SKYWIND
Software Group

Business and Fraud Treasure Hunting (TH)Report

Date: 18/06/2025

Cases Exposed:

- Retroactively created PO by vendor invoice date
- Purchase Orders in Open Status over 60 Days
- Modified Vendor Bank Account
- Purchase Orders Approved by Creator
- Exceptional posting by GL Account

Alert Name:

Retroactively created PO by vendor invoice date

History Scanned:

last 30 days

Alert Business Meaning:

Retroactively creating a Purchase Order (PO) by the vendor invoice date means generating the PO after the goods or services have been delivered, using the invoice date as the PO date. This practice is typically used to align procurement documentation with actual delivery or invoicing timelines, but it may raise compliance or audit risks if not properly controlled.

Possible Business/Fraud Impact:

Retroactively creating POs can lead to compliance violations, misstated financials, and process integrity issues, making it harder to ensure proper authorization and budget control. From a fraud perspective, it opens the door to backdating transactions to bypass approval workflows, conceal unauthorized purchases, or manipulate financial reporting periods.

What was found (excerpt):

Purchasing Document	Item	Posting Date	Creation Date	Vendor	Description purchasing group	Amount	Invoice Document No.
4100056687	00010	2025/05/14	2025/05/19	2008304	Service	20,384.62	5105735839
4100056687	00030	2025/05/14	2025/05/19	2008304	Service	20,384.62	5105735839
4100056687	00040	2025/05/14	2025/05/19	2008304	Service	20,384.62	5105735839
4100056687	00050	2025/05/14	2025/05/19	2008304	Service	20,384.62	5105735839
4100056513	00020	2025/05/19	2025/05/20	2000751	Service	271,034.00	5105736346
4100056513	00030	2025/05/19	2025/05/20	2000751	Service	40,310.00	5105736348
4100056513	00010	2025/05/19	2025/05/20	2000751	Service	271,950.01	5105736349

Alert Name:

Purchase Orders in Open Status over 60 days

History Scanned:

last 365 days

Alert Business Meaning:

When purchase orders remain open for extended periods, it can indicate delivery delays, vendor performance issues, process inefficiencies, or potential financial exposure that requires management attention.

Possible Business Bottleneck Impact:

Excessive open purchase order aging and poor completion rates reveal critical procurement bottlenecks that disrupt operations, delay production, and cause material shortages. These delays weaken vendor performance due to poor follow-up and strained communication, leading to reduced procurement leverage. Financial exposure increases as uncertain delivery timelines complicate cash flow planning, inflate open liabilities, and create disputes over incomplete deliveries. Compliance also suffers, with weak audit trails, segregation of duties risks, and poor contract tracking undermining control. Unresolved purchase order issues slow procurement processes, damage supplier relationships, and expose the organization to operational, financial, and compliance risks.

What was found (excerpt):

Purchasing Document	Vendor	Material	Material Description	Purchase Order Date	Scheduled Qty	Delivered Qty
4200004281	2001187	7347859	COLD_SAW_BLADE_450X3.0X50MMX180_TEETH	2025/03/31	10.000	0.000
4200004281	2001187	7348309	SAW_COLD_450X4X160_TEETH_TiCN	2025/03/31	10.000	0.000
4200004281	2001187	7347857	COLD_SAW_BLADE_400X2.5X50MMX240_TEETH	2025/03/31	15.000	0.000
4200004281	2001187	7343567	COLD SAW BLADE 450X4.0MMX140 TEETH TiCN	2025/03/31	10.000	0.000
4200003895	3888840	7900000	MCL- WELD HOLE DETECTOR	2024/12/02	1.000	0.000
4200004315	2001130	1000045	R/C PAINT-TEX-DC-TOP-CHOCOLATE	2025/04/09	6,650.000	0.000
4200004315	2001130	1000043	R/C PAINT-TEX-DC-TOP-BRICK RED	2025/04/09	6,840.000	0.000

Alert Name:

Modified Vendor Bank Account

History Scanned:

last 365 days

Alert Business Meaning:

A modified vendor bank account refers to changes made to the bank details associated with a supplier in the procurement or finance system. This is typically done to update payment information for legitimate reasons, such as a vendor changing banks or account number but in some cases may indicate fraudulent activity.

Possible Business/Fraud Impact:

If not properly verified, a modified vendor bank account can be a major fraud risk, potentially redirecting payments to unauthorized accounts. Fraudsters may exploit weak controls to alter payment details and divert funds. Even legitimate changes, if poorly communicated, can result in payment delays, strained vendor relationships, and operational disruptions. Incorrect or unauthorized changes may also trigger compliance violations and audit findings. Overall, failure to secure and validate vendor bank modifications exposes the organization to financial loss, reputational damage, and regulatory penalties.

