

Audit Report: latest_audit_report

Report Information

Report ID:	latest_audit_report
Audit Date:	2025-03-18 22:31
Audit Type:	Manual
Department:	All
Period:	2025-02-16 to 2025-03-18

Audit Summary

AI Analysis Insights

Forensic Financial Audit Finding: IT Department Transactions - Potential Anomalies

Date: October 26, 2023

Subject: Analysis of Flagged IT Department Transactions

Executive Summary: An analysis of 67 flagged IT department transactions revealed several potentially anomalous patterns requiring further investigation. The most concerning issues revolve around high-value transactions, unusual payment methods (particularly cash), and inconsistencies in risk scores. While not all anomalies indicate fraud, their presence warrants a comprehensive review to ensure compliance and proper financial controls.

1. Most Serious Potential Issues:

* **High-Value Transaction with Unconventional Payment Method:** Transaction TRX-004720 (\$22,675.16) paid to Vendor I via *check*. The use of check for such a substantial IT-related purchase raises immediate concerns and should be reviewed. This contrasts with smaller transactions to Vendor I. * **High Value Wire Transfers:** TRX-007370 (\$15,823.86) paid to Vendor D via wire transfer stands out. This should be reviewed as the highest wire transfer. * **Cash Payments:** A concerning number of transactions were paid in cash, especially considering the IT Department's reliance on electronic systems and vendors. Cash payments are inherently difficult to track and control, making them a common method in fraudulent schemes. This includes: * TRX-009744 (\$1017.26) to Vendor H * TRX-001010 (\$1334.24) to Vendor C * TRX-004505 (\$1414.59) to Vendor F * TRX-004908 (\$8528.84) to Vendor H * **High Risk Score Transactions:** Transactions with risk scores above 70 warrant immediate inspection. These include TRX-001010 (77.01), TRX-007708 (74.37), TRX-008905 (73.52) and TRX-000545 (79.58). * **Inconsistencies in Risk Scores:** Seemingly similar transactions with widely varying risk scores suggest issues with the risk assessment methodology or potential manipulation. For example, small transactions to Vendor C have higher risk scores than larger transactions to the same vendor.

2. Common Patterns Among Flagged Transactions:

* **Department Focus:** All flagged transactions originate from the IT department. This suggests a department-specific issue, rather than a company-wide problem (although this cannot be confirmed without further review). * **Vendor Concentration:** Several vendors (Vendor D, Vendor H, Vendor I, Vendor B, Vendor G and Vendor C) appear frequently in the flagged transactions, indicating a need to scrutinize the relationships and payment history with these specific entities. Vendor H is particularly concerning, appearing in numerous cash payment transactions. * **Payment Method Discrepancies:** The inconsistent use of payment methods for similar types of transactions (e.g., some IT services paid via electronic payment, others via cash) is a recurring pattern. * **Timing Anomalies:** Transactions are largely concentrated within February and March 2025. Investigating the business activities during this specific period may reveal relevant insights. * **Risk Score Variability:** Risk scores are applied inconsistently, necessitating a review of the risk scoring methodology. * **Vendor Variation:** Some vendors have low-value transactions and others have high-value transactions.

****3. Recommendations for Further Investigation:****

* **Detailed Review of Vendor Relationships:** Conduct thorough background checks on Vendor A through Vendor J and Unusual Vendor 15, including verification of addresses, ownership, and business activities. Verify that these vendors are legitimate and not shell companies. * **Voucher Verification:** Obtain original invoices and supporting documentation for all flagged transactions. Verify the accuracy of the amounts, dates, and descriptions, and compare them to the approved purchase orders and receiving reports. * **Employee Interviews:** Conduct interviews with the IT department staff involved in the procurement and payment processes to understand their roles and responsibilities, and to gather information about the transactions in question. * **Review of Internal Controls:** Evaluate the effectiveness of the IT department's internal controls related to procurement, payment, and risk management. Identify any weaknesses or gaps that may have contributed to the anomalies. * **Payment Method Analysis:** Perform a comprehensive analysis of all payments made to the flagged vendors, focusing on the selection and authorization of payment methods. * **Risk Scoring Methodology Review:** Review the risk scoring system and determine if manipulation has occurred, and to understand the proper protocols.

****4. Possible Non-Fraudulent Explanations for Anomalies:****

* **Emergency Purchases:** The increased activity in February and March 2025 may be due to unforeseen IT needs or emergencies. These needs could also explain the cash payments. * **Vendor Payment Preferences:** Some vendors may have specific payment preferences, such as cash discounts or wire transfer requirements. * **Decentralized Procurement:** A lack of centralized procurement processes within the IT department could lead to inconsistent payment methods and pricing. * **Data Entry Errors:** Some anomalies may be due to simple data entry errors during the transaction recording process. * **Inadequate documentation:** Lack of adequate record-keeping may lead to the use of cash and other unusual payment methods. * **New Vendor relationship:** The vendor that is only seen once may be a new relationship with the company. * **Oversight:** Perhaps, there is no fraudulent activity and proper controls were overlooked.

****Conclusion:**** The flagged transactions warrant further investigation to determine the root cause of the anomalies and to assess the potential for fraud or other financial misconduct. Addressing the identified control weaknesses and implementing appropriate preventative measures will help mitigate the risk of future irregularities and ensure the integrity of the IT department's financial operations.

