Internal Audit of Segregation of Duties in ERP Systems

T.V. VENKATARAMAN
tvvraman72@gmail.com

DEEPAK WADHAWAN
dewaco@gmail.com

Take your stakeholders along in ensuring that the problem identified is solved for – and not just reported

Segregation of Duties (SOD) is a basic building block of sustainable risk management and an integral element of an entity's internal control system. The objective of SOD is quite simple - no individual should be given access to two or more parts of a process that would allow him or her the opportunity to engage in financial or fraudulent activity.

T. V. Venkataraman (Venkat), who held the roles of the Chief Risk Officer (CRO) and the Chief Audit Executive (CAE) simultaneously at a large Indian corporate, provides practical insights during a conversation with Deepak Wadhawan as he shares his experiences of Segregation of Duties (SOD) reviews.

i. Question: Can you share a practical example of how excessive access gives rise to a specific risk?

Ans. Given that midsized and large organisations operate in an ERP environment, planning and management of Segregation of Duties (SOD) is one of the most critical elements in managing an organisation's internal controls in an ERP environment.

Specific risks are many: a typical example is users who have access to create a new vendor, create vendor payments, and authorise vendor payments. Similarly, in addition to SOD conflicts,

one must also review access rights to perform sensitive transactions, such as access to the creation of one-time vendors.

ii. Question: What is your expectation from line management (first line) on planning and reviewing SOD? Could you discuss this as Head of Risk and later as Internal Audit Head?

Ans. A conflict-free SOD is the desired state of this business control as it enables the right environment for transaction processing. This is the stated position of any Risk Management Department. The responsibility to define the user's roles when granting access rights (role entitlements) vests with the first line of defence (i.e., the line management of the business department in singular or jointly with the SAP support team). Where the Risk Manager/Controller role is attached to line management; in that case, the Risk Manager/Controller plays the facilitator role to line management and assists them in deciding on the roles and entitlements.

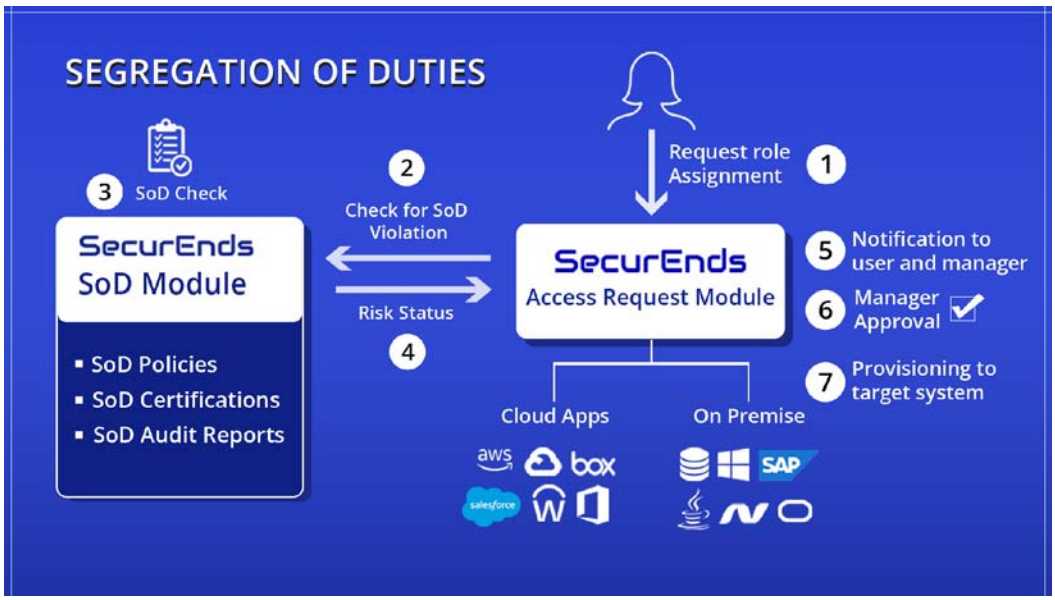
There could be instances (due to staffing constraints) where certain users may have transaction rights vested, which may pose a SOD conflict. In such cases, the departmental head should sign off the exception at the time of grant of access. Every quarter, such department head should review the transactions performed by such individuals to ensure that the transactions that are approved by role-conflicted decision makers [E.g., Receiving & Inventory adjustments; or Purchase Order & Receiving] are authorised and performed to the test of 'In line with nature of duties.'

