feature

# Implementing Segregation of Duties

## A Practical Experience Based on Best Practices

Segregation of duties (SoD) is a central issue for enterprises to ensure compliance with laws and regulations. The importance of SoD arises from the consideration that giving a single individual complete control of a process or an asset can expose an organization to risk. Enforcing SoD is, thus, an important control element to support the achievement of an effective risk management strategy.[1, 2, 3]

This article, which contains conclusions derived from real-world SoD experience, is divided into two parts: applied methodology and implementation issues.

## Applied Methodology

The traditional approach to SoD mandates separation between individuals performing different duties. Duties, in this context, may be seen as classes, or types, of operations.

> *The basic concept underlying segregation of duties is that no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated are:*
>
> - *Authorization or approval of related transactions affecting those assets*
> - *Custody of assets*
> - *Recording or reporting of related transactions*[4]

In *IT Control Objectives for Sarbanes-Oxley, 3rd Edition*—a fourth duty—the verification or control duty is listed as potentially incompatible with the remaining three duties. This fourth duty encompasses operations that verify and review the correctness of operations made by other individuals, whether they are custody, recording or authorization operations.[5]

**Stefano Ferroni,** CISM, ISO 27001 LA, ITIL Expert
Is a senior consultant and trainer in the information and communications technology services and solutions business unit at Beta 80 Group (Italy). He concentrates on the telecommunications and finance industries. His areas of expertise include IT governance and compliance, information security, and service management. He has contributed to and guided many ISACA® white papers. He can be reached at *stefano.ferroni@beta80group.it.*

Some of the core SoD elements are actors, duties, risk, scope, activities, roles, systems and applications, and user profiles.

### Actors

When proper SoD is applied, actors performing incompatible duties are different entities. Such entities may be single individuals or groups. Requiring segregation to be applied between individuals or between collective entities gives rise to the following different levels of segregation, depending on the organizational constraints that are required for SoD to be recognized as such:

- **SoD by individuals (individual-level SoD)**—This is the traditional and most basic level of segregation. In this case, SoD is accomplished by having different duties performed by different individuals, such as clerks being authorized by their manager to make a payment.
- **SoD by functions or organizational units (unit-level SoD)**—At this level, different functions perform the separated duties. For example, the sales department might prepare an offering, which is then signed off by the operations department or the risk management function.
- **SoD by companies (company-level SoD)**—At this level, operations must be performed by different legal entities. For example, investments made by a subsidiary might require authorization by the controlling company. Third-party audits may be viewed as an example of company-level SoD as well.

### Incompatibilities

In the relevant literature about SoD,[6] duties and their incompatibilities have (unsurprisingly) been extensively analyzed. The most widely adopted SoD model requires separation between authorization (AUT), custody (CUS), recording (REC) and verification (VER).

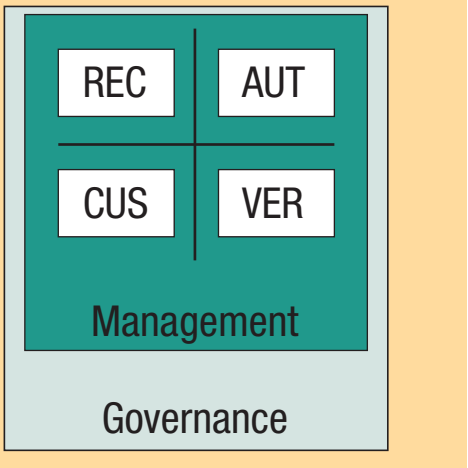
Given the lack of consensus about best practices related to SoD, another viewpoint proposes a simplified approach.[7] It divides custody and recording duties from authorization duties and introduces a third category of duties: the authorization of access grants. In this model, agents

may perform operations related to different duties on the same assets as long as they are authorized by a second person. This model embraces some common practices, e.g., a clerk receiving cash payments and entering related data in a computer application.

In addition to the aforementioned duties from the traditional model and from the simplified approach, a consistent framework should also encompass management duties (e.g., granting or revoking the proper rights to the appointed people, reporting and managing any exception to the procedures) and governance duties (evaluating, directing and monitoring SoD rules and practices in accordance with corporate governance). This alternate model encompasses some management duties within the authorization of access grant and segregates them from the other duties. The resulting model is depicted in **figure 1**.

