examples of Compensating Controls (Continued)

6. Increase Supervisory Oversight: Other forms of activities a manager may perform as compensating control are observation and inquiry. Where appropriate, increasing supervisory reviews through the observation of processes performed in certain functions and making inquiries of employees are good administrative controls that may help to identify and address areas of concerns before a transaction is finalized.

7. Rotate Jobs: Many companies rotate jobs in the finance and accounting department every 1-2 years. This creates an environment of control and can prevent collusion. As example, accounts payable processors should be rotated on a regular basis so that they don't become too involved with specific suppliers.

Combining SoD Controls with Compensating Controls

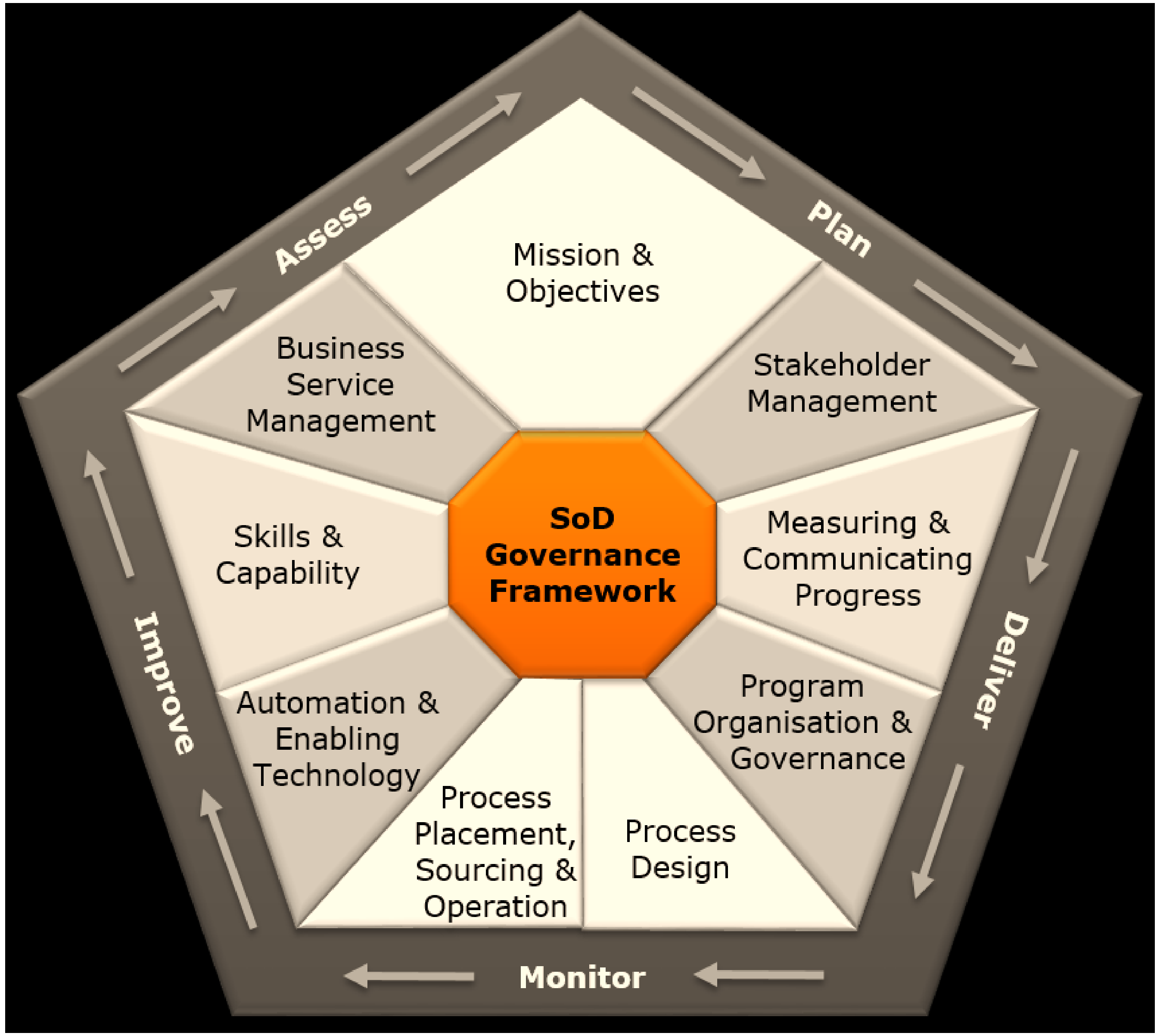


Polling Question 3

- What percentage of your monthly payments are made by paper check?
  - 0% - 25%
  - 26% - 50%
  - 51% - 75%
  - 75%+

The Specifics of an SoD Policy

Segregation of Duties (SoD) Governance Framework



Risks Addressed by the Implementation of an SoD Policy

- Misstatement of financial accounts and management information due to: intentional or unintentional errors, omissions, and fraud
- Loss of audit trail which validates detail analysis, approval, and implementation of transactions
- Non-compliance with legal requirements
- Loss of Company Reputation
- IT security weaknesses

Domains of an SoD Policy

These domains of an SoD policy are organizational, functional, and technological.