As an Internal Auditor, I would expect the line management to apply due diligence when assigning roles to avoid role conflict or its associated risk arising in the first place, rather than doing post facto reviews, unless the situation warrants on account of staffing constraints. Finally, I expect visibility of transactions approved by users with SOD conflict roles through a monthly management report. Also, the Risk Manager/Controller (where present) should periodically test-review these transactions.

iii. Question: Should the quarterly review be done by the first line or the Risk department?

Ans. Ideally, by the first line, but in this instance, the IA team was mandated to do the review as it was felt that the IA team had the requisite competencies to understand the nature of the risks and controls required to mitigate the inherent risks. However, to clarify, there is a difference in roles between a Risk Manager/Controller attached to line management and the Risk department

iv. Question: In your experience, are internal audit reviews of SOD rights now a standard practice?



Ans. Yes, SOD reviews are typically undertaken by Internal Audit, as SOD conflicts form a high inherent risk in any risk assessment. Internal Auditors and Independent Auditors will evaluate the

business control of Segregation of Duties (SOD). This review is performed as a part of their analysis of an entity's internal controls system that supports financial reporting and safeguards organisational assets. For Internal auditors, after they have documented and understood the business process, including the IT environment, SOD reviews should form part of the overall test procedures depending on the identified control objectives.

v. Question: Where there is a SOD conflict, could you share a practical example of a compensating control that could be seen as an anti-fraud measure?

Ans. In the earlier example of multiple user profiles having access rights for creating a one-time vendor (OTV), this is a clear tell-tale sign of an elevated risk of fraudulent/ unauthorised payments. This can be mitigated by restricting the payment process to one individual through the OTV route. An oversight review over a monthly report on all payment transactions done through the OTV by the Financial Controller would be the compensating control (anti-fraud measure) for the SOD conflict.

vi. Question: In a SOD conflict situation, just having compensating control is not good enough. Please explain why?

Ans. As a recently appointed Chief Audit Executive, while going through Internal audit reports, I sensed that something was amiss at a fundamental level, given the number of similar internal control deficiencies relating to SOD conflicts identified across process assurance reviews undertaken. Individually they did not warrant a material rating of the control deficiency. Compensatory controls are monitoring controls through reviews by an independent person (usually the department head) and are always post-facto (after the event has occurred). Given my company's environment that required a dynamic transaction processing capability, these controls appeared perfunctory. A proactive user access rights management governance framework and continuous

monitoring were required to prevent fraud risk.

Ideally, preventive controls through a robust access rights provisioning governance framework implemented through an SOD management solution will arrest a substantial number of risks at the root level. However, the risk of fraud arising from collusion between individuals cannot be ruled out.

vii. Question: What in your assessment leads to SOD conflicts in organisations?

Ans. Typically, the problems start with not implementing the GRC module of the ERP, which usually contains an SOD risk analysis tool. Without the tool, easy visibility of SOD conflicts is not there, resulting in inappropriate entitlements to roles. Also, the process owner may not want to get involved while giving entitlements as they may not realise the significance of this activity. There is also a tendency of procrastination, which results in keeping role conflict unresolved, untimely deactivation of ex-employee access rights, and so forth.

viii. Question: What type of points caught the attention of the Audit Committee?

Ans. At an overall level, both the IA team and the independent auditors showcased the extent of the problem relating to SOD conflicts and sensitive access rights vested with a large number of individuals to the Audit Committee. The Audit Committee felt

that the residual risk was unacceptable and had to be mitigated on priority. This led to the formation of the CFT for risk mitigation, as outlined.

ix. Question: Could you elaborate on the SOD Risk analysis tool?

