SKYWIND
Software Group

Enhance and automate control upon SAP operations

Protect your SAP against
Cyber and Internal Fraud

Skywind Profile

Software

Development of
Skywind Analytical Platform
for SAP Cloud based SAP® related solutions

4C™ + JAM™ + soda™

Solutions

- Design and implementation of SAP Business Intelligence, Performance Management, Planning and Data Warehousing solutions.
- Development, optimization and maintenance of SAP Infrastructure (Basis) incl. SAP upgrades and migrations to HANA On Premises and On Cloud.
- Development, optimization and maintenance of SAP Infrastructure (Basis) incl. SAP upgrades and migrations to HANA On Premises and On Cloud.

Discover Intelligent Platform for SAP Observability, Automation and Control

Business Protection

Prevent fraud and cyber threats.

Business Control

Enhance process efficiency.

Access Governance

Secure and optimize user access.

Jobs Control

Optimize background jobs performance.

Technical Control

Ensure stable infrastructure performance.

S/4HANA Excellence

Post-migration stability assurance.

Protect Your Business, Control Your Processes

The SkyAPS™ Solutions Pool:

Skywind 4C™

to increase the transparency of all SAP activities by enhancing control upon business and technical events and processes

to identify fraud, reveal problems and bottlenecks earlier, to protect against cyber threats

to prevent unwanted outcomes and quickly compensate the damage by diminishing the consequences and restraining further risks

Skywind JAM™

to gain visibility, agility, better management, analysis and control of SAP background jobs

Skywind SoDA™

to analyze and monitor your segregation of duties, perform in-depth authorizations analysis and inform you in real time about corresponding suspicious activities

Solutions and Content

SKYWIND ANALYTICAL PLATFORM FOR SAP

✔ Analytics ✔ Monitoring ✔ Alerting ✔ Smart Data Distribution

4C™

- Fraud & Cyber detection
- Business Processes monitoring
- Infrastructure, Communications, Interfaces monitoring
- Business Warehouse monitoring

JAM™

- Background Jobs analysis and monitoring
- Background Jobs management and optimization

soda™

- Segregation of Duties (SoD) analysis and monitoring
- Authorizations analysis and monitoring

YOUR SAP

S/4HANA · ECC · BW · CRM · SRM

Skywind Selected Customers

Solutions and Content

- **Skywind 4C™ Anti Fraud and Cyber Pack**
  for ultimate SAP protection against cyber attacks and internal fraud
- **Skywind 4C™ Business Bottlenecks Pack**
  for superior business control and transparency
- **Skywind 4C™ Basis and Infrastructure Pack**
  for continuous validation of SAP technical consistency and performance
- **Skywind 4C™ Business Warehouse (BW) Pack**
  for smooth BW operation and maintenance
- **Skywind 4C™ Generator**
  for instant, no-code creation of your own controls and reports
- **Skywind SoDA™ SoD and Authorizations Violations Analysis**
  – to eliminate and prevent SoD violations and protection against internal fraud
- **Skywind JAM™ Analysis and Control**
  to analyze, control and optimize all SAP Background Jobs activities
- **Skywind Security and Administration App.**
  Internal application for ultimate control of platform usage

info@skywind.com | www.skywind.com

Skywind 4C™ Anti Fraud and Cyber Pack

for Ultimate SAP Protection

- Financial Accounting
- Master Data Management
- Stock and Inventory
- Logs Analysis

- Purchasing
- Sales and Logistics
- Cyber
- Integration with SOC / SIEM

01. Financial Accounting – anti fraud controls

EXAMPLES:

Exceptional postings by GL account
Possible misbehavior and fraud

Financial Documents are parked and posted by the same user
SoD violation

Payment advice of One-Time Vendor with regular vendor bank details
Payment clerk fraud

Vendor related accounting document without Purch. Order reference
A wrong purchasing procedure or fraud

Payment except regular incoming payment bank accounts
Incorrect / Fraudulent posting

Sensitive financial transactions usage
Tracked by User/Terminal ID/Transaction/Time/ Duration/IP Address

02. Master Data Management - anti fraud controls

EXAMPLES (by Vendor):

- **GR/IR of PO and Vendor's Master Data was altered by the same user**
  SoD violation and possible fraud
- **Vendor's bank account was changed and in a short period of time the change was reversed**
  Possible fraud
- **Vendor's name / bank account / other vendor's credentials were changed multiple times in a short period**
  Possible fraud
- **Alternative payee was assigned to a vendor**
  A wrong purchasing procedure or possible fraud
- **Inactive / Rarely used vendor with open balance**
  Possible fraud / money loss
- **A new ONE TIME vendor was created**
  Should be tracked for purchasing and financial posting

03. Stock and Inventory – anti fraud controls

EXAMPLES:

Suspicious material movements
Possible case for a merchandize to be stolen

Inappropriate Material conversions
Convert a car to a pencil. Possible case for a merchandize to be stolen

Inventory count - Plant or Single Document level differs from the books statement
Possible theft

High amount inventory variance (booked vs. counted)
Possible theft

Moving average material price changes
Discover misbehavior by side effect

Material price has exceeded the threshold
Discover misbehavior by side effect

04. Purchasing – anti fraud controls

EXAMPLES:

Purchase Order approved by creator
SoD violation and possible fraud

Purchase Requisition approved by creator
SoD violation and possible fraud

PO created retroactively
(after the date placed in Vendor's invoice)
Misbehavior leading to possible money loss or fraud

