# Skopos

ADVANCED RISK ANALYSIS FOR ERP SYSTEMS
BUILT FOR THE AI ERA

MEYLAN TECHNOLOGIES & CONSULTING | December 2025

# Table of Contents


**About Meylan Technologies & Consulting** 2

*Quality, Innovation, and Expertise in SAP Security*

**What is MTC Skopos?** 3

*Advanced Risk Analysis for ERP Systems*

**Reimagining SAP Security** 5

*Why We Built MTC Skopos*

**Practical SAP Security** 7

*A Collaborative Approach to Addressing Segregation of Duties Risks*

**From Data Chaos to Security Intelligence** 9

*Why Flexible Insights Beat Rigid Dashboards*

**AI Meets SAP Security** 12

*How MCP Transforms MTC Skopos*

# About Meylan Technologies & Consulting

**Meylan Technologies & Consulting** delivers SAP services encompassing security, authorization, risk management, and audit, alongside optimizing systems and processes. By integrating profound IT risk and audit proficiency with extensive SAP solutions expertise, we ensure our clients receive the most efficient and effective support.

### Quality First

We are committed to delivering high-quality services and solutions, ensuring reliability, security, and excellence in every project.

### Efficiency & Innovation

We streamline processes and leverage cutting-edge technology to enhance SAP environments, making operations faster, more secure, and more efficient.

### Expertise & Excellence

With years of specialized experience, we provide top-tier SAP Security consulting and software development, ensuring clients receive the best industry practices.

### Customer-Centric Approach

We prioritize our clients' needs, offering tailored solutions that align with their business goals and maximize value.

### Integrity & Trust

We believe in transparent, ethical, and honest partnerships, building long-lasting relationships based on trust and accountability.

### Our Vision

We envision a future where businesses operate seamlessly and securely within their SAP environments, protected from security threats and inefficiencies. By continuously innovating and leveraging our deep expertise, we aim to be a leading partner in SAP Security and digital transformation, delivering solutions that drive long-term success.

# What is MTC Skopos?

Organizations face significant security and compliance challenges when managing user access across complex ERP systems. Without proper monitoring, excessive privileges can create opportunities for fraud, errors, and compliance violations that could damage the company financially and reputationally.

**MTC Skopos** streamlines and accelerates the monitoring process to regain control and reduce risk exposure through:

### Access Risk Monitoring

Knowing who has access to what isn't just best practice: **it is your competitive advantage**

- User & Role Analysis
- Cross-System analysis
- Comprehensive ruleset maintenance

### Access Risk Remediation

Detailed remediation reporting delivers comprehensive analysis and key statistics for remediation planning.

- Deep dive into remediation opportunities
- AI friendly dataset (JSON)
- Identify potential business impact

### User Provisioning

Stopping risks before they enter your system is **smarter than remediation**

- Predictive risk modeling
- Analyze risk impact
- Model compliance effects

### Access Reviews

Understanding your permission landscape is **the intelligence that drives informed security decisions**

- Enhanced access review accuracy
- Streamlined detailed investigation
- Bulk action capabilities

### Role Management

Prevention during design is not just efficient: **it is strategic architecture**

- Simulate role modification impacts
- Analyze downstream effects
- Assess compliance risks

## Core Capabilities

- **Segregation of Duties Analysis:** Identify conflicting access rights across roles and users
- **Users Role Explorer:** Intuitive interface for authorization review

## Advanced Features

- **Cross-System Risk Detection:** Assess risks spanning multiple platforms (SAP, Navision, Odoo)
- **Permission Simulation:** Test authorization changes before production deployment
- **Remediation Reports:** Step-by-step action plans
- **Management Reporting:** Executive-level insights
- **Model Context Protocol AI Agent:** Leverage power of AI for role optimization
- **Did-Do Analysis:** Analyze transactional data and detect if access risks were exploited

## Key Differentiators

- **Performance:** Ultra fast user data processing and fluid UI
- **Portable Desktop App:** No installation required. No Cloud.
- **Privacy First:** Data stays on your local environment
- **Power BI Integration:** Ready-to-use business intelligence