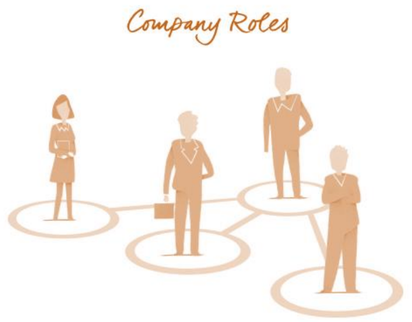
1. The organizational domain addresses segregation of duties issues that may develop due to the organizational structure of the company.
2. The functional domain addresses segregation of duties issues that may develop due to the job functions for which individuals are assigned responsibility.
3. Finally, technological domain addresses segregation of duties issues may develop due to the security configuration of various IT systems and considers strong system access controls.

SoD Roles and Responsibilities

a) Each functional business area shall be responsible for developing and implementing a schedule for assessing its area for potential or actual segregation of duties on a recurring basis.

b) Each functional business area shall formally evaluate its area for the existence of potential or actual segregation of duties issues on a periodic basis.

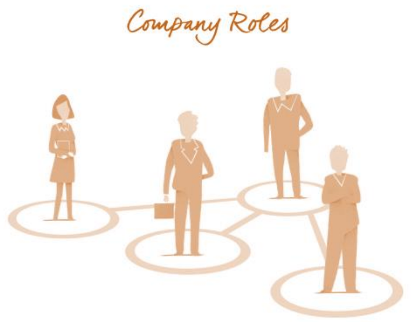
c) Organizational segregation of duties issues shall be considered during the periodic evaluations. The positioning of the business area in company, its relationships with other functional business areas, and the nature of its responsibilities shall be considered.



SoD Roles and Responsibilities (Continued)

d) Functional segregation of duties issues shall be considered during the periodic evaluations. The assigned job functions of personnel in the business area shall be considered from a standpoint of incompatible duties.

e) Technological segregation of duties issues shall be considered during the periodic evaluations. The assigned system and application security of personnel shall be considered from a standpoint of access within systems to perform incompatible functions.



Responsibilities for Remediating SoD Issues

a) Each functional business area shall document the segregation of duties issues identified during the formal periodic evaluations.

b) The nature of the issue, the domain (i.e. organizational, functional, or technological), and the involved parties/systems shall be included in the documentation of the segregation of duties issues.

c) Business area management shall review the documentation and determine remediation options for each issue.

d) Remediation options may include a combination of corrective or mitigating measures.

e) Business area management shall document the selected remediation method, along with the effective date of the remediation.

f) Senior management and Internal Audit shall be provided copies of all documentation relating to segregation of duties analyses and remediation

Case Study

Case Study – The Alberta Motor Association

- The Alberta Motor Association (AMA) has filed a large-scale lawsuit against its former vice-president of information technology (IT) after it discovered he allegedly defrauded the company $8.2 million over a period of three years—one of the top five most costly cases of fraud to hit the province in 20 years.

- In what appears to be an absence of segregation of duties (SoD), the employee was the only individual with authority to approve payments for goods and services invoices for the AMA's IT department.

- The AMA alleges that the worker devised a fraud scheme whereby he created false invoices for amounts ranging from $30,000 to $450,000 USD. It also involved funds being transferred electronically to banks in the U.S.

Case Study – The Alberta Motor Association (Continued)

- In the case of the fraud scheme that impacted the AMA, stronger SoD will be required to avoid this type of fraud going forward.
- Segregation of duties is an essential internal control that helps deter fraudsters by reducing the number of opportunities for abuse.
- SoD conflicts can be caused by insufficient staffing, which makes it difficult to segregate duties appropriately because there are simply not enough employees.
- These conflicts can then be exacerbated by poor or missing controls; for example, in the case of the AMA, having only one person rather than two authorized to approve invoice payments, or allowing just one individual to create and approve a company budget.

Source: https://www.casewareanalytics.com/blog/millions-lost-due-segregation-duties-failings

Benefits of Automating AP

mineraltree®
AP and Payment Automation

How can your AP process benefit from automation?

- Lower Processing Costs
- Increase Efficiency
- Control Outgoing Cash
- Improve Internal Accounting Controls
- Optimize Working Capital

