

## SAP Customer Success Story High Tech



**“[Our audit firm] agreed to use the SAP GRC Access Control reports in the audit as evidence for control effectiveness. We saved very significantly on time and money spent on external audit fees.”**

Deepak Mehrotra, SOX Compliance Manager, Synopsys

### AT A GLANCE

#### Company

- Name: Synopsys Inc.
- Location: Mountain View, California
- Industry: High tech
- Products and services: Software for semiconductor design
- Revenue: Nearly US\$1 billion
- Employees: 4,800
- Web site: [www.synopsys.com](http://www.synopsys.com)

#### Challenges and Opportunities

- Limited time frame for filing annual financial report and complying with Sarbanes-Oxley (SOX) requirements
- Numerous potential violations of key SOX requirement: segregation of duties (SoD)
- Less time for resolving violations than originally scheduled

#### Objectives

- Resolve SoD issues rapidly and efficiently
- Create foundation for avoiding SoD compliance risks in the future

#### SAP® Solution and Services

SAP® GRC Access Control application

#### Implementation Highlights

- Completed rules configuration in less than 2 days
- Reduced SoD conflicts by 80% within 1 week
- Modified or redesigned more than 100 roles significantly
- Reduced number of transaction codes in basic end-user roles from 16,000 to 45
- Detected and eliminated more than 100,000 SoD violations

#### Why SAP

- Ease of use
- Low maintenance cost
- Accuracy
- Ability to scan custom code for violations
- Large, preconfigured rule set

#### Benefits

- Met SOX deadline and filed year-end report on time with no unresolved SoD issues
- Saved hundreds of hours of labor through preconfiguration
- Equipped internal and external auditors to complete testing in 4 weeks through continuous compliance, saving substantial audit costs
- Achieved ROI in less than 3 months through productivity improvements and audit cost savings
- Improved processes to avoid SoD compliance risk and reduce audit costs in future years

#### Existing Environment

SAP R/3® software (functionality now found in the SAP ERP application)

## SYNOPSYS

### Clean Sweep of SOX Compliance with SAP® GRC Access Control

Mountain View, California-based Synopsys Inc. is a world leader in semiconductor design software. The company recently needed to resolve segregation of duties (SoD) issues in its SAP® software rapidly and efficiently in order to file its annual financial report and comply with Sarbanes-Oxley (SOX) requirements on time. Synopsys used the SAP GRC Access Control application, which provides a comprehensive set of preconfigured rules and a real-time analysis engine for detecting and preventing SoD violations, to detect and eliminate more than 100,000 such infringements. The company completed its audit on time and met its compliance deadline with no unresolved SoD issues. The company's auditors leveraged the reliability and accuracy of the application's rules and reports and agreed to use those reports as evidence in its audit. Synopsys achieved ROI in less than three months, based on significant productivity gains and audit cost savings.

With revenues of nearly US\$1 billion in 2005, Synopsys has operations across the globe, including in North America, Europe, Japan, and Asia Pacific. Synopsys supports its key business processes using SAP software for functions such as finance, sales, and human resources. Out of a total global workforce of approximately 4,800 employees, more than 1,000 use SAP applications.

### **SoD Issues Raise Red Flag**

Based on its fiscal year-end of October 31, Synopsys faced a deadline of January 2006 to comply with year-one SOX requirements. In approaching its SOX initiative, Synopsys identified 18 “mega business processes” where it needed to satisfy requirements for control identification, documentation, testing, and reporting. In July 2005, three months prior to its fiscal year-end, the company found that while compliance was on track for 17 of these issues, 1 was behind schedule – SoD.

SoD, an internal control to help prevent fraud, errors, and abuse, means that an individual is not permitted to initiate, approve, and review the same action. For example, an employee who is authorized to create new vendor accounts in the organization’s financial system should not be permitted to approve vendor payments. Over the previous four years, Synopsys had constructed user roles in its SAP software to provide maximum business flexibility. Whenever users changed jobs, they retained whatever roles they had before, which ultimately resulted in user authorization conflicts.

### **SAP GRC Access Control Provides the Lowest Total Cost, Highest Accuracy**

To address its SoD issues, Synopsys selected SAP GRC Access Control. “We evaluated a number of products on the market and found that SAP had the best solution,” says Deepak Mehrotra, SOX compliance manager at Synopsys. “We wanted an application that was easy and inexpensive to maintain. We also wanted a highly accurate solution to minimize false positives, and SAP GRC Access Control was the best.”

Two other factors drove Synopsys’s selection. One was the fact that only SAP GRC Access Control was able to scan custom code for SoD violations. Like most SAP customers, Synopsys had developed a considerable number of custom transactions, so the ability to detect authorization conflicts in this custom code was critically important. The other factor was the large, preconfigured rule set provided with the SAP GRC Access Control application.

The extensive and detailed preconfiguration reduced the amount of custom configuration Synopsys had to perform dramatically, saving the company hundreds of hours of labor. After developing an understanding of the requirements for Synopsys’s specific functional areas, the company’s SAP security specialist completed the rules configuration for SAP GRC Access Control in less than two days.