## System Compatibility

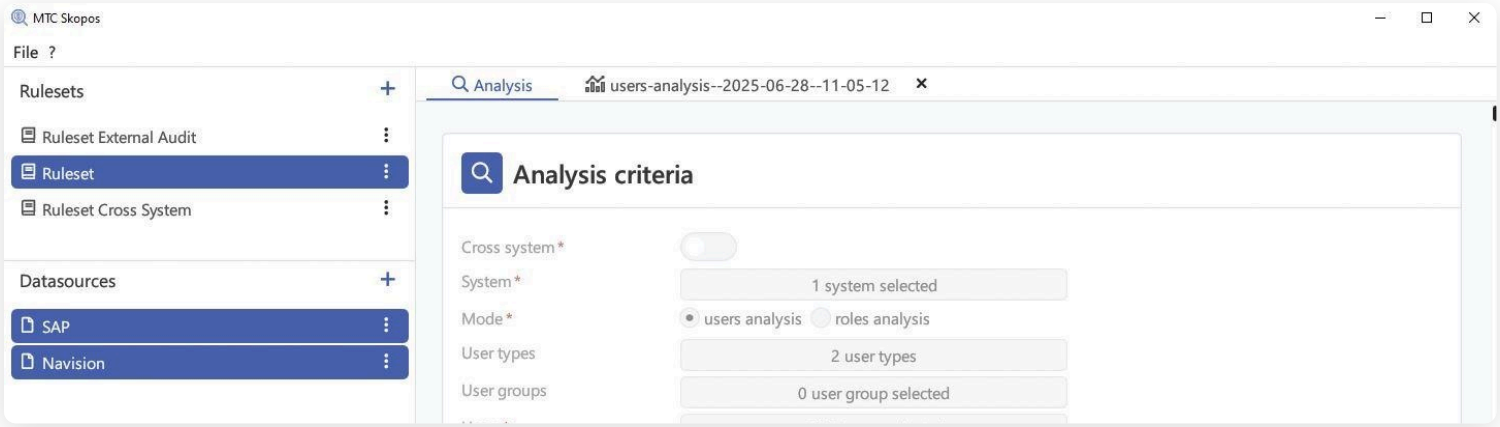
**Universal Approach:** If there's data, MTC Skopos can analyze it. System-agnostic design ensures compatibility across your entire IT landscape.

- **SAP Systems:** Direct RFC connection or folder import
- **Any ERP System:** Generic User-Privilege format via folder import

On-demand connector creation: our development team can create a custom integration for you.

# Reimagining SAP Security

## Why We Built MTC Skopos




The enterprise security market is crowded with solutions promising comprehensive risk analysis and governance. Yet for security professionals working in cross-systems environments, a persistent frustration remains: tools that are either too slow, too complex, or simply miss the mark on what practitioners actually need. This frustration led us to build MTC Skopos, a tool born from the intersection of deep SAP security consulting expertise and modern software engineering principles.

## The Problem: Where Experience Meets Reality

As SAP Security Consultants and Software Architects, we've spent years navigating enterprise risk analysis complexities. In our daily work, we consistently encountered pain points that existing solutions failed to address adequately.

> *The most glaring issue? Performance. When conducting time-sensitive security assessments, waiting for tools to process data isn't just inconvenient, it's a barrier to effective security work.*

## The Technical Foundation: Why Rust Changes Everything

While most competitors chose .NET, Python, or Java using a database in-between, our decision to build MTC Skopos in Rust wasn't driven by technology trends, it was driven by results. Rust delivers the performance characteristics that security analysis demands while maintaining enterprise-grade safety and reliability.

### Performance First

Rust's zero-cost abstractions and memory safety without garbage collection mean MTC Skopos runs fast and stays fast, even when processing large SAP environments with thousands of users and complex role hierarchies.

### True Portability

No installation headaches, no environment variables, no library dependencies, and no elevated privileges required. MTC Skopos runs immediately, wherever you need it: a game-changer for consultants working across multiple client environments.

### Privacy by Design

With local processing and no cloud dependencies for core functionality, sensitive enterprise data stays under your organization's control.

## Rethinking the Economics of Security

Existing solutions use pricing models that create perverse incentives: the larger and more complex your SAP landscape, the more expensive your security tools become. For on-premises solutions especially, this makes little sense—an engine built to analyze 10 users or 1 million is fundamentally the same.