AP Automation Streamlines the Entire Process

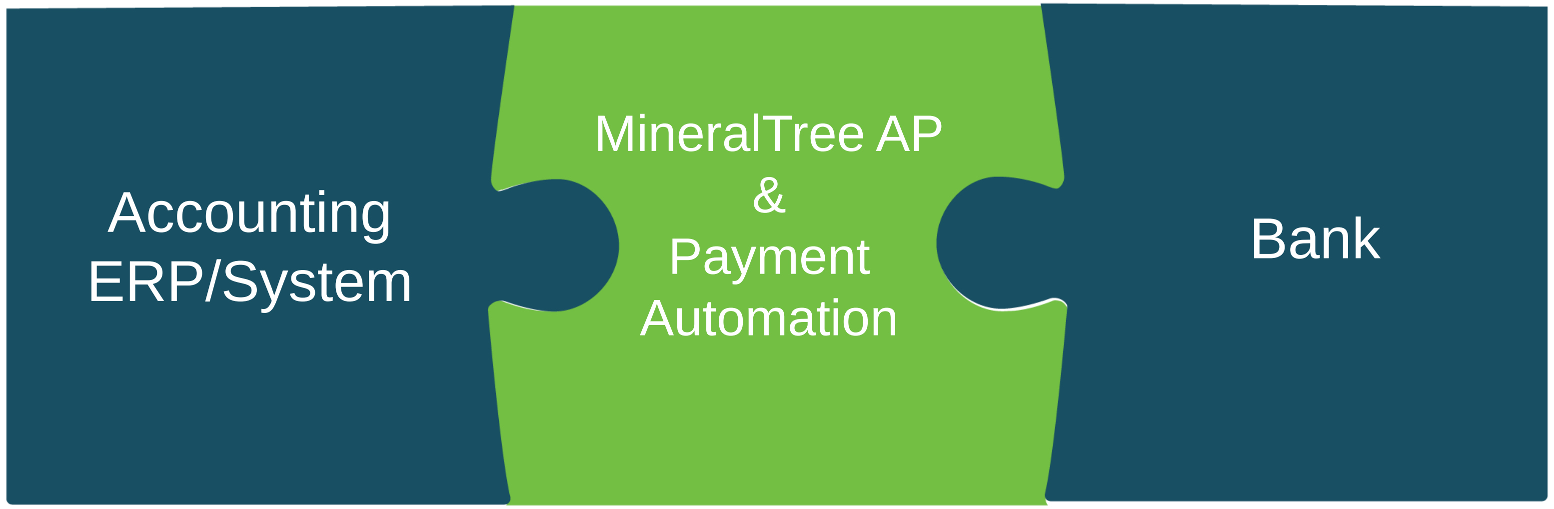
Signs It's Time To Automate

- High volume of invoice/payments (50+/month)
- Considering hiring to keep up with volume
- Accounting team struggling to find time to handle more business critical matters
- Distributed entities or locations, making approvals & coding problematic to complete & track
- Concerned with protection against internal, external, and online fraud

Polling Question 4

- Do you plan to introduce automation to your AP processes?
  - No plans
  - Already have
  - Yes, within 1 year
  - Yes, within 2 years or more

