Deloitte.

ERP Security & Controls
Getting access rights under control

Organizations implement ERP (Enterprise Resource Planning) systems like SAP, Microsoft Dynamics AX (former Axapta) to improve and automate business processes. Expected benefits of implementation include a reduction in the cost of operations, greater asset efficiency, and enhanced quality of information. ERPs can help you achieve this, however there is one area that proves to be difficult to get it right—security & controls.

Given the size and complexity of most organizations, effectively managing user access to ERPs is challenging and can cause inefficiencies across the organization. Also, when different legal units share one and the same system platform, special focus should be given to logical segregation of access to avoid the risk of cross-site access.

The key questions any organization needs to answer are:

Giving you answers

Deloitte believes that effective internal control is a key element in protecting the integrity of your operational and financial information.

Despite the technology you are using, the best way to protect your data is by controlling access to the systems where that data is being processed and stored.

Financial Statements Integrity

- How do you assure that information presented on your financial statements has not been corrupted?
- How do you prevent the intentional financial misstatements?
- How do you assure that only limited people have authority to approve and execute direct GL accounts adjustments above 250.000 EUR?

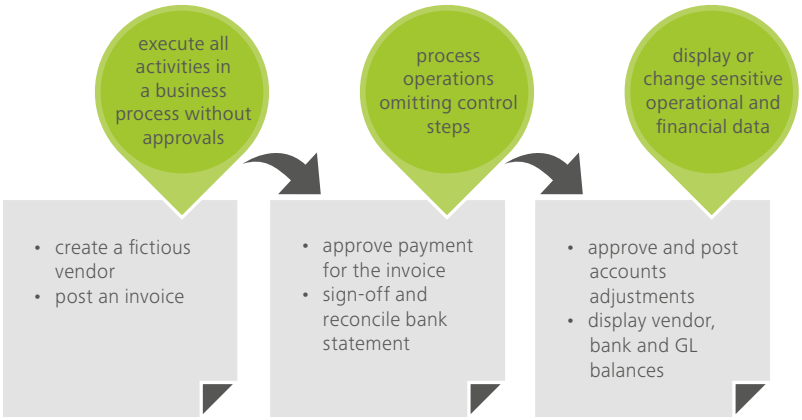
Fradulent Behaviour

- How do you prevent fraudulent behavior in your organization?
- How do you assure that your warehouse operators (blue collar) are not performing stock adjustments?
- How do you protect against the risk of paying for fictions invoices?

The basic elements of access controls for ERP systems include:

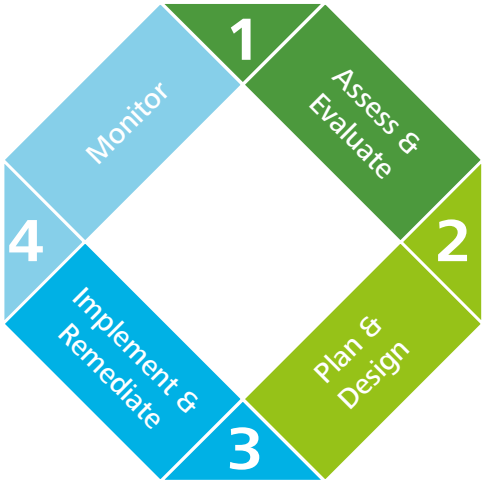
- Controls within processes of granting (and changing) user access to the ERP system, and
- Regular monitoring of users who already have access to the system.

Designing a standard process that regulates how users are granted access to the system is the first defense against data corruption and data leakage. Clearly defined steps and responsibilities between IT and business staff help to assure that only authorized personnel is given access to the system and that proper authorizations are granted to each user.



As ERP systems can support majority of business functions in organization, the concern of segregating conflicting duties is being transferred from organizational to ERP level. In IT dimension, the organization has to monitor which users are assigned conflicting combinations of access rights in ERP.

Such combinations of access rights represent conflicts of interest and create risk of fraudulent behavior by allowing one user to execute the majority of activities in the process and to skip any control and approval steps.



We follow a 4-step process:
At Deloitte we follow the 4-step process that helps your organization to better protect access to and within your ERP system.

We believe that effective internal controls are based on 3 pillars: people – process – technology.

Step 1 – assess & evaluate
First, we work with you to assess the current status of SOD conflicts as well as evaluate the maturity level of access and security controls.

Step 2 – plan & design
Depending on the results of the assessment, we can assist you in establishing an SOD program and creating control & risk awareness in the organization; re-design internal controls to better support SOD program and adjust IT processes to achieve synergy between IT department and business personnel.

Step 3 – implement & remediate
During the implementation phase, our team of experts updates and documents procedures and controls assuring that the user access management and SOD processes are well established. We develop the SOD matrix and assist you in clean-up activities (remediation). For IT related processes we streamline the processes for user access management; if required, we provide assistance in automating them.

Whenever the tools are needed, our team selects the proper technology solution adjusted to your needs.

Step 4 – monitor & operate
Once the processes are established and all technology enablers implemented, we provide you with security dashboards to facilitate regular monitoring.

	Assess & Evaluate	Plan & Design	Implement & Remediate	Monitor & Operate
People	Identify users with excessive access rights in ERP;	Establish the SOD program;	Develop & Implement SOD Matrix;	SOD risk awareness; Regular SOD checks & user access reviews;
Process	Evaluate access & security controls for ERP;	Map internal controls to SOD conflicts; Identify overlapping controls; Standardize controls across organizations;	Remediate identified SOD conflicts; Implement unified mitigating controls;	Run Security Assessment for ERP and/or GRC systems.
Technology	Run Security Assessment for ERP and/or GRC systems.	Design security dashboard; Streamline user access management processes with SOD verification;	Implement unified processes for user access management; Automate the process;	Security Dashboard; Monitor effectiveness of the process;

Stay in control and get the balance right between risk and controls to effectively run your business.

Contacts

For more information, please contact:

Erik Luysterborg
+32 2 800 23 36
eluysterborg@deloitte.com

Joanna Kazimierska
+32 2 800 23 51
jkazimierska@deloitte.com

For further information, visit our website at www.deloitte.com

2783