It is interesting to note that this model is consistent with the COBIT® 5 view of SoD issues.[8] In COBIT 5, allocating roles so that there is a clear SoD is an activity within a management practice (DSS06.03), which takes direction from a governance practice (EDM04.02). Roles, responsibilities and levels of authority are established, agreed upon and communicated through a second management practice (APO01.02).

**Figure 1—Alternate SoD Model**




**Source:** Stefano Ferroni. Reprinted with permission.

From those considerations, it can be assumed that, for efficiency and for economic reasons, an effective SoD may be achieved by relaxing the requirements for separation between operational duties, such as custody and recording, as long as they are subject to independent authorization or verification.[9] Note that, in some cases, such segregation is simply impossible to achieve, e.g., when a recording operation creates an automatic payment (thus giving rise to a custody duty). In some cases, separation may not be required between control duties such as authorization and verification, which are often delegated to the same authority.

Whenever such simplifications are introduced, some may be concerned that SoD is weakened to the point that it becomes ineffective. To address such concerns, compensating controls can be introduced after thorough risk analysis[10] to reduce the vulnerabilities in ineffectively segregated functions, which include the risk of errors, omissions, irregularities and deficiencies in process quality. For example, if recording and custody are combined, independent authorization and verification (e.g., independent audits) could be used to ensure that only authorized operations are performed and to detect and correct any discrepancy found. When proper SoD cannot be enforced, the need for compensating controls is widely recognized in current practice among enterprises and institutions.[11, 12]

### Risk and Risk Scenarios

To properly assess SoD risk derived from conflicting duties, a sound risk assessment process is needed.[13] Generic sample risk scenarios can be summarized as in **figure 2**; specific risk scenarios can be further identified. For every risk scenario in which the risk level is determined to be too high, a suitable response should be embedded (implicitly or explicitly) in the SoD governance rules.

**Figure 2** describes the risk arising when proper SoD is not enforced; for every combination of conflicting duties, it reports one or more generic, related risk

categories, along with some risk scenario examples. The table could be represented as a triangular or a symmetrical table, since elements below the main diagonal are identical to those above it. This derives from the observation that if c(X,Y) denotes duty X conflicting with duty Y, then it can be assumed that c(X,Y) is equivalent to c(Y,X), while c(X,X) would violate the principles of SoD. The first observation means that one can assume that, for example, given that custody is incompatible with authorization due to the risk of embezzlement, then, for the same reason, authorization is incompatible with custody: the cell at row CUS, column AUT and the cell at row AUT, column CUS should be identical. The second observation means that, for example, custody is always compatible with custody, so c(CUS, CUS) cannot be true and the corresponding cell can be safely omitted from the matrix.

Governance is not included in **figure 2** since risk factors due to lack of governance are less specific and more difficult to match with single duties (nonetheless, they may have high impacts on businesses). Lack of governance may result in general inconsistencies or a possibly fraudulent attribution of conflicting duties to the same actor.

An effective SoD mitigates all risk deriving from the risk scenarios presented in **figure 2**. Still, SoD governance may benefit from introducing further controls to reduce risk to acceptable levels. For example, third-party audits by a separate function (e.g., internal audit) or an external entity (e.g., external audit) may be beneficial. In this case, a function-level or company-level SoD may be used, for example, to assess effectiveness of individual-level SoD. This is a secondary level of controls that provides assurance about the effectiveness of existing SoD controls.

### Scope

In the literature about SoD, there is not much discussion about scoping SoD requirements. But scoping is a central topic for the correct assessment

**Figure 2—Risk Scenario Examples**

| | CUS | | AUT | | VER | | MGMT | |
|---|---|---|---|---|---|---|---|---|
| | Risk Category | Risk Scenario Examples | Risk Category | Risk Scenario Examples | Risk Category | Risk Scenario Examples | Risk Category | Risk Scenario Examples |
| REC | Material error | Undetected input of incorrect data | Embezzlement | A rogue authorizer enters forged data. | Fraud, embezzlement | Forged records go undetected. | Fraud, embezzlement | Recording grants are given to unauthorized people; privilege elevation. |
| | Fraud | Recorded data do not correspond to real money exchange. | | | | | | |
| CUS | | | Embezzlement | A rogue authorizer diverts money to his/her advantage. | Fraud, embezzlement | Frauds related to the material handling of assets (e.g., money diversion) go undetected. | Fraud, embezzlement | Custody grants are given to unauthorized people; privilege elevation. |
| AUT | | | | | Fraud, embezzlement | Misuse of authorization grants goes undetected. | Fraud, embezzlement | Privilege elevation |
| VER | | | | | | | Fraud, embezzlement | Privilege elevation |

**Source:** Stefano Ferroni. Reprinted with permission.

of SoD within an organization. In fact, checking SoD among all actors against all activities in a complex enterprise, aside from being impractical, would be meaningless.