MTC Skopos challenges this approach by making risk analysis genuinely accessible. **Security shouldn't be a luxury reserved for organizations with unlimited budgets.** Every company running SAP deserves comprehensive risk analysis tools, regardless of environment size or complexity.

## Filling the Feature Gaps

Our consulting experience revealed critical capabilities that existing solutions either lacked or implemented inadequately:

- **In-Depth Simulation:** Real-world security scenarios require modeling complex "what-if" situations. Most tools provide basic reporting but fall short when simulating security implications of role changes or organizational restructures.
- **Step-by-Step Remediation:** Identifying risks is only half the battle. Security professionals need clear, actionable guidance. We built detailed remediation workflows that guide users through exact steps needed to resolve security issues.

## Built by Practitioners, for Practitioners

What sets MTC Skopos apart isn't just its technical implementation, it's the perspective behind it. This tool was conceived, designed, and built by professionals who use security analysis tools daily. Every feature decision was informed by real-world consulting experience, every performance optimization addresses actual bottlenecks and pain points.

> *For security professionals tired of tools that slow them down rather than speed them up, MTC Skopos offers a different path forward. One where technology serves security expertise, not the other way around.*

# Practical SAP Security

## A Collaborative Approach to Addressing Segregation of Duties Risks

Managing segregation of duties (SoD) risks in complex SAP environments is a common challenge many organizations face. Yet many organizations are still overlooking this control or do not possess the proper tooling to support this activity. A recent project collaboration between MTC Skopos and **Protiviti the Netherlands**' SAP Security team provides a practical example of how the right tools and expertise can help address audit findings efficiently.

## The Situation

### Audit Findings Require Systematic Response

Our client, a multinational company, implemented an SAP authorization concept years ago but did not invest in tools to maintain or monitor it. Over time, role changes occurred without SoD or critical access controls, leading to significant SoD and critical access risks.

Their external auditor neither relied on the IT environment nor conducted thorough risk analyses, leaving these issues undetected and potentially exposing the company to financial loss or system errors. Like many organizations, they need to address specific audit findings within reasonable timeframes:

- Understand their current authorization landscape better
- Receive insights and detailed reports to aid decision-making at the executive level
- Design sustainable controls to prevent similar issues
- Plan remediation activities

## The Approach

### Combining Analysis Tools with Consulting Experience

Protiviti The Netherlands partnered with MTC Skopos to conduct a thorough assessment of the client's SAP authorization structure (Business & IT Risks). This combination brought together practical analysis capabilities with experienced SAP security consulting.

### Risk Analysis with MTC Skopos

Protiviti loaded their global golden rulesets to MTC Skopos. The tool assisted us in:

- **Identify Conflicts:** We identified SoD violations and Critical Access in the client's role and user assignments.
- **Analyze Cross-System Access:** The assessment covered access patterns spanning multiple systems, providing a comprehensive view of potential risk areas.
- **Reporting:** As a result of the analysis a "ready-to-import" report enable direct visualization on Power-BI to transform risk analysis results into Business-oriented insights.
- **Remediation insights:** Thanks to usage data being available in the environment we could easily determine users' behaviors and better understand how business activities are performed.
- **Test Remediation Options:** Using the simulation feature, we could evaluate different remediation approaches to ensure business continuity.

### SAP Security Expertise from Protiviti NL

Protiviti's team brought the SAP Security and IT Audit knowledge needed to interpret findings and develop practical remediation strategies. Their experience helped ensure recommendations were realistic and aligned with business needs. The collaboration produced practical results:

**Rapid Risk Assessment:** The comprehensive analysis was completed within days of project initiation, giving the client immediate visibility into their security posture when they needed it most.
**Precision-Focused Strategy:** Rather than recommending sweeping impact. This structured approach ensures that remediation efforts are not only technically effective but also aligned with business continuity requirements and organizational change management capabilities.

**Precision-Focused Strategy**

Rather than recommending sweeping impact, this structured approach ensures that remediation efforts are not only technically effective but also aligned with business continuity requirements and organizational change management capabilities.