What was found (excerpt):

Vendor ID	Field name	Field Description	Previous Value	Current Value	Date	Table name
0002001218	BANKL	Bank Key	11-032	11-000	2024/07/04	LFBK
0002000905	BANKN	Bank Account	1643770131	1000152575	2024/07/04	LFBK
0002011731	BANKN	Bank Account	0100012585661	0102446298100	2024/07/15	LFBK
0002011731	BANKL	Bank Key	31-034	02-084	2024/07/15	LFBK
0002011714	BANKN	Bank Account	1323936726	00602860-0011	2024/07/16	LFBK
0002011714	BANKL	Bank Key	01-308	NBADEGCAPSU	2024/07/16	LFBK
0002011766	BANKL	Bank Key	14-007	07-000	2024/07/24	LFBK
0002000819	BANKN	Bank Account	500167741201	00500167741201	2024/08/05	LFBK

Alert Name:

Purchase Orders Approved by Creator

History Scanned:

last 30 days

Alert Business Meaning:

Purchase Orders approved by their creator occur when the same individual both initiates and approves a purchase order. This usually happens in systems with weak controls or small teams but creates a conflict of interest by bypassing independent review.

Possible Business/Fraud Impact:

Allowing creators to approve their own POs increases the risk of unauthorized or fraudulent purchases. It eliminates the critical control of segregation of duties, making it easier to conceal inappropriate spending. This practice may lead to budget overruns, unapproved commitments, and purchases from non-compliant vendors. Audit trails become unreliable, raising red flags during internal or external reviews. Ultimately, it exposes the organization to financial loss, compliance violations, and reputational risk.

What was found (excerpt):

Purchasing Document	Company Code	Purchasing Document Type	Purch. Doc. Type Description	Created On	Vendor	Purchasing Group	Purchasing Group Description
4100058505	SA02	Z001	Domestic PO	2025/06/18	2008186	004	Consumables
4100058503	SA02	Z001	Domestic PO	2025/06/18	3888840	004	Consumables
4800005307	NA01	Z011	Intercompany PO	2025/06/09	100036	008	SFG & FG
4800005307	NA01	Z011	Intercompany PO	2025/06/09	100036	008	SFG & FG
4100058013	SA02	Z001	Domestic PO	2025/06/10	2008307	008	SFG & FG
4800005326	NA01	Z011	Intercompany PO	2025/06/13	100044	008	SFG & FG
4800005334	NA01	Z011	Intercompany PO	2025/06/16	100036	008	SFG & FG

Alert Name:

Exceptional posting by GL account

History Scanned:

last 7 days

Alert Business Meaning:

Exceptional posting by GL account refers to unusual or irregular transactions recorded in general ledger accounts that deviate from normal business activity. These postings may result from manual adjustments, error corrections, or potentially unauthorized financial entries.

Possible Business/Fraud Impact:

Irregular GL postings can indicate mistakes, process gaps, or intentional manipulation of financial results. Without proper review, such entries may distort financial statements, affecting decision-making and external reporting. Fraudsters may exploit exceptional postings to hide misappropriations or shift expenses improperly. These anomalies often trigger audit findings and regulatory scrutiny, especially if documentation or approvals are missing. Ultimately, exceptional postings without clear justification can expose the business to financial misstatements, compliance failures, and reputational damage.

What was found (excerpt):

Document Number	User (Masked display)	Posting Date	Document Date	Amount	G/L Account	G/L Account Long Text (masked)
4002004327	5v4M6F	2025/06/17	2025/06/17	3,122,902.23	320001600	pPIlc3T5I2l750o
4002004298	eYsGuvs	2025/06/17	2025/06/17	3,482,431.43	320001600	pPIlc3T5I2l750o
4002004250	eYsGuvs	2025/06/17	2025/06/17	2,499,395.60	320001600	pPIlc3T5I2l750o
1000365648	RBXrIl	2025/06/18	2025/06/18	2,307,037.90	370240501	t9Do9cnxLTfaWqQHGCzrlAAAAAAAAAAAAAAAAAAAAAAAAAA
1000365648	RBXrIl	2025/06/18	2025/06/18	2,307,037.90	370240504	1Aok+767YfrIWLjCu--vNAAAAAAAAAAAAAAAAAAAA
4002004327	5v4M6F	2025/06/17	2025/06/17	2,188,725.96	320001600	pPIlc3T5I2l750o
4002004250	eYsGuvs	2025/06/17	2025/06/17	2,523,826.77	320001600	pPIlc3T5I2l750o