**Assets as Scoping Boundaries**

The first scoping considerations involve assets. Duties that are related to an asset should be segregated.[14] An individual may be in charge of different duties as long as they do not involve the same asset. This kind of SoD is allowed in some SoD models.[15]

Again, SoD may be accomplished on different levels. In some cases, segregation is effective even when some conflict is apparently in place. For example, two employees may be in charge of recording and authorizing transactions on the same set of assets, provided that, for every single asset, one employee records the transaction's data and the other employee authorizes the operation.

In this case, if assets are, for instance, accounts receivable, two employees can both record the account receivable data and authorize transactions. For every single account receivable, one employee records the data and the other employee authorizes the related transaction; roles can be inverted between the two employees when a second account receivable is processed. The traditional form of segregation leaves all authorizations to an individual (e.g., the department manager) and custody or recording operations to a second individual.[16]

Therefore, the first scoping rule is that duties must be segregated for every single asset to avoid conflicts (as in the first example in which two employees exchange their duties). More commonly, particularly in medium or large enterprises, duties are segregated with respect to a set of assets (as in the second example, in which authorization for paying accounts receivable is performed by the department manager).

**Processes as Scoping Boundaries**

A second boundary may be created by the processes that transform the assets or their status. Again, such boundaries must be assessed to determine if they introduce any residual risk. "Considering processes and [risk factors] outside of the system are just as important as those inside the system, if one wants to look at fraud risk holistically."[17] For example, a manager may authorize payments for accounts receivable; the same manager might use the same data coming from accounts receivable to draft a report to be shared with the company's executives.

In the first case, there are two assets involved: the accounts receivable and the related amount of money. The manager performs an authorization duty. In the second case, there are still two assets: the accounts receivable and the report. But in this scenario, the manager performs a recording duty. Processes are separate, but they are related to an asset they have in common. The second process carries some risk related to SoD due to conflicting activities on the same asset. Duties can be seen, then, as properly separated if there is a set of controls on each process so that the risk is properly mitigated (e.g., authorizations are independently verified and reconciled and reports are independently checked against accounts receivable).

Thus, it can be said that in SoD, the scope may be limited to a process or a set of processes that creates an asset or transforms it, bringing the asset itself from one stable state to another stable state.

In summary, the scope in which to look for SoD conflicts can be defined by the assets that are involved and by a set of processes that operates on them.

Applying scoping rules to demarcate the playing field can provide numerous advantages during the implementation phase. They also introduce some risk, namely the risk of not detecting some conflict

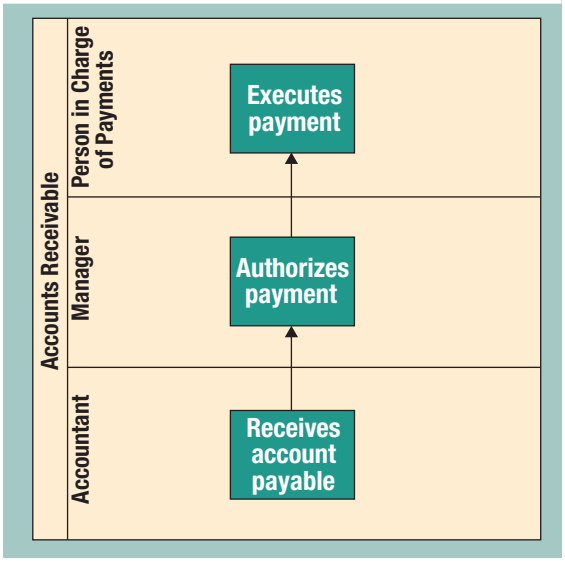
(e.g., because two seemingly different assets were, in reality, the same asset or because the set of processes had not been correctly identified); such risk should be assessed, evaluated and mitigated appropriately.[18]

## Implementation Issues

In enterprises, process activities are often described by means of some procedure or in a diagram in some standard notation, such as a business process model and notation. Often, these descriptions are at a level of detail that does not immediately match with duties as previously defined. This may generate confusion when checking to see if there has been some kind of conflict in the attribution of duties. For example, **figure 3** shows a schematic example of a fictitious accounts receivable process. It is only a part of the process and is grossly simplified, but it helps to illustrate this point.