## Moving Forward

Whether addressing current audit findings or improving ongoing security governance, having the right combination of tools and expertise can make the process more manageable. The collaboration between MTC Skopos and Protiviti demonstrates how practical analysis tools combined with experienced consulting can help organizations address SAP security challenges effectively. For organizations dealing with similar challenges, consider how proper analysis tools and experienced guidance can help you better understand and manage your authorization risks.

# From Data Chaos to Security Intelligence

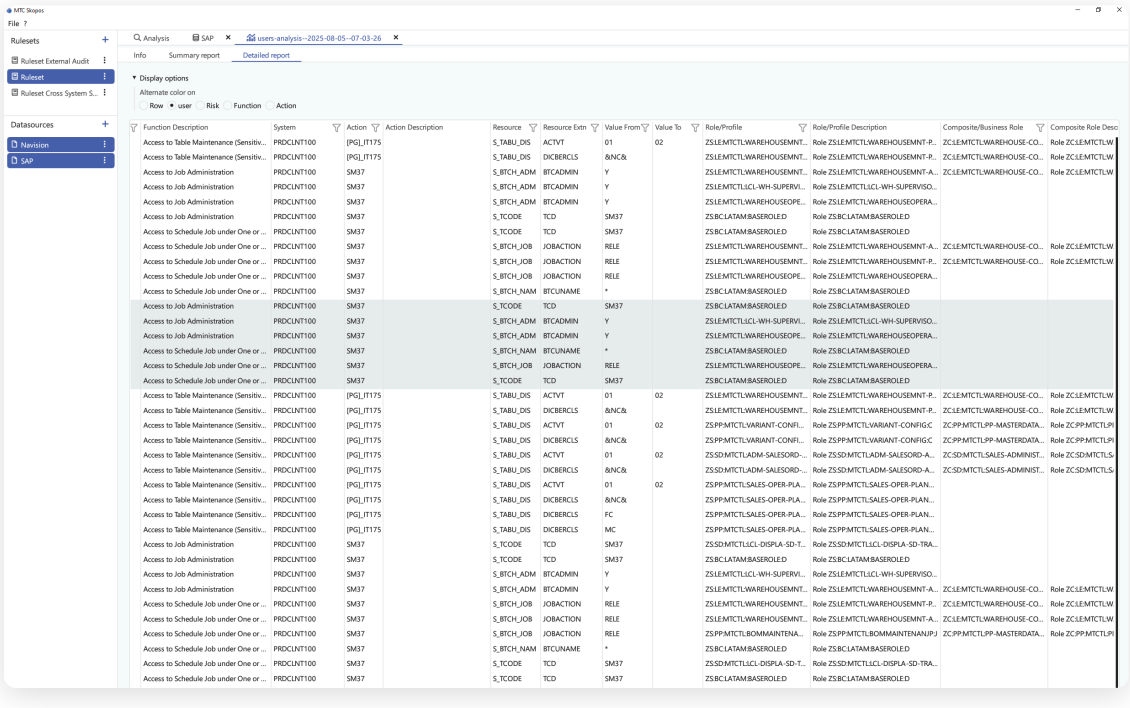
## Why Flexible Insights Beat Rigid Dashboards

Most GRC platforms lock you into their idea of what security insights should look like. Cookie-cutter dashboards that may miss what matters in your environment. MTC Skopos works differently: we give you the security intelligence, you decide how to use it and how to visualize it.

## We're Security Consultants, Not a BI Company

Here's the thing, we're not trying to build the prettiest interface. We're security consultants who know what data actually helps you fix access risks. While other vendors focus on flashy dashboards, we focus on delivering the insights that matter.

That's why MTC Skopos provides ready-to-use data models and plug-and-play Power BI dashboards instead of another proprietary platform. You get proven security intelligence without getting locked into our way of visualizing it.



# Real Flexibility, Not Just Marketing Speak

## Start Smart, Customize Everything

Our data models come from years of security consulting. They focus on the access patterns and risks that actually cause problems, not just what's easy to chart.