**“SAP GRC Access Control, with its comprehensive preconfigured rule set, reflected deep expertise within SAP that would have taken us a very long time to replicate.”**

*Deepak Mehrotra, SOX Compliance Manager, Synopsys Inc.*

“Before we deployed SAP GRC Access Control,” recalls Mehrotra, “we considered developing our own SoD analysis solution by constructing an SoD matrix based on the SAP roles we had defined. But we soon realized the enormous complexity of that approach and concluded it was not a viable option. SAP GRC Access Control, with its comprehensive preconfigured rule set, reflected deep expertise within SAP that would have taken us a very long time to replicate.”

### **Setting the Tone at the Top**

“We had a large scope of work to cover in a limited time,” explains Mehrotra. “Without the complete cooperation of all the stakeholders across the company, we would not have been able to pull it off.” Key to getting everyone focused on the task was the fact that senior management made it a top priority. “SOX compliance, and the segregation of duties issue in particular, had high awareness among management,” notes Mehrotra. “We had senior executive sponsorship from the very start, with several VPs participating in our kickoff meeting in July. I can’t overemphasize the importance of this.”

When Mehrotra ran the first SAP GRC Access Control analysis on the company's system, the report came back with over 100,000 SoD violations. "We needed a strategy to accelerate remediation," he says. Synopsys followed SAP best practices by focusing initially on cleaning up roles and then moving to user-level authorizations. Using SAP GRC Access Control to analyze SAP roles, Synopsys identified key problem areas rapidly. "For example," explains Mehrotra, "our basic role worldwide for SAP application users included 16,000 transaction codes, giving users too many authorizations that created SoD conflicts. Once we started cleaning up roles, we quickly reduced the remaining number of SoD violations to clean up at the user level. Within one week we reduced SoD conflicts by 80%."

### **SoD Conflicts Cleaned Up Globally in Less Than Five Months**

To expedite the role clean-up process, Mehrotra formed 14 teams working in parallel. Each team focused on 1 of 14 major processes and was comprised of people from the SOX compliance group, IT security, and the particular business function, such as payroll or procurement. Each team analyzed its SAP GRC Access Control reports, provided by Mehrotra's SOX compliance group, and determined how to clean the roles for its area. The Synopsys finance project manager responsible for financial processes such

**"The clean-up process has brought a tremendous degree of discipline to the way we think about and manage user access and authorizations."**

*Deepak Mehrotra, SOX Compliance Manager, Synopsys Inc.*

as general ledger, accounts payable, financial reporting, financial close, and fixed asset management considered this a highly efficient approach. Synopsys had about 300 roles in finance and held daily check meetings, quickly resolving SoD issues every day.

In all, Synopsys significantly modified or redesigned more than 100 roles across the enterprise. For example, they reduced the number of transaction codes in the basic role for end users worldwide from 16,000 to 45, removing all SoD conflicts from the role. Once all the roles had been cleaned up, 545 SoD violations remained at the user level. The company resolved 534 of them by removing conflicting authorizations from individual user assignments. For the remaining conflicts, the company implemented mitigating controls or decided that the level of business risk was acceptable. "Management now has a much clearer understanding of these risks and mitigating controls," says Mehrotra. "The clean-up process has brought a tremendous degree of discipline to the way we think about and manage user access and authorizations."

**"With SAP GRC Access Control, we have SoD under control for good."**

*Deepak Mehrotra, SOX Compliance Manager, Synopsys Inc.*

Mehrotra and his team implemented the clean-up process in phases by geographic region. They completed the North America phase in just five weeks during July and August, followed by Japan in September, Europe in October, and Asia Pacific in December. The team completed the entire project globally in less than five months.

### **Significant Audit Cost Savings Contribute to Payback in Less Than Three Months**

To get buy-in from the company's big-four external auditor, Mehrotra presented the SAP GRC Access Control rule set and reports in detail. "The auditors analyzed the rules and conducted sample testing to validate the SAP GRC Access Control reports," explains Mehrotra. "Once they were convinced of our methodology and the reliability of the SAP GRC Access Control application, they agreed to use the SAP GRC Access Control reports in the audit as evidence for control effectiveness. We saved very significantly on time and money spent on external audit fees." The internal and external auditors completed all their testing within a period of just four weeks.

Mehrotra calculates that, based on its savings in audit costs as well as productivity gains, Synopsys achieved a return on its SAP GRC Access Control investment in less than three months. More importantly, Synopsys was able to meet its SOX deadline and file its fiscal year-end report in January 2006 with no unresolved SoD issues. The company ended up accepting a total of 11 SoD conflicts, for which management identified mitigating controls or determined an acceptable level of business risk. “Without the use of SAP GRC Access Control, we would not have met our deadline,” says Mehrotra.

**Lessons Learned: Building Risk Analysis into Business Processes to Avoid Compliance Issues in the Future**

“Although the driving force was compliance with Sarbanes-Oxley, this initiative helped us improve our business processes, such as how we manage setting up master data,” says Mehrotra. “For example, in our procure-to-pay process, we now restrict the number of people who can create new vendors. Similarly, in our sales process we limit the number of users who can create new customer accounts.” In addition, Synopsys now builds SoD risk analysis into the way it designs and manages roles for SAP users. Using additional functionality contained in SAP GRC Access Control, the company will be able to keep roles clean as it grants new individuals access to SAP software functionality and rescinds access for others. “We now use SAP GRC Access Control to check for potential SoD conflicts before we create a new role or modify an existing role,” Mehrotra explains. “With SAP GRC Access Control, we have SoD under control for good.”