In such a process description, one can easily attribute duties to the three actors involved: the accountant, who performs a custody duty or possibly a recording duty; the manager, who authorizes payment, which is an authorization duty; and the person in charge of payments, who performs a custody duty. There are no individuals performing two different duties; there are two individuals performing the same duty (a custody duty). There are no conflicts.

**Figure 3—Accounts Receivable Process**




**Source:** Stefano Ferroni. Reprinted with permission.

Process descriptions may be described at a closer level of detail in the enterprises. The previously discussed process is depicted in **figure 4**.

In this case, duties cannot be matched directly to activities. Each of the actors in the process executes activities, which apparently relate to different duties. For example, the accountant who receives a payment performs a series of checks against order details before sending the invoice to the manager for approval, possibly suspending the invoice until any discrepancy has been fixed. Such checking activity may be viewed as an authorization duty or a verification/control duty. Similarly, the person in charge of payments performs some checks before fulfilling the payment request.

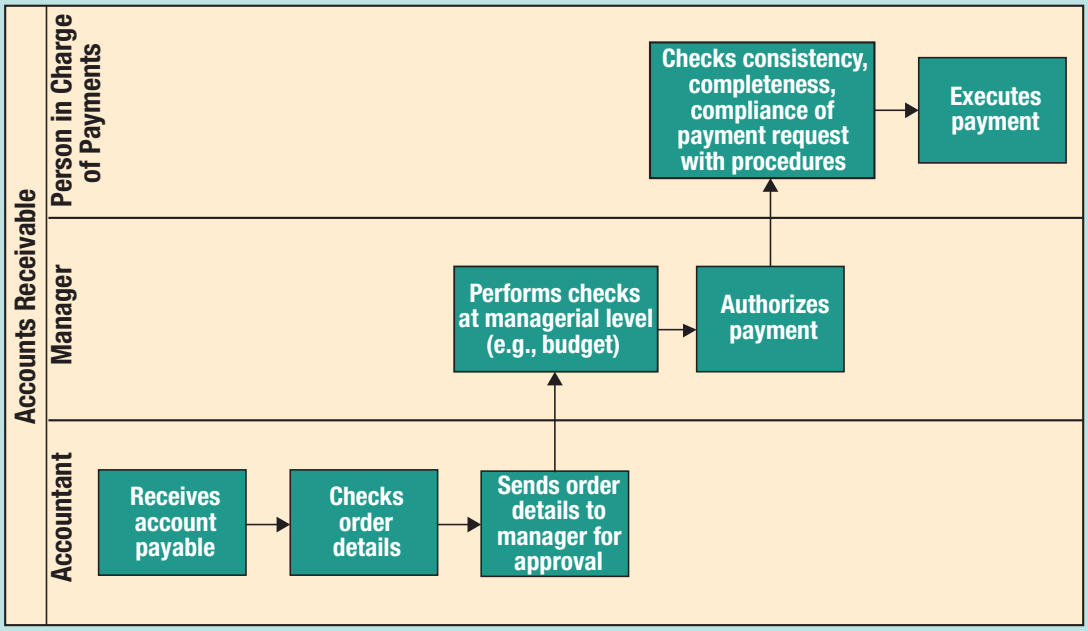
In both cases, at first glance, such activities may seem to conflict with other activities performed by the same actor, but this is not the case. Such conflicts can be seen as purely formal, since they are caused by the form that a procedure has taken (i.e., the level of detail) and not by the very essence of the activities themselves. Preliminary activities requiring verifications from every actor involved are the very reason to invoke SoD: They provide a consistent set of checks and balances that ensures that operations abide by rules and procedures.

### Mapping Activities With Duties

A visual depiction of processes can be used as the basis to build a matrix of activities, which are then checked for incompatibilities.[19] Those who evaluate SoD on processes written at this high level of detail should consider doing the following:

1. Alter the process description by grouping or removing activities in order to hide details that are not relevant to SoD.

**Figure 4—Accounts Receivable SoD in Detail**




**Source:** Stefano Ferroni. Reprinted with permission.

2. Keep all the activities in the matrices, but label any formal conflict as such; do not raise any exception to the rules of SoD in case of formal conflicts.