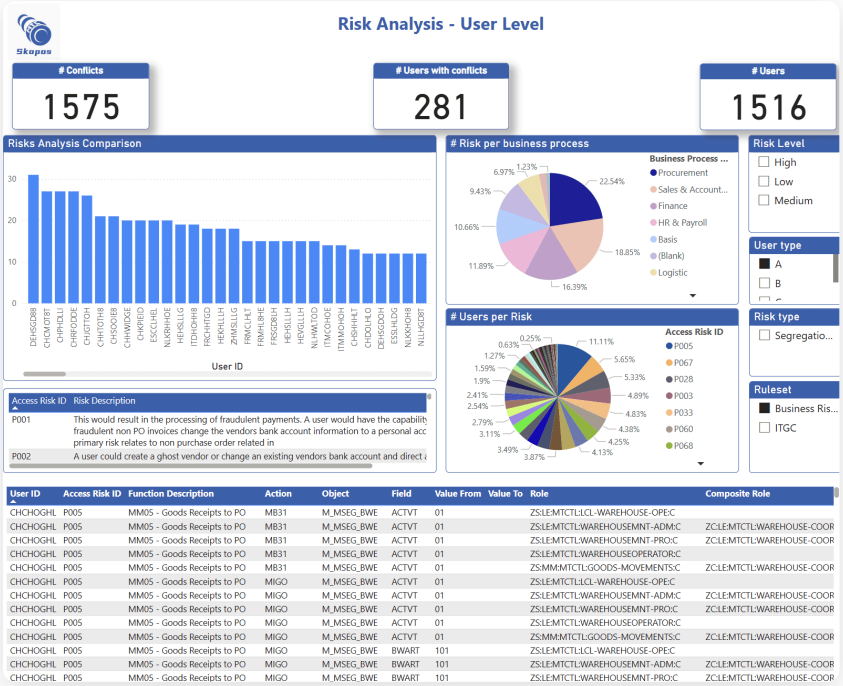
Use our Power BI templates as a starting point, then adapt them to your environment.

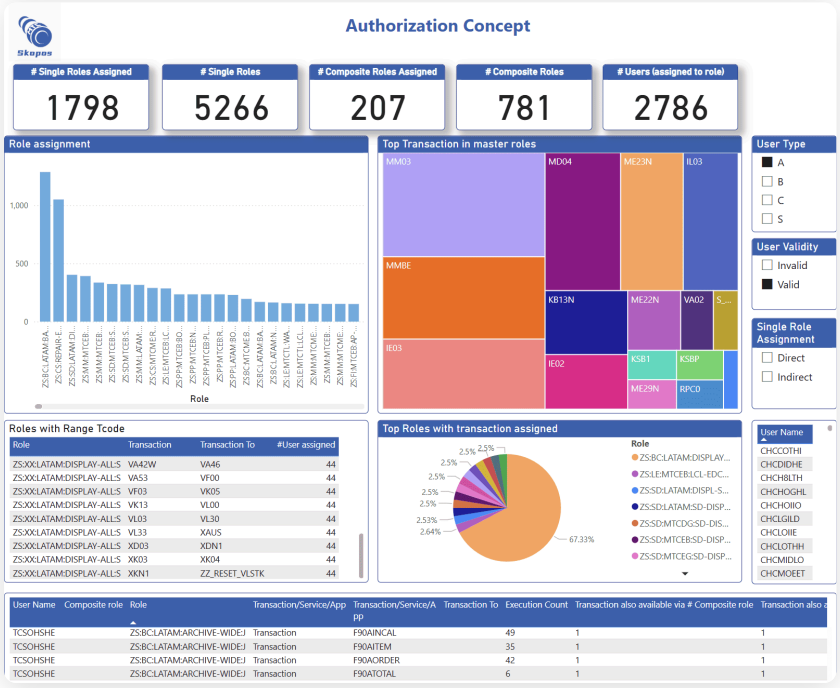
## Use Your Existing Tools

Already invested in Power BI, Tableau, or other analytics platforms? Great. Our data models integrate with what you already have instead of forcing you to learn another system.

## Own Your Analytics

No vendor lock-in means you control your security insights. Modify reports, add new metrics, or integrate with other tools, it's your data and your choice.



## Built by People Who Actually Do Security Work

We've seen how access risks play out in real environments. We know which compliance violations cause the most damage and what information security teams actually need to prioritize their work. Our data models emphasize the stuff that matters: risky privilege combinations, segregation of duties violations, and access patterns that signal real threats. Not just vanity metrics that look good in executive presentations.

