



# AP Payment Testing Memo

<b>Client</b>	Meridian Capital Group, LLC
<b>Period</b>	FY 2025 (January 1 – December 31, 2025)
<b>Source Document</b>	AP Payment Register — FY2025 Export
<b>Source File</b>	meridian_ap_fy2025.csv
<b>Source Context</b>	Exported from Meridian ERP (QuickBooks Enterprise) on Jan 15, 2026
<b>Reference</b>	APT-2026-0302-143
<b>Prepared</b>	2nd March 2026

## I. Scope

---

Source ... AP Payment Register – FY2025 Export (meridian\_ap\_fy2025.csv)  
Period Tested ... FY 2025 (January 1 – December 31, 2025)  
Total Payments Tested ..... 710  
Tests Applied ..... 13  
Data Quality Score ..... 94%

The automated AP payment testing procedures documented in this workpaper were performed on the accounts payable payment detail provided by management for the period under examination. These procedures are designed to identify potential data anomalies that may warrant further investigation by the engagement team. The analysis was performed with reference to the FASB Accounting Standards Codification and applicable professional auditing standards.

## Proof Summary

Metric	Value
Data Completeness	94%
Column Confidence	92%
Tests Executed	13
Tests Clear	0
Items for Review	91

## II. Methodology

---

The following automated tests were applied to the AP payment register in accordance with professional auditing standards (ISA 240, ISA 500, PCAOB AS 2401):

Test	Tier	Description
Exact Duplicate Payments	Structural	Identifies payments with identical vendor, invoice number, amount, and payment date.
Missing Critical Fields	Structural	Flags payments missing vendor name, amount, or payment date.
Check Number Gaps	Structural	Flags gaps in sequential check numbering that may indicate voided or missing payments.
Round Dollar Amounts	Statistical	Flags payments at round dollar amounts that may indicate estimates or manipulation.
Payment Before Invoice	Structural	Flags payments made before the invoice date, indicating prepayment errors or fraud.
Fuzzy Duplicate Payments	Statistical	Flags payments to the same vendor with matching amounts on different dates within a window.
Invoice Number Reuse	Structural	Flags invoice numbers that appear across multiple vendors, indicating possible fraud.

Test	Tier	Description
Unusual Payment Amounts	Statistical	Uses z-score analysis to identify statistically unusual amounts per vendor.
Weekend Payments	Structural	Flags payments processed on weekends, indicating unauthorized or unusual activity.
High-Frequency Vendors	Statistical	Flags vendors receiving an unusually high number of payments in a single day.
Vendor Name Variations	Statistical	Flags similar vendor names that may indicate ghost vendors or deliberate misspellings.
Just-Below-Threshold	Advanced	Flags payments just below approval thresholds and same-vendor same-day splits.
Suspicious Descriptions	Advanced	Flags payments with descriptions containing fraud indicator keywords.

**Interpretive Context:** The results presented herein reflect automated data analytics and are intended to support, not replace, professional judgment. Identified anomalies may indicate areas requiring additional inquiry but do not, in themselves, constitute evidence of error, fraud, or material misstatement. The engagement team should evaluate each flagged item in the context of the overall engagement risk assessment and perform corroborating procedures as deemed necessary under applicable professional standards.

### III. Results Summary

Composite Risk Score ..... 24.7 / 100  
Risk Tier ..... ELEVATED  
Total Payments Flagged ..... 91  
Overall Flag Rate ..... 12.8%  
High Severity Flags ..... 11  
Medium Severity Flags ..... 27  
Low Severity Flags ..... 53

Test	Flagged	Rate	Severity
Round Dollar Amounts	34	4.8%	LOW
Weekend Payments	11	1.5%	LOW
Check Number Gaps	8	1.1%	LOW
Vendor Name Variations	7	1.0%	MEDIUM
Fuzzy Duplicate Payments	6	0.8%	MEDIUM
Missing Critical Fields	5	0.7%	MEDIUM
Just-Below-Threshold	5	0.7%	HIGH
Unusual Payment Amounts	4	0.6%	MEDIUM
Payment Before Invoice	3	0.4%	HIGH
Suspicious Descriptions	3	0.4%	MEDIUM
Exact Duplicate Payments	2	0.3%	HIGH
High-Frequency Vendors	2	0.3%	MEDIUM

Test	Flagged	Rate	Severity
Invoice Number Reuse	1	0.1%	HIGH

#### IV. Key Findings

1. 2 exact duplicate payments totaling \$14,200 to vendor 'Apex Office Solutions'
2. 3 payments processed before invoice date — potential prepayment fraud
3. 1 invoice number reused across vendors 'Metro Supplies' and 'Metro Supply Co.'
4. 5 payments just below \$10,000 approval threshold on same dates

#### V. Authoritative References

Body	Reference	Topic	Status
FASB	ASC 405-20	Liabilities — Extinguishments of Liabilities	Current
FASB	ASC 450-20	Contingencies — Loss Contingencies	Current

#### VI. Conclusion

Based on the automated AP payment testing procedures applied, the AP payment register exhibits an ELEVATED risk profile. Select flagged payments should be reviewed for proper authorization and documentation.

Paciolus Intelligence • Generated 02 Mar 2026 00:52 UTC • Meridian Capital Group, LLC • Period: FY 2025 (January 1 – December 31, 2025)

This memo documents automated AP payment testing testing procedures per ISA 240 (Fraud), ISA 500 (Audit Evidence), and PCAOB AS 2401. Results represent data anomalies identified through analytics and are not conclusions regarding internal control effectiveness, fraud, or material misstatement risk. The auditor must evaluate each flagged item in the context of the engagement and perform additional procedures as necessary per professional standards. This memo does not constitute audit evidence sufficient to support an opinion without corroborating procedures. Generated by Paciolus — Zero-Storage Audit Intelligence.