The first choice has the advantage in that it reduces the size of the matrices. On the downside, it is detached from the approved representation of processes, requires some preliminary effort, and may introduce errors or oversimplifications. The second alternative generates huge matrices, but keeps them aligned with the existing representation of processes and to their practical implementation.

Both of these methods were tested, and it was found that the first one was more effective. Matrices were more manageable. Since the number of activities was reduced, this approach led to a more effective and focused examination of possible SoD conflicts when validating results with the process owners. Not all false conflicts were eliminated, though. In some cases, conflicting activities remained, but the conflict was on only a purely formal level.

### Managing Conflicts

Detected conflicts can be managed by modifying processes, e.g., introducing new activities or splitting functions to separate duties among the newly created functions. Eliminating some conflicts may be impractical or too expensive sometimes; in such cases, risk should be assessed and properly managed.[20, 21]

The SoD implementation tested for this article listed more than 80 potential SoD conflicts, along with the compensating controls that had been applied to reduce risk to acceptable levels.

### Roles and Role Engineering

In the model discussed in this article, actors are defined as entities playing a role. Roles may be generic (e.g., requester) or specific (e.g., purchasing department manager). Either way, they are associated with one or more process activities.

Role engineering is a discipline in itself, aimed at defining a common set of roles that can be used to assign to users grants and privileges on applications in a consistent and repeatable way.[22] Role-based access control (RBAC) follows some common models, as described by the American National Standards Institute (ANSI) standard 359-2004.[23]

Role-engineering processes may follow two main approaches: a top-down approach (i.e., a business-driven approach in which roles are defined based on the users' job descriptions) or a bottom-up approach (i.e., roles are inferred by examining existing grants and permissions on systems and applications). The latter technique is often known as role mining. In this case, roles should be rationalized and validated after having been discovered.

Top-down and bottom-up approaches may be used simultaneously to complement each other, giving rise to the third common alternative, the hybrid approach, which is often claimed to be the most valid approach.[24, 25] The implementation examined in this article used a hybrid-like approach to match the business view of user activities with the actual permissions granted on systems and applications. On the top-down side of the approach, the organization was analyzed to determine what the roles were for every department, function or office involved. Then, roles were matched with actors described in process-flow diagrams and procedures. This resulted in the ability to match individuals in the process flow with a specific job description within the organization.

**Systems and Applications**

The access rights granted to individuals were assessed to gather information about systems and applications. This is a (bottom-up) role-mining activity, which was performed by leveraging the identity management product chosen for the implementation of the identity management system.

There was also a second source of information about applications and systems. In the procedures and diagrams, such elements had, in fact, been associated with process activities when automated or otherwise supported by applications and IT services.

For example, for all employees in a given office, role mining contained a list of the permissions they had been granted on the applications that support the enterprise architecture of the company. Then, the actual permissions provided to users on applications and systems (from role mining) was compared to the intended use of IT services (from procedures and diagrams). In cases of mismatch, it was possible to check if excessive grants had been provided to users or if process and activity descriptions were inaccurate and needed to be updated.

Roles can be composed hierarchically; in this case, simpler roles act as building blocks that must be combined to form a single role. For example, an accountant may have a role built as a composition of generic building blocks, such as employee; less-generic blocks, such as member of the financial department; and specific blocks that are closely related to the accountant role.

**Profiles**

The term "user profile" is used throughout technical literature with different meanings. In this article, a user profile is defined as a set of permissions granted on a single application or system. Profiles are related to roles, which means that from the perspective of applications and systems, a role can be thought of as a collection of user profiles.

The hybrid approach provides some clear benefits:

- Grants on the applications can be matched with roles, leading to optimal and consistent attribution of grants to the users.
- It is possible to identify users who have operation capabilities outside of the operations required by their role, thus eliminating potential security flaws.
- Unnecessary and redundant roles can be detected and eliminated.
- User profiles can be designed more effectively based on role-mining results.

In implementing roles with the support of an identity management system, a balance has to be achieved when legacy systems are involved. The conflict is between keeping all profile details and the grants associated with systems and applications on one side and keeping the complete user profile on the applications and systems on the other side. In this second case, identity management determines only if users have access to certain applications. (Such profiles are called "Yes/No" profiles, meaning that a user is either authorized or not authorized to access an application.)