## Focus on Security

- **Identify Real Risks:** Spend less time fighting with inflexible reporting tools and more time addressing the access risks and compliance gaps that our models help you identify.
- **Scale Your Analytics:** Build on proven data models that grow with your security program
- **Stay Independent:** Avoid vendor lock-in by building your security insights on industry-standard platforms like Power BI, ensuring you retain control over your analytical investments.

## MTC Skopos: Security Intelligence, Your Way

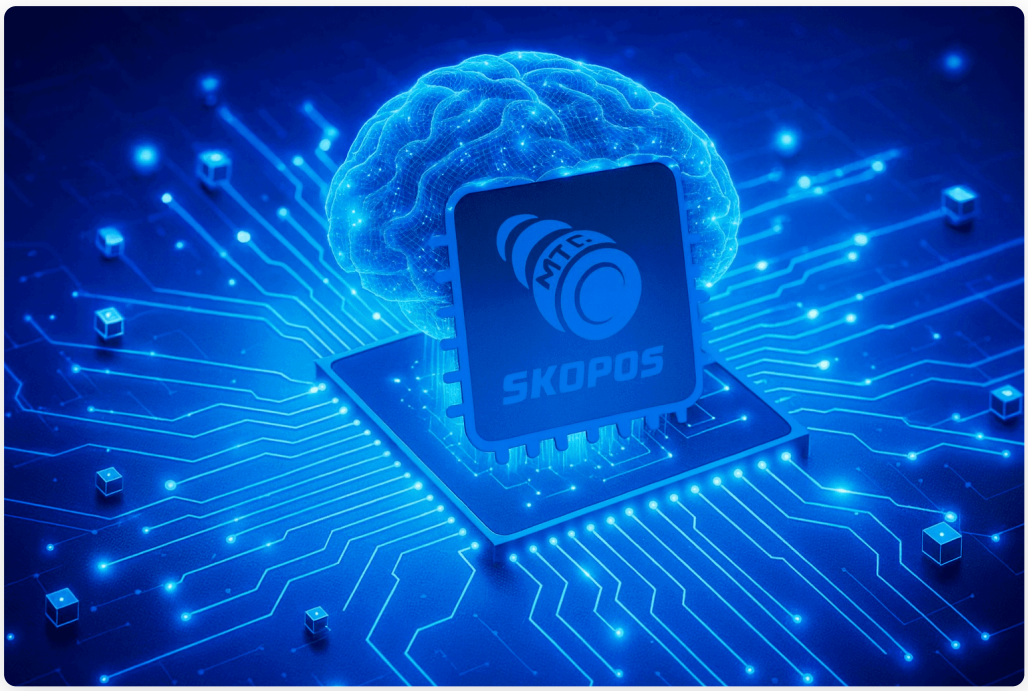
MTC Skopos transforms access governance by providing the security intelligence foundation your team needs without constraining how you use those insights.

Our approach recognizes that effective security analytics require both deep domain expertise and analytical flexibility: combining our security consulting experience with enterprise-grade data models that adapt to your unique environment.

> *Say goodbye to one-size-fits-all security dashboards and hello to intelligent, flexible access governance with MTC Skopos: empowering your security team to build the insights that matter most to your organization's risk profile.*

# AI Meets SAP Security

## How MCP Transforms MTC Skopos




We've connected MTC Skopos to AI assistants using Model Context Protocol (MCP). Translation: you can now have a conversation with your SAP security data.

## What is MCP and Why It Matters

Model Context Protocol is a standardized way for AI to connect with specialized applications. Think of it as a universal connector between AI and your data sources. Instead of AI providing generic advice based on general knowledge, MCP creates a structured communication channel that lets AI access actual analysis from your systems.

The breakthrough isn't just about connecting things, it's about doing it efficiently. Querying SAP tables directly would consume enormous amounts of AI tokens and processing time. A single comprehensive SoD analysis might require joining millions of rows across dozens of tables, potentially exceeding context windows and making real-time interaction impossible.