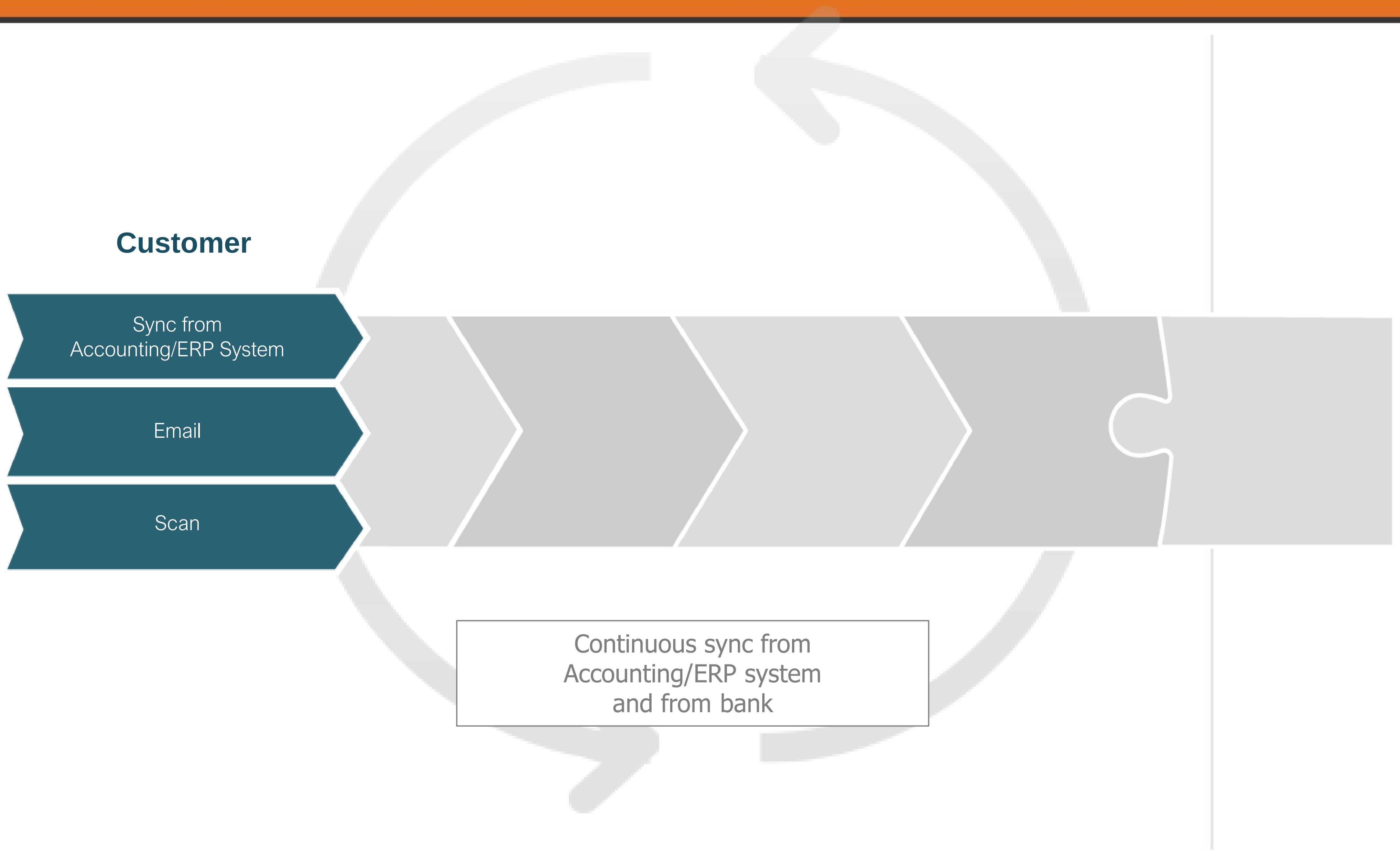
How end-to-end AP Automation works



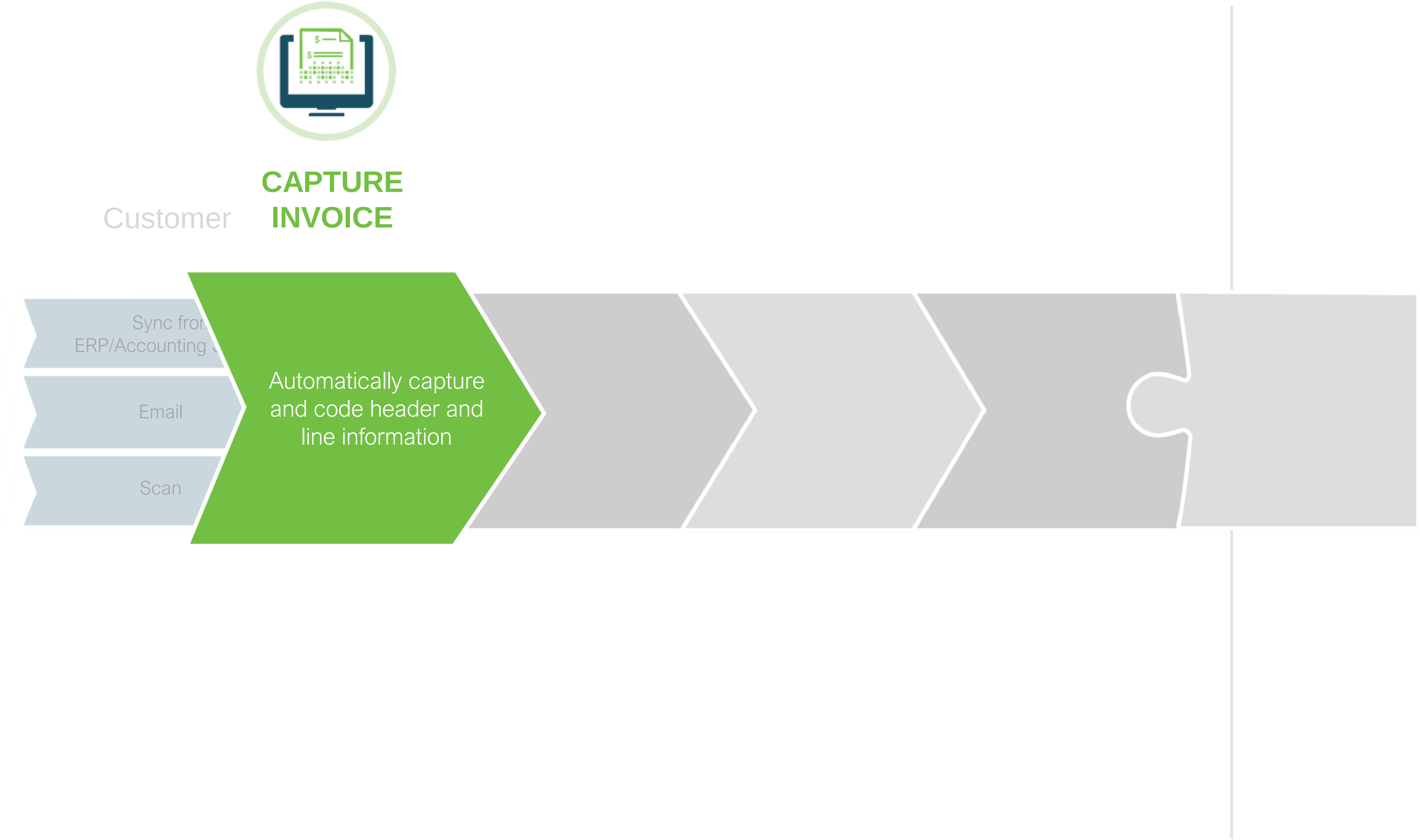
Microsoft Dynamics GP | xero | NETSUITE | CALIBER SOFTWARE