Flagged Transactions

Showing 50 of 80 flagged transactions

Transaction Id	Date	Amount	Department	Risk Score
----------------	------	--------	------------	------------

TRX-003285	2025-02-25T22:30:04.400	95.1374435269	IT	60.0951394238
TRX-009744	2025-03-15T22:30:04.400	1017.2560240598	IT	50.7212412596
TRX-001214	2025-03-18T22:30:04.400	135.0039070549	IT	36.6551154453
TRX-000075	2025-02-21T22:30:04.400	562.4803922351	IT	31.3067745293
TRX-008252	2025-02-25T22:30:04.400	480.5138707634	IT	42.8459806136
TRX-000821	2025-03-01T22:30:04.400	130.8012322761	IT	68.1741187821
TRX-009307	2025-03-01T22:30:04.400	54.2987717524	IT	32.813327177
TRX-001010	2025-02-22T22:30:04.400	1334.2409958409	IT	77.0082915216
TRX-005220	2025-03-01T22:30:04.400	78.9762422412	IT	53.4768144056
TRX-005461	2025-03-12T22:30:04.400	610.5811962584	IT	42.9665618706
TRX-000456	2025-02-19T22:30:04.400	837.9623702247	IT	51.8657683907
TRX-004720	2025-02-19T22:30:04.400	22675.1570570663	IT	49.8068368122
TRX-007976	2025-02-19T22:30:04.400	458.1174993004	IT	8.9558102218
TRX-006656	2025-03-05T22:30:04.400	385.9839436391	IT	49.8727390628
TRX-004505	2025-02-23T22:30:04.400	1414.5908721592	IT	57.1536718667
TRX-002006	2025-02-19T22:30:04.400	29.0428105481	IT	52.8620166646
TRX-001644	2025-02-23T22:30:04.400	271.7906441957	IT	35.6217909926
TRX-000691	2025-02-21T22:30:04.400	502.2101782496	IT	39.7157804947
TRX-000850	2025-03-04T22:30:04.400	333.1342835145	IT	46.9958983647
TRX-003193	2025-02-20T22:30:04.400	383.9051802835	IT	38.1712247926
TRX-007115	2025-03-07T22:30:04.400	1118.2628007953	IT	37.9161121945
TRX-003617	2025-02-21T22:30:04.400	693.2538901668	IT	65.043713148
TRX-004299	2025-02-25T22:30:04.400	143.0849726403	IT	44.3626820736
TRX-000547	2025-02-25T22:30:04.400	1446.463997341	IT	28.6456979662
TRX-007708	2025-03-01T22:30:04.400	942.0411525467	IT	74.3733488277
TRX-009458	2025-02-22T22:30:04.400	69.0508141555	IT	40.6398839944
TRX-000945	2025-02-19T22:30:04.400	72.4763912107	IT	49.0596373085
TRX-006869	2025-03-15T22:30:04.400	321.0842178367	IT	43.1269025741
TRX-005838	2025-02-28T22:30:04.400	242.1422572595	IT	71.1254525152
TRX-008438	2025-03-01T22:30:04.400	1143.5113113864	IT	52.5779193323
TRX-003955	2025-02-21T22:30:04.400	1131.3290573173	IT	53.3228060724
TRX-006970	2025-03-01T22:30:04.400	1337.6748980481	IT	45.0621772121
TRX-007504	2025-03-07T22:30:04.400	299.5250380333	IT	26.0198195209
TRX-000164	2025-02-17T22:30:04.400	274.1475525543	IT	40.414229489
TRX-007348	2025-03-03T22:30:04.400	406.6146683086	IT	45.1893772114

TRX-007266	2025-03-14T22:30:04.400	1220.549252394	IT	51.6144787847
TRX-001025	2025-02-24T22:30:04.400	228.3275540445	IT	50.069254142
TRX-007616	2025-03-03T22:30:04.400	56.8502331295	IT	50.9653404375
TRX-002067	2025-02-25T22:30:04.400	83.2329767309	IT	52.5547996316
TRX-006277	2025-02-21T22:30:04.400	118.8923943658	IT	46.6736645095
TRX-000545	2025-02-28T22:30:04.400	355.8824177644	IT	79.5795158151
TRX-008856	2025-02-19T22:30:04.400	66.1426575182	IT	52.6490792635
TRX-000957	2025-02-23T22:30:04.400	610.3882700948	IT	57.8325475643
TRX-007330	2025-02-20T22:30:04.400	270.2011330381	IT	38.2749074811
TRX-001433	2025-03-15T22:30:04.400	260.207465132	IT	41.749513079
TRX-005050	2025-02-19T22:30:04.400	81.1640505319	IT	38.1841305789
TRX-000367	2025-02-20T22:30:04.400	133.8882387262	IT	37.161298915
TRX-009875	2025-03-16T22:30:04.400	853.7129261505	IT	71.0559890877
TRX-009163	2025-02-22T22:30:04.400	236.2436551256	IT	58.4125704082
TRX-001705	2025-03-03T22:30:04.400	1187.8285586023	IT	33.0241928987

Generated on: 2025-03-18 22:36:37