**That's why the MCP server connects directly to MTC Skopos, not to raw SAP tables.**

## The Transformation: See It In Action

### Before MCP: Generic AI Guidance

When asked "What is the most triggered Segregation of Duties conflicts in Finance?", AI provides theoretical knowledge:

- F001 (General Ledger Maintenance + Posting) - undetected errors and financial misstatement
- F002 (Cost Center Maintenance + Cost Transfer) - hiding fraudulent costs
- F012 (Asset Master Maintenance + Asset Transactions) - asset misappropriation
- F064 (Asset Maintenance + Invoice Processing) - manipulation of capitalization

This is helpful background, but it's not YOUR data. It doesn't tell you which risks exist in your environment or who's affected.

### After MCP: Your Actual Data

The conversation transforms when you ask: "Can you load analysis from users-analysis--2025-09-28--23-24-58.log"

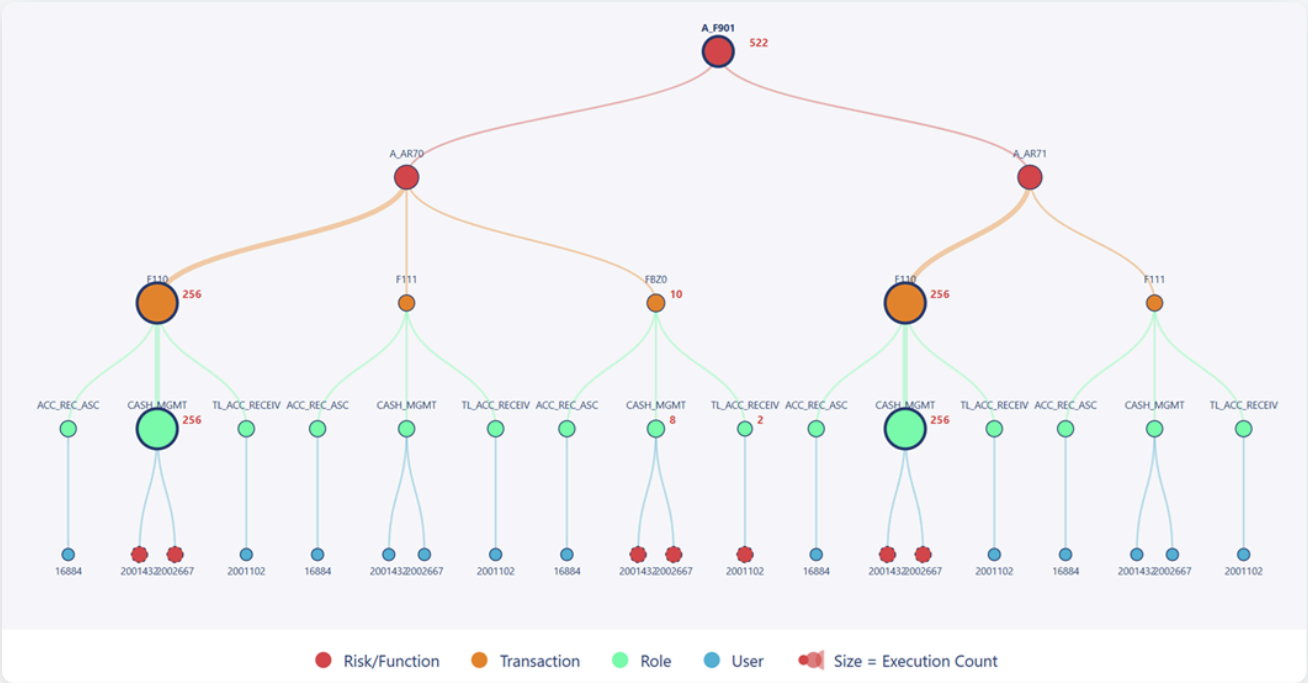
| 2,417 | 75 | 433 | ~18% |
|---|---|---|---|
| Total Users Analyzed | Distinct SoD Risks | Impacted Users | Impact Rate |