intuit quickbooks | sage 50 | sage 100 | sage Intacct

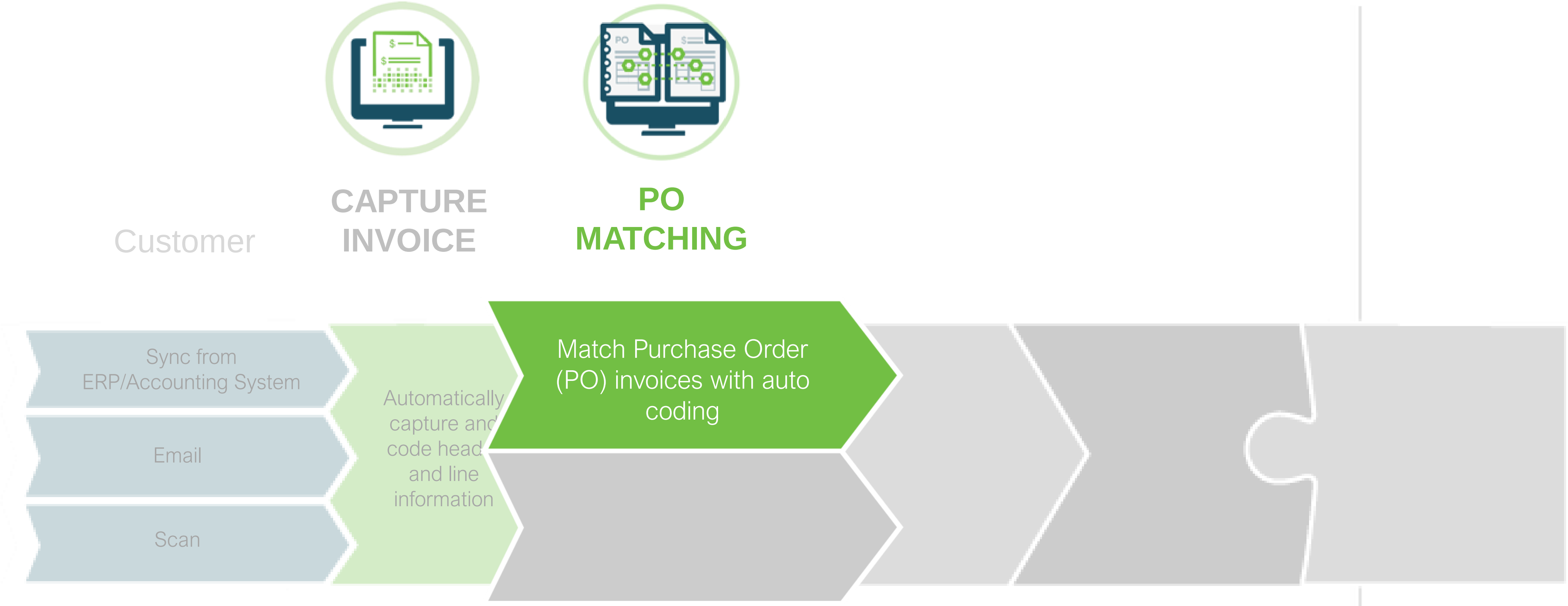
How end-to-end AP Automation works



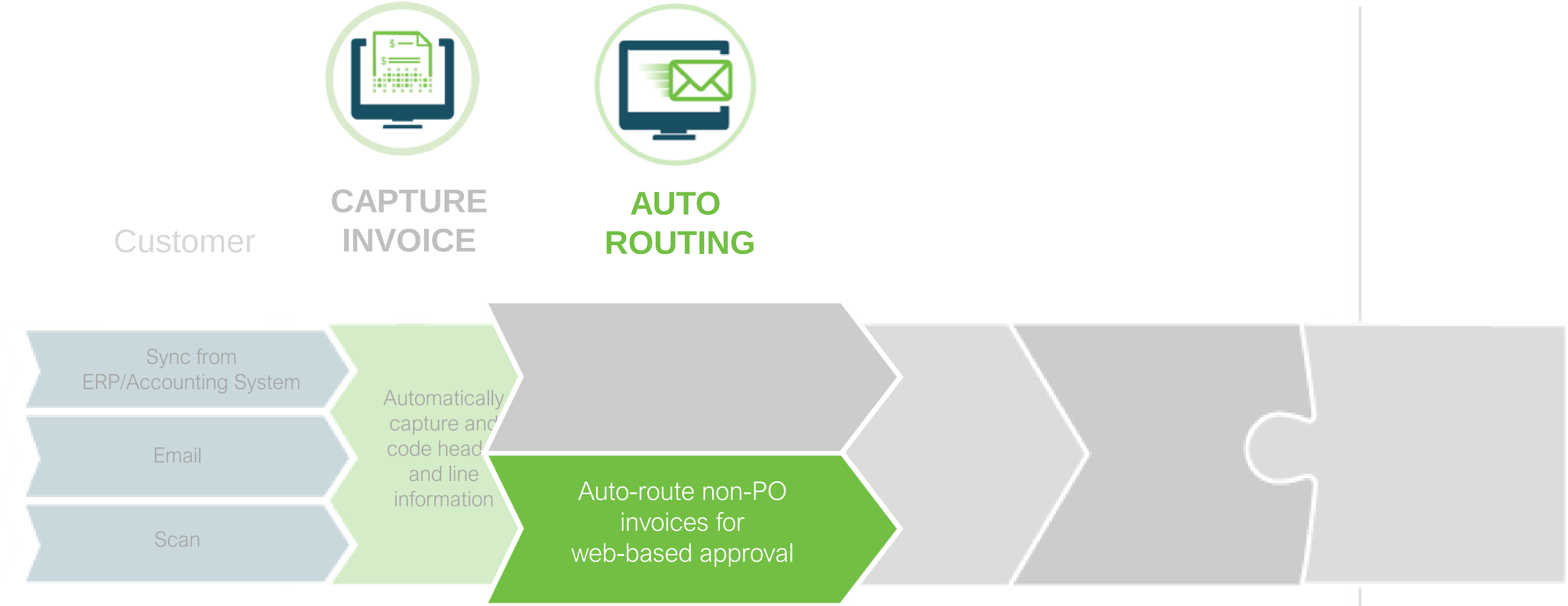
How end-to-end AP Automation works



How end-to-end AP Automation works

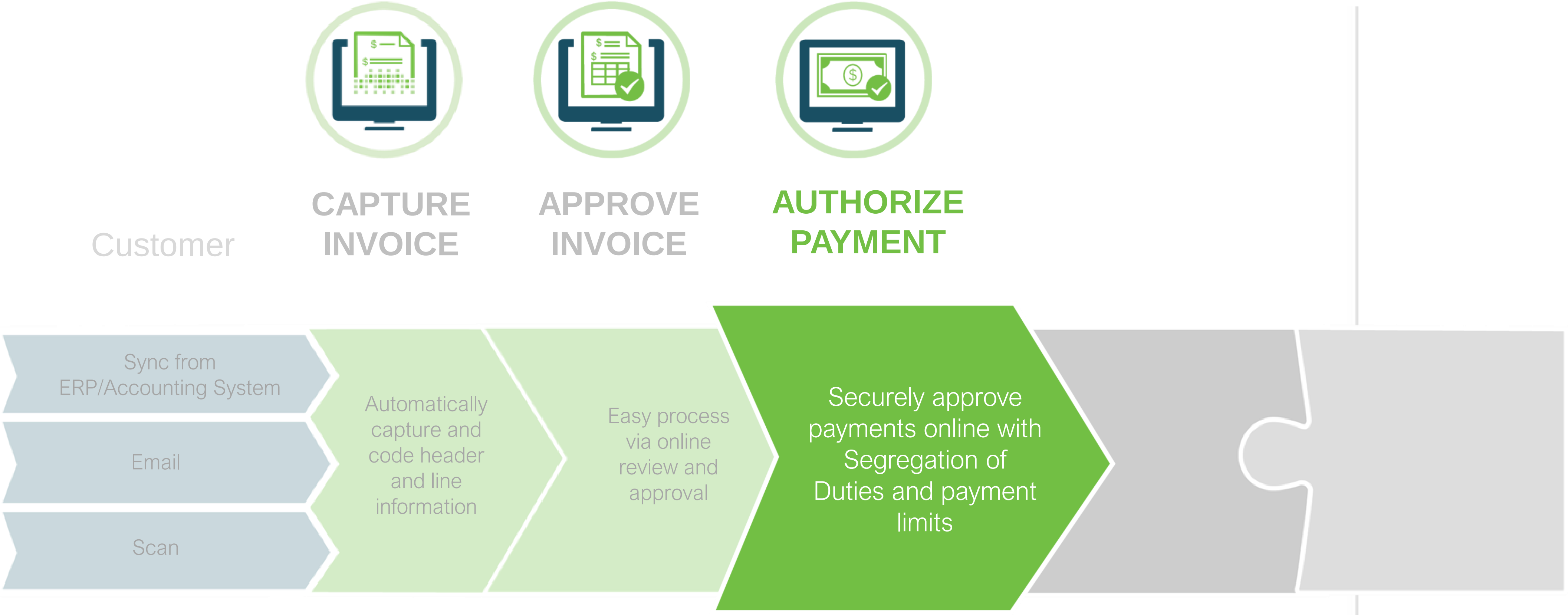