Ans. Post identification of the Internal Audit findings relating to SOD conflicts, a detailed access controls review within the ERP environment was undertaken with the support of a third-party service provider. The results showed a significant quantum of SOD conflicts and a major number of users having access to perform transactions beyond their responsibility (essentially, user profiles being vested with rights beyond their defined job roles).

Arising out of the above and at the behest of the Audit Committee, a cross-functional team was formed with IA, IT, and Finance to remediate the residual risks as a first step. One of the key outcomes achieved was the development of the SOD risk analysis tool by the in-house SAP support team.

The tool enabled performs SOD risk analysis, provides access certification by process owners, and undertakes transaction monitoring.

It was an easy-to-use front-end transaction code available for the reviewer to:

a) View the details of the transactions posted by the user against the SOD conflicts.

b) Confirm transactions performed by updating against the remarks/text column.

c) Remove conflicting roles if the same was not required/the time frame on a "need to have" basis had elapsed.

We also ensured that the tool addressed zero-tolerance conflicts, i.e., we did not give any leverage to enable zero-tolerance conflicts by any user.

x. Question: What were the challenges faced while doing the review?

Ans. From an overall project point of view, the problem statement was well known – so it boiled down to rolling up the sleeves and remediating the known risk! Having said that, the veracity of the data collated on role entitlements had to be ascertained as there were a few false positives in the user access rights data, given that some of the newer user profiles were created with historical roles as defined.

So, the cross-functional team had the following challenges:

a) Getting to validate the quality of data tabulated as SOD conflicts.

b) Making sure the users understood the need for a robust access rights management framework, undertaking workshops across locations, and creating SPOCs within the business across locations (primarily within Finance) who would champion the user access rights project.

c) Getting the departmental heads to sign off on the end user roles and responsibilities.

d) Removal of the excessive access rights based on the sign-offs received within the time frame assigned (we had two months to resolve the same, but it got extended to three months to ensure all loose ends were tied in).

e) Developing an access rights management governance framework to ensure that this risk did not manifest going forward.

xi. Question: With over a hundred roles and many times more entitlements, how did you

get the SOD project review going?

Ans. The IA function initiated an end-to-end "Access rights review" within the ERP system with an action plan, project framework and a project team. This included:

- Issuance of communication to all key stakeholders explaining the problem and requesting their support in the risk mitigation exercise.
- Appointing SPOCs within each core business/support function who would be key to track and report the closure of the identified risks concerning the removal of sensitive access rights.
- SAP support team to remove excessive rights vested with individuals as a one-time exercise and block IDs with the highest gross risk from a fraud risk perspective.
- Redundant IDs were revoked.
- Weekly monitoring cadence and reporting to the Leadership team on the function-wise status of progress instituted.

- Clean-up activity concluded in 90 days; validated by Independent auditors; status of residual risks reported to the Audit Committee.

As a way forward, the SAP support team [IT] developed an in-house SOD analysis solution (with a SOD Risk Analysis Tool) to track remediation progress and prevent further SOD conflicts.

Closing Remarks:

Last but not least, I would like to add the following pointers for an effective IA function:

a) Risks have to be seen holistically across the enterprise – and not just in silos (here, the magnitude of the issue at hand would not have surfaced if not for the IA team 'connecting the dots' across the reviews undertaken). Hence foresight, in addition to insights, is crucial.

b) Take your stakeholders along in ensuring that the problem identified is solved for – and not just reported.

c) The soft skills of the Internal Audit team are as critical if not more important than technical skills – these include skills of negotiation/persuasiveness, influencing, communication and project management.

d) It is easy to pass the buck around – "not my problem, but someone else's!" However, no one wins – the IA team will create a brand only when it has skin in the game (taking as much ownership in problem resolution) and is seen as part of the solution and not the problem itself!