**Detecting Conflicts on the Rise**

Conflicts originate from the attribution of conflicting duties to the same actor. This may happen because activities related to two conflicting duties have been associated with the same role (e.g., custody, authorization). In this case, conflicts are introduced while designing processes, procedures and roles. In practice, conflicts arise more frequently because two conflicting roles are attributed to the same individual while creating or modifying the individual's account. Moreover, in the case of a profile change, an individual may be asked to temporarily play two roles in order to guarantee a smooth transition from the previous role to the next.

In such cases, SoD rules may be enforced by a proper configuration of rules within identity management tools. Such rules can detect a conflicting assignment in the creation or modification phase and report such violations. A more complex and flexible set of rules is needed if dynamic RBAC is to be applied.

## Conclusion

SoD is a control and, as such, should be viewed within the frame of risk management activities. This key element must be kept in mind when assessing potential conflicts and designing rules.

Processes must be thoroughly analyzed and some choices have to be made to detect and resolve potential conflicts. If any conflicts are left, some compensating control must be put in place to properly manage the associated risk.

Role engineering plays a significant role in supporting SoD rules within an identity management system, as it enforces access rights and detects conflicts as they happen. Finally, and most important, SoD requires a clear understanding of actors, roles and potential conflicts. As Kurt Lewin said, "There's nothing more practical than a good theory."[26]

## Endnotes


1 Singleton, T.; "What Every IT Auditor Should Know About Proper Segregation of Incompatible IT Activities," *ISACA® Journal*, vol. 6, 2012, *www.isaca.org/Journal/archives*

2 Ghosn, A.; "Segregation of Duties," American Institute of Certified Public Accountants, 2014, *https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Auditing/InternalControl/Pages/value-strategy-through-segregation-of-duties.aspx*

3 Ernst & Young, "A Risk-based Approach to Segregation of Duties," *Insights on Governance, Risk and Compliance*, May 2010, *www.ey.com/Publication/vwLUAssets/EY_Segregation_of_duties/$FILE/EY_Segregation_of_duties.pdf*

4 ISACA, *IT Control Objectives for Sarbanes-Oxley: Using COBIT® 5 in the Design and Implementation of Internal Controls Over Financial Reporting, 3rd Edition*, USA, 2014, www.isaca.org/cobit

5 *Ibid.*
6 Kobelsky, K.; "A Conceptual Model for Segregation of Duties: Integrating Theory and Practice for Manual and IT-supported Processes," *International Journal of Accounting Information Systems*, 15(4), 2014a, p. 304-322
7 ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, *www.isaca.org/cobit*
8 Kobelsky, K.; "Enhancing IT Governance With a Simplified Approach to Segregation of Duties," *ISACA Journal*, vol. 4, 2014, *www.isaca.org/Journal/archives*
9 Hare, J.; "Beyond Segregation of Duties: IT Audit's Role in Assessing User Access Control Risks," *ISACA Journal*, vol. 5, 2009, *www.isaca.org/Journal/archives*
10 Yale University, "Segregation of Duties," 17 November 2008, *www.yale.edu/auditing/balancing/segregation_duties.html*
11 Office of Risk and Internal Controls Service, *Control Awareness Bulletin—The Use of Compensating Controls*, Dartmouth College, 17 February 2012, *www.dartmouth.edu/~rmi/documentsunprotect/theuseofcompensatingcontrols.pdf*
12 *Op cit,* Hare
13 *Op cit,* ISACA, 2014
14 *Op cit,* Kobelsky, 2014
15 ISACA, *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, USA, 2006
16 *Op cit,* Hare
17 *Ibid.*
18 *Op cit,* ISACA, 2006
19 *Op cit,* Singleton
20 *Op cit,* Ernst & Young
21 Vanamali, S.; "Role Engineering: The Cornerstone of RBAC," *ISACA Journal*, vol. 3, 2008, *www.isaca.org/Journal/archives*
22 ANSI-INCITS, "ANSI/INCITS 359-2004," *Information Technology—Role-Based Access Control*, American National Standards Institute (ANSI) and InterNational Committee for Information Technology Standards (INCITS), 2004
23 *Ibid.*
24 Colantonio, A.; *Role Mining Techniques To Improve RBAC Administration*, Rome, Italy, 2011
25 Kern, A.; M. Kuhlmann; A. Schaad; J. Moffett; *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies*, SACMAT '02, p. 43-51, Monterey, California, USA, 2002
26 Kurt Lewin, 1890-1947, was a German-born American social psychologist known for his theory that human behavior is a function of an individual's psychological environment. Encyclopaedia Britannica, *www.britannica.com/biography/kurt-lewin*