How end-to-end AP Automation works

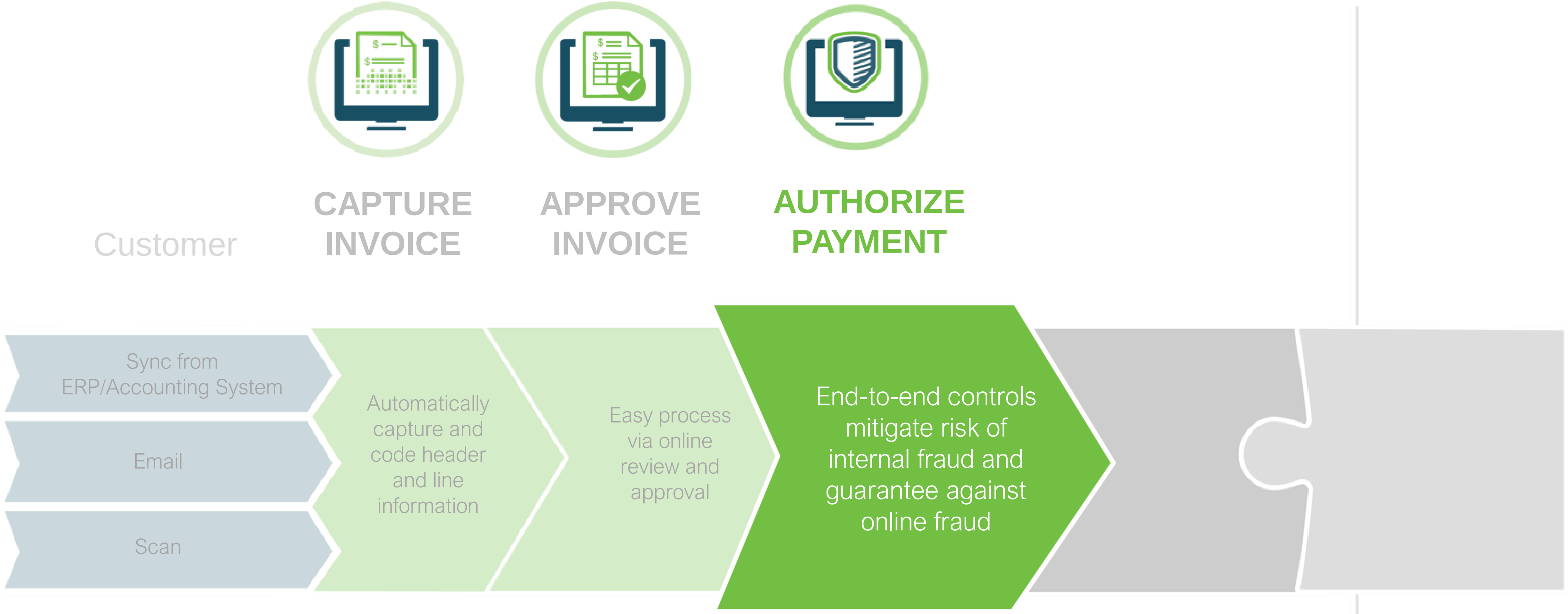


How end-to-end AP Automation works

How end-to-end AP Automation works



How end-to-end AP Automation works



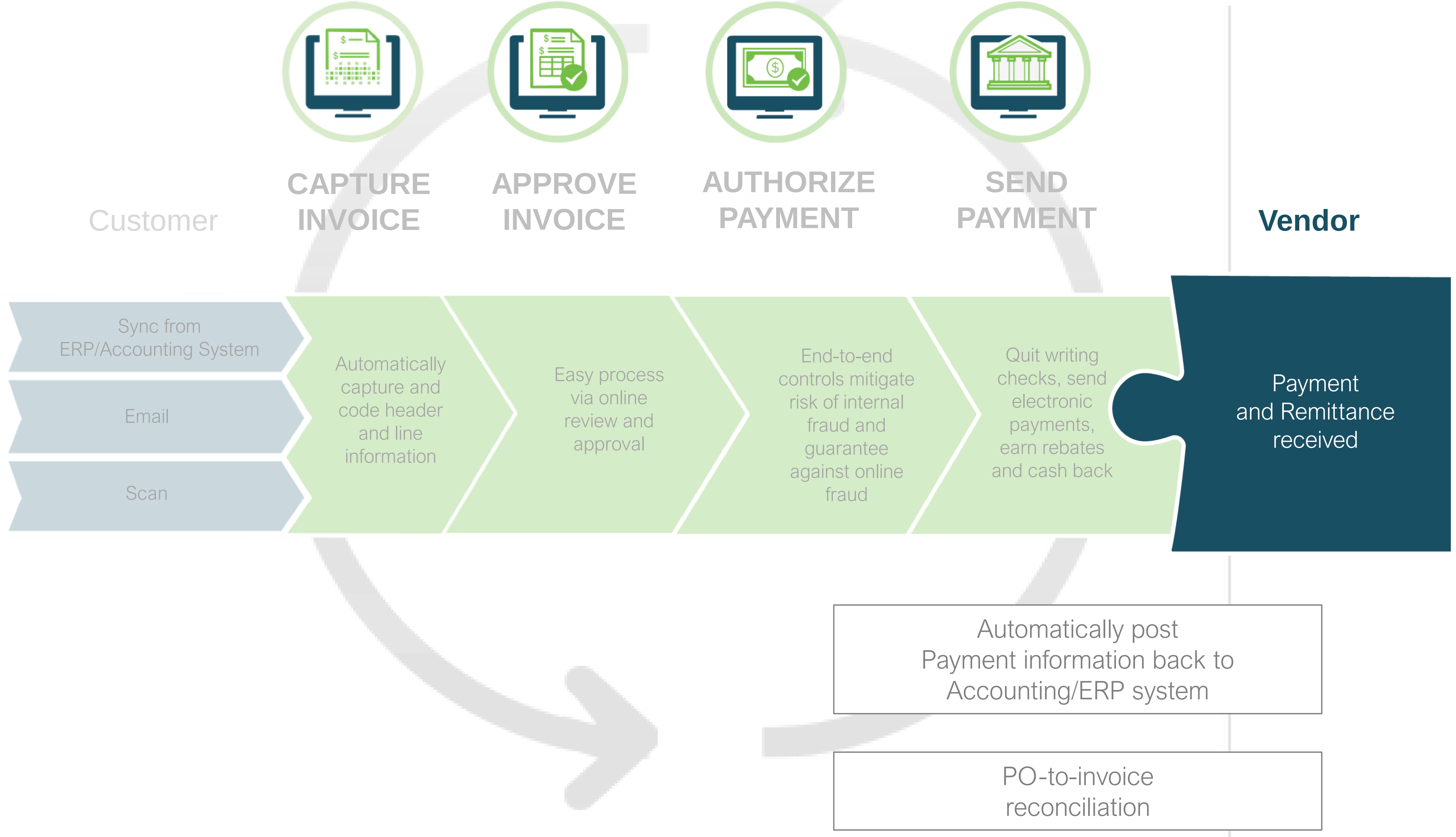
How end-to-end AP Automation works

How end-to-end AP Automation works