## Risk Distribution by Business Process

- **Procure to Pay (PR00/MM00):** 18 risks - Vendor maintenance, invoice processing, payments, inventory
- **Sales & Distribution (SD00):** 18 risks - Customer maintenance, invoicing, credit management, AR clearing
- **Financial Accounting (FI00):** 12 risks - GL posting, asset management, bank accounts, cost centers
- **Human Resources (HR00):** 14 risks - Employee maintenance, payroll processing, time entry
- **Basis/Security (BS00):** 6 risks - Security administration, transport management, configuration
- **Treasury (TR00):** 5 risks - Securities, payments, treasury transactions

## Now you can have focused conversations based on real data:

> ***"Which Finance risks affect the most users?"*** *Skopos shows F001 (GL Maintenance + Posting) has the highest user count, while F002 (Cost Center manipulation) shows the most transaction activity.*
>
> ***"Show me users with F001 conflicts"*** *Immediate list with role assignments, usage patterns, and last activity dates from your actual system.*
>
> ***"If I remove XK01 from Z_FI_AP, who else is affected?"*** *Skopos returns that 15 users have this role, with usage statistics showing 3 users actively employ the transaction while 12 have never used it.*
>
> ***"Show me users with F001 conflicts"*** *Immediate list with role assignments, usage patterns, and last activity dates from your actual system.*
>
> ***"If I remove XK01 from Z_FI_AP, who else is affected?"*** *Skopos returns that 15 users have this role, with usage statistics showing 3 users actively employ the transaction while 12 have never used it.*
>
> ***"What alternative roles could work?"*** *Skopos suggests Z_FI_AP_VIEW as a display-only alternative, already validated against your role catalog.*
>
> ***"Explain our S2P risks to the CFO"*** *18 users can both create vendors AND process payments to them. That's like giving someone both the company checkbook and the ability to add recipients. Here's the fraud scenario: Monday they create a vendor for their friend's company, Tuesday they process a payment. Without segregation, there's no control stopping this."*
>
> ***"Can you create a visualisation of the risk in the process flow?"*** *Creates a visual*



## Why This Architecture Works

### Token Efficiency

Instead of processing millions of SAP table rows through the AI's context window, only Skopos's analyzed results flow through MCP. A query that might require 100,000 tokens if parsing raw tables directly needs only 2,000 tokens when Skopos provides pre-processed insights.

### Response Speed

Skopos maintains optimized indexes and cached analyses. Responses are instant because the computational heavy lifting happened during the analysis phase, not during your conversation.

### Data Security

Sensitive authorization data stays within Skopos's infrastructure. The AI reasons about summaries and aggregates, not raw user permissions. Your security data never leaves your environment.

### Flexibility

The MTC Skopos MCP server declares what resources, tools, and prompts it exposes. As Skopos evolves, adding support for new authorization objects, Fiori app permissions, cloud applications, the MCP server updates its capabilities without requiring changes to the AI applications using it.

## What This Means for Security Teams

You're managing thousands of users and roles across 10+ SAP systems in hybrid cloud and on-premise landscapes. A typical first-time risk analysis might reveal 50,000 SoD violations, that's approximately two years of part-time work to remediate to zero. You're responding to constant access requests while maintaining audit readiness and demonstrating control effectiveness.

> *The shift is fundamental: from data gatherer to strategic risk manager.*

Instead of spending days extracting and cross-referencing information, you focus on high-value decisions:

- Evaluating risk trade-offs
- Coordinating with business process owners
- Prioritizing remediation efforts
- Designing controls aligned with organizational objectives

## The Bottom Line

MCP doesn't replace Skopos's analytical engine, it makes that engine conversationally accessible. Skopos continues doing what it does best: continuously analyzing SAP authorization data, computing complex conflict patterns, tracking multi-dimensional relationships, simulating remediation scenarios, and maintaining optimized intelligence about your security posture. The MCP server transforms this from a platform you query through reports and interfaces into one you can converse with naturally. Ask questions. Get specific answers based on your data.

> *The future of SAP security analysis isn't about choosing between specialized tools and AI, it's about using MCP to make specialized tools like Skopos work through AI interfaces. The analytical engine that took years to build remains the source of truth. The AI becomes the interface, making that truth accessible, explainable, and actionable through natural conversation.*

**Join Forward-Thinking companies using MTC Skopos for comprehensive access risk management.**

info@meylan-tc.com

Ready to secure your ERP Systems?

MEYLAN TECHNOLOGIES & CONSULTING | December 2025