TITAN CONSULTING

10 MINUTES, 10 HOURS OR 10 YEARS – IN JAIL?
How SAP GRC Reduces the Cost and Risk of Compliance!

Sarbanes-Oxley (SOX) was invoked more than 15 years ago. It seems like yesterday when Enron and many other reckless companies cooked their books.

The goal of SOX was to restore confidence and close loopholes that allowed companies to defraud investors. The regulatory impact of compliance on companies is considered a major concern according to a recent survey of C-level executives. The Cost of Compliance and risk on these companies has increased exponentially and digitization will substantiate this trend.

Section 404 of the regulation is one of the most arduous to implement. It requires companies to perform extensive internal control tests and include the results in the audit report. However, over the past 15 years, most companies have attacked this approach using standalone tools that target the various controls.

The current trend is to combine your governance and controls requirements and build synergistic solutions. SAP GRC accomplishes this integration and lowers your cost of compliance and reduces your risk.

Another significant trend is to combine management objectives of business performance, compliance, and value / cost control.

There are many areas of risk, but one certain violation of controls, risk for fraud, deception, and loss is user access. The four primary functions of User Controls in SAP GRC are:

- Access Risk Analysis (ARA),
- Business Role Management (BRM),
- Access Request Management (ARM), and
- Emergency Access Management (EAM).

Where should you start?

Audits or the notification of an audit is the catalyst for many businesses to tighten up their controls. When audits trigger your actions, we see ARA or Access Risk Analysis as the starting point.

For instance, one of our clients resolved their Access Controls challenges with SAP GRC. This $1 billion USD manufacturing company resided in the portfolio of a private equity group for many years. As a privately-held company, access controls weren't aggressively enforced. Management's goal was to grow the company for future sale. Controls were a secondary objective for management and to ensure major breaches did not occur.

Then they were sold to a publicly-traded global company that had governance and risk controls as a measurable objective of management. They had a controls program in place co-sponsored by the CEO, CFO, and CISO and were rolling it out to the newly acquired entity.

The first time they ran ARA for the new business there were over 4,000,000 conflicts. The divisions management had to

abate these conflicts or suffer the consequences. The task fell squarely on the shoulders of the division controller and IT Director.

It took two months of reviewing the conflicts and either remediating or mitigating them. In today's manufacturing and economic environment, you will never remove all conflicts due to:

- Lean Manufacturing Environment,
- Overlap of Primary and Secondary Responsibilities,
- Cost and Risk Analysis.

After the focused effort, the conflicts were reduced by 75%.

Some of the challenges that occur in lean companies are **False Positives**. A false positive typically happens when secondary roles are assigned; for example, a user can receive goods and put them away. This is common in smaller warehouses and lean plants.

In these situations, you need to ensure that remediation occurs and is reviewed and signed off by the appropriate approval levels and internal audit. This may be as simple as running a weekly report or performing random sampling of conflicted areas.

Even in the best governance practices, there will always be conflicts. The balancing of conflicts and risk is the art and science of a well-designed GRC environment. Attention to the business roles, part of BRM, is the activity where you weigh the cost/risk of the roles.

A function that streamlines a burdensome workload and provides great benefits is Access Request Management (ARM).

"*I don't have enough time to do all of this compliance work*!" is a common complaint we hear from controllers and plant managers. By leveraging the ARM functionality, you automate the role creation process and it saves you time and frustration.

One IT Director we work with loves this functionality.

Now, when a new employee is hired, the hiring manager submits an electronic request for the new employee or contractor. The GRC system builds all the necessary user ids, roles, and authorizations – no human intervention other than to review the audit report.

Where should you start is a common quandary. We recommend a diagnostic that targets areas of risk in your processes. The diagnostic will highlight the low hanging fruit: risks, rules, opportunities, and effort to remediate or mitigate.

If you need assistance getting your Cost of Compliance under control, Titan Consulting is here to advise and guide you. Contact Warren Norris at 972-679-5183, or warren@titanconsulting.net; or contact your Titan Sales Director.