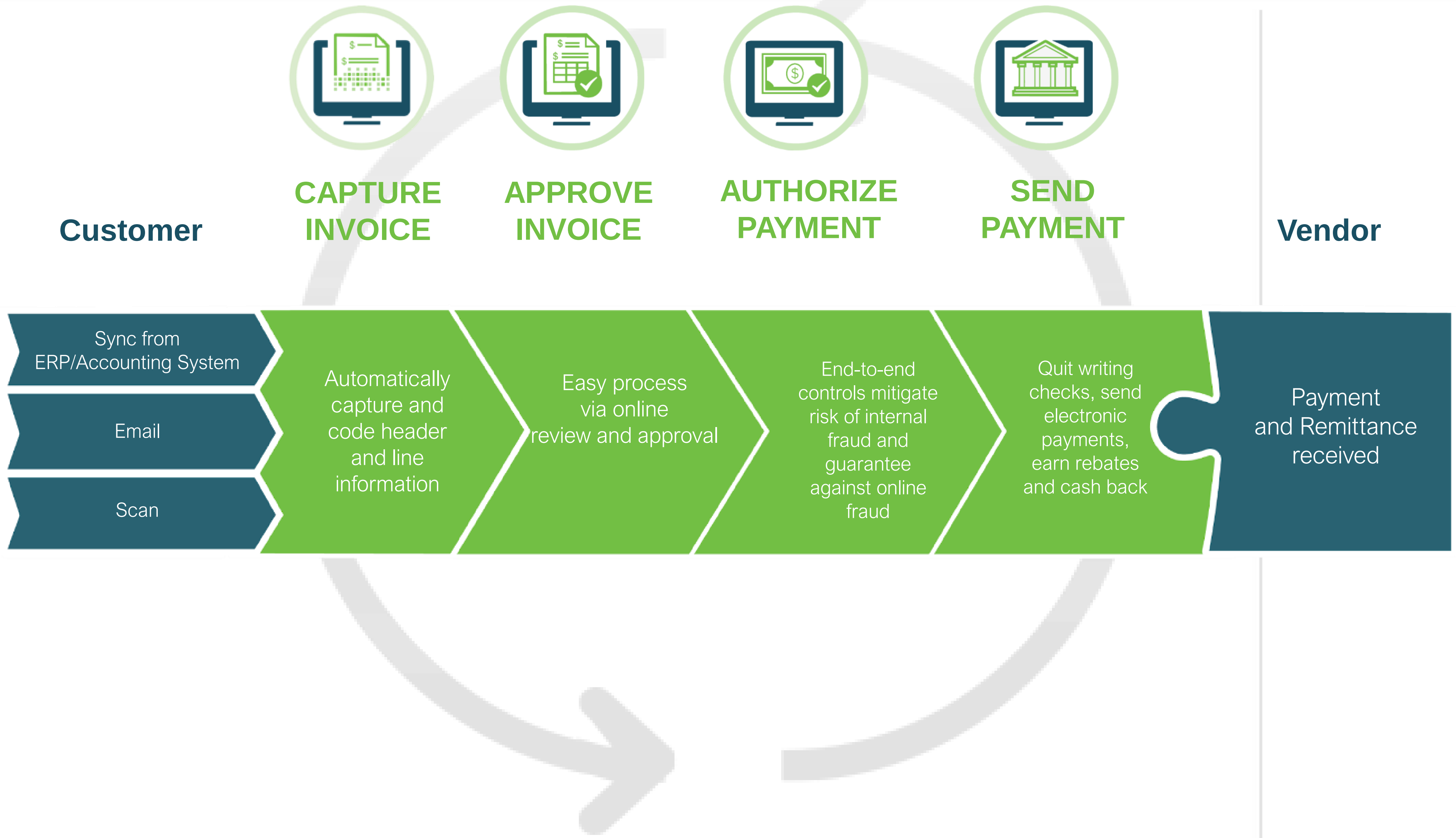
Customer

Customer	CAPTURE INVOICE	APPROVE INVOICE	AUTHORIZE PAYMENT	SEND PAYMENT
Sync from ERP/Accounting System Email Scan	Automatically capture and code header and line information	Easy process via online review and approval	End-to-end controls mitigate risk of internal fraud and guarantee against online fraud	Quit writing checks, send electronic payments, earn rebates and cash back

How end-to-end AP Automation works



How end-to-end AP Automation works



Thank You & Questions

Want to learn more about MineralTree?

Email: info@mineraltree.com
Visit: MineralTree.com (chat now)