Plug-and-Play GRC Overhaul in One Week

Mahindra CIE Automotive Ltd. Reduces Risk and Hours of Manual Effort by Automating Its SAP User Provisioning Processes

by **Joe Mullich**, Contributing Writer

Mahindra CIE Automotive Ltd. (MCIE), headquartered in Mumbai, India, makes crankshafts, axle beams, piston rods, and some 250 other products that are under the hoods of some of the biggest automotive brands. In the past decade, the MCIE business has been on the move as well. A series of acquisitions and alliances has transformed the company from a small player in the automotive industry to a global powerhouse, topping $1 billion in revenue for 2019.

As with any growing international company, risk and compliance have become a paramount concern. A publicly traded company and a subsidiary of CIE Automotive group of Spain, the business must follow a variety of regulations and compliance standards and undergo various statuary audits.

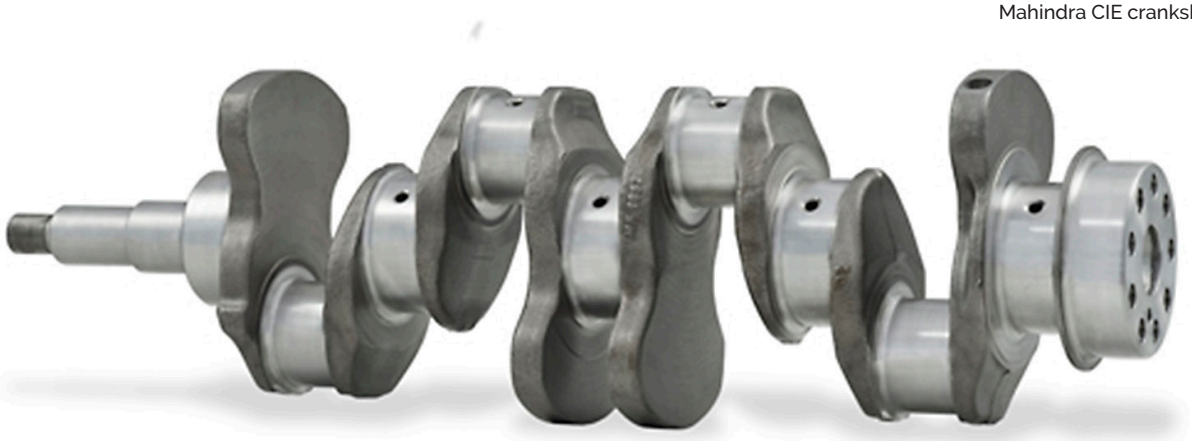
In the first quarter of 2019, the company's board of directors stressed the importance of putting in place stronger security and compliance controls to provide better assurance to investors and customers. The centerpiece of the company's information stores is SAP ERP 6.0. As such, the system is a critical component of the compliance and security strategy.