Vendor's master payment terms differs payment terms in invoice
Misbehavior leading to possible money loss or fraud

Purchase Order for one-time Vendor
Threshold preventing inappropriate purchasing procedure

Over delivery tolerance in PO was changed
Since the Over delivery flag does not trigger a re-approval process, there is a danger of misuse of this flag

05. Sales and Logistics – anti fraud controls

EXAMPLES:

- **Customer's credit limit was changed**
  Possible financial risk exposure
- **Credit Memo monthly vol. by Payer have been exceeded an amount of XX in doc. currency**
  Misbehavior leading to possible money loss or fraud
- **Sales Order pricing conditions were multiplied and/or changed manually**
  Intentional Fraud
- **Returns monthly volume by Sold-To-Party have been exceeded an amount of XX in doc. currency**
  Misbehavior leading to possible money loss or fraud
- **Credit Management Block flag is disabled**
  Suspicious activity leading to a possible fraud
- **Minimum/Maximum Sales Order quantity violation**
  Misbehavior leading to possible money loss or fraud

06. Cyber Controls

EXAMPLES:

Login to the DIALOG user's system using a password and not by using Single Sign ON
Violation of secured Logon

Creating a DIALOG user by NOT authorized parties (not by Authorizations/Basis team)
Cyber related changes made to User Master

Any system update through DEBUG, performed by the SYSTEM / DIALOG user
Unacceptable and dangerous action

Activation of critical SAP Business / Technical processes via transactions
Unsecured transaction start

Activating transactions by unauthorized DIALOG users
Successful run of a transaction even when a user is not authorized to activate it

Notification of granting/receiving critical authorization (e.g., SAP_ALL/SAP_NEW)
Potential to a malicious, unauthorized grant of critical rights in the SAP system

SKYWIND
Software Group

info@skywind.com | www.skywind.com

SAP Logs Monitoring Analysis

Detect anomalies, ensure system security, integrity

Potential Impact: SAP Operational Efficiency and Business Disruptions

EXAMPLES:

SM20: Analysis of Security Audit Log - Details

Impact: unauthorized access attempts, suspicious transactions, user activity patterns, changes to sensitive data

SM20: Analysis of Security Audit Log - Anomalies

Impact: unauthorized access attempts, suspicious transactions, user activity patterns, changes to sensitive data (en masse)

SM21: Analysis of Debugging Log - Details

Impact: program execution, variable values, error messages, program flow, and potential debugging issues

SLG1: Analysis of Application Log - Details

Impact: potential processing bottlenecks, leading to delays in data transmission and potential system instability

SM21: Analysis of System Log - Details

Impact: system errors, warnings, performance issues, background job status, user logon/logout activities

SM21: Analysis of System Log - Anomalies

Impact: system errors, warnings, performance issues, background job status, user logon/logout activities (en masse)

SCU3: Analysis of Change Log (CDHDR / CDPOS)

Impact: changes made to critical data objects, including who made the changes, when they were made, and the old and new values, aiding in audit trails, compliance and data integrity maintenance

DB20: Analysis of DBTABLOG

Impact: detailed records of database table changes, including insertions, updates, deletions, and the associated user information, timestamps, and affected fields

Integration with SOC / SIEM Platforms

BENEFITS: Pushes pre-filtered SAP data instead of raw logs, dramatically reducing SIEM processing costs while providing laser-focused security insights.

Enable SAP insights within your Security Operation Center (SOC)

PROTOCOLS:

Syslog Protocol

Centralized Logging: Centralize logs from various devices, systems, and software applications into a single repository.
Security Monitoring: Used in security information and event management (SIEM) systems

Web Services

Use Case: Synchronize data flows between SAP and Non-SAP systems such as CRM, eCommerce platforms, or custom databases.
Benefit: Ensures consistency and accuracy of data across different systems, improving operational efficiency and reducing errors.

Files Transfers

Impact: Interruptions or errors in file transfers can lead to data loss, incomplete data records, and compliance risks, especially in data-driven decision-making environments

SUPPORTED PLATFORMS:

splunk>
IBM QRadar
Microsoft Sentinel
solarwinds
SECURONIX
exabeam
AlienVault USM Anywhere
LogRhythm
ArcSight

Realise Tangible Benefits

Save Time

Reduce manual effort through an automated business rule engine.

Increase Protection

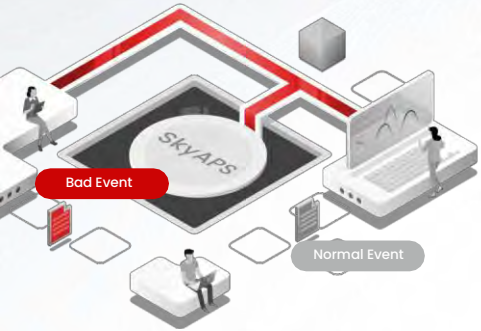
Prevent fraud with proactive alerts and comprehensive insights.

Save Money

Optimize the way you do business by identifying process bottlenecks or violations.

Complete Coverage

Search your entire transactions database versus only a sample achieved during an audit.



To Conclude...

Our software continuously checks the validity of the processes by catching “bad” or “about to become bad” events. Sophisticated data distribution mechanisms seamlessly and securely distribute critical info to the right audiences.

When mission critical data will start flowing securely, yet seamlessly across all organizational levels, timely reaching key users... only then will your company start a journey to the real Business Transformation.

SKYWIND
Software Group

The Science of Data.
The Art of Business.

INFO@SKYWIND.COM

WWW.SKYWIND.COM