



## Oracle Customer Spotlight



### CHARTERED SEMICONDUCTOR MANUFACTURING LIMITED

Singapore  
www.charteredsemi.com

**INDUSTRY:**  
High Technology

**ANNUAL REVENUE:**  
US\$1.7 billion

**EMPLOYEES:**  
6,500

**ORACLE PRODUCTS  
& SERVICES:**  
Oracle Application Access  
Controls Governor

### ORACLE PARTNER:



Deloitte & Touche Enterprise Risk  
Services Pte Ltd  
www.deloitte.com

"Implementing Oracle  
Application Access Controls  
Governor enabled us to  
thoroughly check access rights  
and segregate conflicting  
duties. This eliminates  
improprieties that would reflect  
badly on our business and  
ensures we meet SOX  
compliance obligations."

– Manju Jalali, Director, IT  
Applications, Chartered  
Semiconductor Manufacturing  
Limited

## Chartered Semiconductor Avoids Expensive Audit and Remediation, Resolves Segregation-of-Duty Conflicts

Singapore-based Chartered Semiconductor Manufacturing is one of the world's leading semiconductor foundries, with five wafer fabrication facilities capable of producing approximately 2.4 million 8 inch equivalent wafers, annually. The company is listed on the Singapore Stock Exchange and NASDAQ, and reported revenue of US\$1.7 billion for the 2008 financial year.

### Challenges

- Implement a solution to address a lack of segregation-of-duties (SOD) controls within the organization
- Enable senior managers to proactively resolve conflicting access rights
- Comply with Sarbanes-Oxley legislation

### Solution

- Engaged Oracle Certified Advantage Partner Deloitte & Touche Enterprise Risk Services Pte Ltd to deploy Oracle Application Access Controls Governor, the first successful implementation of the software in the Asia Pacific region
- Automated the identification and prevention of SOD conflicts within the organization's Oracle E-Business Suite ERP system
- Configured the software to detect SOD conflicts in three other applications
- Identified more than 33,000 SOD conflicts and enabled action to be taken to correct these control deficiencies prior to the half-yearly and yearly audit periods
- Prevented users from accessing systems that conflicted with their roles, such as barring access to systems that approved purchase orders to those not allowed to submit them
- Eliminated access to unused functions, processes, and programs
- Avoided the need for manual SOD assessments, which was time consuming and open to human error
- Gained ability to enforce controls in real time and prevent violations before they occur
- Enabled the organization to avoid expensive audit and remediation costs
- Gave staff the ability to simulate SOD policies before implementation to determine long-ranging impacts and identify areas of potential conflict