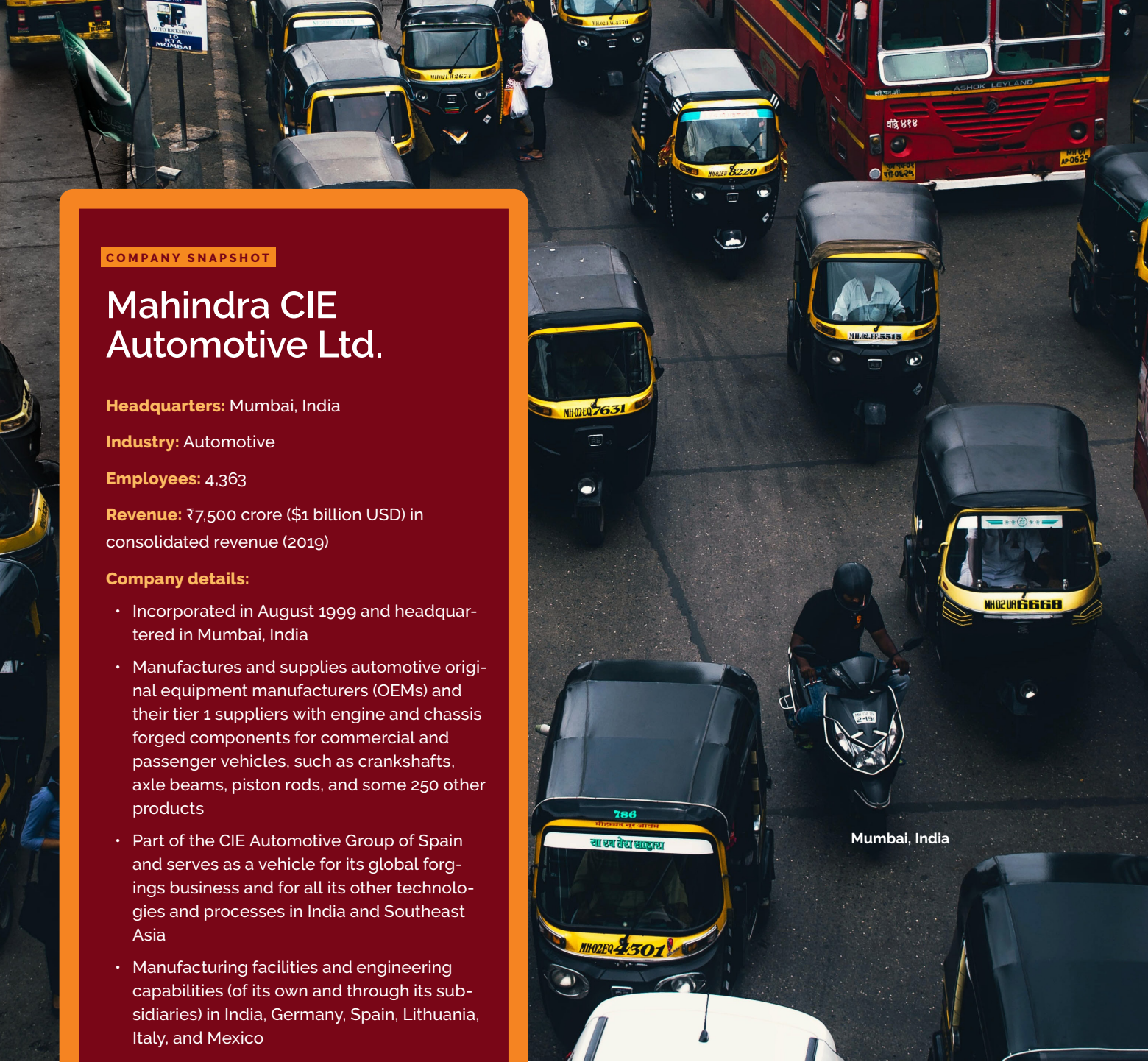
"Oversights could be costly for the organization's brand and trust with customers," says Ajitsingh Nawale, Head of Information Technology for MCIE. "We want to eliminate any threat of possible violations and misuse of the system."

Fixing Manual Mire

Consider when MCIE hires a new vendor. This results in a complex series of transactional workflows that are fraught with potential for risk and fraud. Someone has to set up the vendor in the SAP system so the vendor's invoices can be paid. An employee needs to draft and improve the purchase order, process payments, and issue and sign checks for the vendor.

Mahindra CIE crankshaft





Mumbai, India

COMPANY SNAPSHOT

Mahindra CIE Automotive Ltd.

Headquarters: Mumbai, India

Industry: Automotive

Employees: 4,363

Revenue: ₹7,500 crore ($1 billion USD) in consolidated revenue (2019)

Company details:

- Incorporated in August 1999 and headquartered in Mumbai, India
- Manufactures and supplies automotive original equipment manufacturers (OEMs) and their tier 1 suppliers with engine and chassis forged components for commercial and passenger vehicles, such as crankshafts, axle beams, piston rods, and some 250 other products
- Part of the CIE Automotive Group of Spain and serves as a vehicle for its global forgings business and for all its other technologies and processes in India and Southeast Asia
- Manufacturing facilities and engineering capabilities (of its own and through its subsidiaries) in India, Germany, Spain, Lithuania, Italy, and Mexico
- Listed on the BSE Limited (BSE) and the National Stock Exchange of India Limited
- https://www.mahindracie.com/

SAP solution: SAP ERP 6.0

Third-party solutions: Security Weaver Separations Enforcer and Security Weaver Secure Provisioning

At each stage of the vendor onboarding process, it's necessary to ascertain that only approved employees are authorizing each task. As new employees are hired, leave the company, or change roles, it becomes even more challenging to ensure that everyone has the specific system usage capacity and appropriate access.

In the case of MCIE, these safeguards were handled manually by two full-time equivalent (FTE) employees. These individuals conducted regular segregation-of-duties (SoD) reviews, which determine if any risks or conflicts have occurred with a specific user or function.

This review required them to go through a lengthy process of defining the organization structure, mapping out the steps with each transactional workflow, and correlating them to specific user roles.

The two FTE employees also provided risk analysis before provisioning changes, handled the provisioning and de-provisioning process, and oversaw the manual records of requests and reporting. Each of these tasks was a time-consuming ordeal:

- Regular SoD checks and review (of all users) — took two weeks every quarter to complete
- Risk analysis before provisioning changes (per user request) — took two to three hours for each user
- Provisioning/de-provisioning process (per user) — took two to three days for each user
- Manual reporting to show record of requests — took two days for each run

As the number of users increased, continuing to handle these tasks manually was not the most efficient or desired path, according to Nawale. "Users were becoming frustrated by the delays in access provisioning," he says. MCIE considered adding a third FTE employee to handle the increased work, but that would have increased the cost of the compliance activities, and they needed a more cost-effective solution.

Two Applications Met All Requirements

To satisfy the board's mandate for improved security and compliance controls, MCIE wanted to completely automate its current compliance tasks related to access provisioning and reviewing access to the SAP system.

In addition, the company wanted to add another level of security by proactively checking for risk before any access change was allowed. "We wanted an end-to-end automated process, where we could manage the process from the time an employee was hired to the time they retired," Nawale says.

This led MCIE to SAP partner Security Weaver. Security Weaver's flagship governance, risk, and compliance (GRC) software suite provides a unified view of the enterprise-wide application environment, and according to Nawale, it was quickly apparent that two Security Weaver applications —Separations Enforcer and Secure Provisioning — would meet the company's entire list of requirements.

The Separations Enforcer application — an analytical tool used by internal audit and compliance team members (including the financial controllers, security administrators, Basis administrators, supervisors, and functional or department heads) — offers organizations a single, well-organized solution for storing and analyzing access management data and mitigations. The application automatically detects conflicts and critical access at the role and user levels, supports simulations, offers support for mitigating controls, and reports on user activities, allowing administrators to dramatically reduce time, errors, and risks.

The Secure Provisioning application — an access request automation tool that allows users to request new SAP access, remove existing access, or make master data changes — helps organizations simplify user access provisioning in SAP systems with an automated approach that ensures employees can quickly get the access they need, while protecting the enterprise from inappropriate access. Appropriate parties are notified and kept involved through email workflow. Each request is tracked, including the status of the request, who approved the request, and any SoD conflicts that the request would create. These conflicts automatically trigger exception reviews and tracking.

An Easy Plug-and-Play Process

"An important benefit was the plug-and-play nature of the Security Weaver products," Nawale says. "No additional hardware was necessary, and there was no overlay with our existing SAP environment. The rapid implementation allowed the applications to be installed and operating in our environment within a week."

The implementation team that deployed the two applications included senior personnel as project managers, representatives from risk management and security, and an employee who was currently handling the SoD, provisioning, and compliance tasks manually.

Over five days, the implementation followed a three-stage process. The applications were installed in a development environment, and then moved to quality assurance for testing, before finally being migrated to production.

During the following 15 days, the IT department added some specific configurations, such as defining which stakeholders would be allowed to take action on specific requests.

> "No additional hardware was necessary, and there was no overlay with our existing SAP environment. The rapid implementation allowed the applications to be installed and operating in our environment within a week."
>
> **– AJITSINGH NAWALE, HEAD OF INFORMATION TECHNOLOGY, MAHINDRA CIE AUTOMOTIVE LTD.**

Two types of training sessions, lasting for two to four hours, were conducted for all the application users. One training was for the IT and project team to learn how to perform tasks such as applying changes and patches, and the other training was for the internal compliance team and end users, explaining the user interface and how to make changes and requests.

Benefits: Moving Faster and Safer

The two new applications resulted in clear benefits for both users and IT. Automating the compliance and security tasks eliminated a host of manual efforts, which reduced costs equivalent to two to three FTEs per quarter. In addition, eliminating the delays that the manual processes had introduced allowed employees to gain access to the system faster, reducing process times from a week to one or two days (depending on the required approvals in the system).

The self-service features improved end-user productivity. Managers and users now have a clear view of the status of their access request, including the implications of their requests, without needing to contact IT for assistance. Also, users don't need to collect excessive authorizations as they move from job to job, providing them with quicker access to the system.

"The solution has been so successful that we no longer accept any manual requests for role changes," Nawale says. "That was a part of the mandate rolled out from senior management."

MCIE is currently evaluating other Security Weaver applications, such as Automated Mitigations, to build on its ability to track existing users who have been granted exception-based access that could contribute to SoD risk. These users must be audited on a regular basis. Among other things, MCIE will be able to determine not only what access those employees have been granted, but whether they execute any critical transactions. If those users have access conflicts, appropriate personnel are automatically notified.

As MCIE continues to grow in the automotive world, with these applications in play, the business can rest assured that its GRC risks will not grow.