Maciej Szkoda
Politechnika Krakowska im. Tadeusza Kościuszki
E-mail: maciej.szkoda@mech.pk.edu.pl
Kacper Cieplik
Politechnika Krakowska im. Tadeusza Kościuszki
E-mail: cieplikkacper@gmail.com

ANALYSIS OF SoD CONFLICTS IN SAP ERP SYSTEM LOGISTICS WITH THE USE OF THE SAP GRC APPLICATION

ABSTRACT

Background: Nowadays, the management and integration of various areas in an enterprise require the implementation of an adequate IT system. There are many such systems, often intended for enterprises of various sizes and industries. An example of an integrated IT system which offers comprehensive support to logistic processes is SAP ERP. In order to perform the different tasks, it is necessary to allocate relevant permissions to system users. Permission management in IT systems is necessary for protecting data against accidental, malicious manipulations, damage or unintentional wrong use.

Methods: The analysis of users' permissions in SAP ERP and identification of SoD conflicts, if any, is performed automatically in practice, with the use of analytical tools matching the task. In order to get full control over the process of conflict identification and resolution, managing staff decide to implement the appropriate tool of the GRC (Governance Risk and Compliance) class. One of the solutions of the type is the dedicated SAP solution – SAP GRC Access Control. The SoD conflict matrix identified in the analysis is translated into so-called Rulebook written in the form of a specialist scheme integrated with the SAP GRC application. The set contains information about the business processes going on in the enterprise (e.g. materials management or purchases), identified business functions (e.g. acceptance of orders or stock taking exercises) and conflicts. It also includes, inter alia, identifiers of conflict creating functions, their level and type as well as the status of activity in the system (on / off).

Brzeziński Ł. et al. (Eds.), Modern solutions in production and warehousing, Spatium, Radom 2019.
https://doi.org/10.17270/B.M.978-83-66017-87-0.8

Results: In the chapter, 17 examples of SoD conflicts are identified for the logistics of the SAP system which, after a user is given too wide access, may involve the risk of wilful or unintentional abuse having a negative effect on the enterprise.

Conclusions: In order to prevent situations of this type, enterprises use applications which supervise users' permissions. One of such applications is SAP GRC Access Control. This tool supports user- and role-level analyses, enabling automatic support for the process of resolving SoD conflicts, which reduces to the minimum the need to do manual analyses of large quantities of data whilst minimizing the probability of committing errors.

Keywords: SAP ERP, SAP GRC, User permissions, Segregation of Duties (SoD)

INTRODUCTION

IT systems are tools which make extensive functionalities available to users enabling them to process large data quantities. Nowadays, the management and integration of various areas in an enterprise require the implementation of an adequate IT system. There are many such systems, often intended for enterprises of various sizes and industries [Cieplik 2018]. An example of an integrated IT system which offers comprehensive support to logistic processes is SAP ERP. It is a fully integrated application which meets the principal business requirements of medium and large-sized businesses of all industries and market sectors. The system covers a wide spectrum of business processes helping firms carry out their financial operations, manage their personnel, perform logistic tasks, design and manufacture products, as well as carry out sales and servicing [Szkoda 2008, Lorenc and Szkoda 2015].

In order to perform the different tasks, it is necessary to allocate relevant permissions to system users. Permission management in IT systems is necessary for protecting data against accidental, malicious manipulations, damage or unintentional wrong use [Lamotte-Schubert and Weidenbach 2009]. In SAP systems, user permissions are role-based (Fig. 1). Role in SAP system can be described as compilation of transactions and permissions that are assigned to one or more user master records; usually includes commonality amongst a job role or job task [Juran 2016]. With the appropriate role assigned in the SAP, the user gets the possibility of performing specific activities within it, e.g. using a transaction, generating a report or obtaining information from a data table. The required authorizations are designed within the roles and assigned to the particular users [Cieplik, 2018]. The principal role components include:

Brzeziński Ł. et al. (Eds.), Modern solutions in production and warehousing, Spatium, Radom 2019.
https://doi.org/10.17270/B.M.978-83-66017-87-0.8

- Transactions – unique codes enabling the performance of programmes / operations in the SAP system;
- Authorization objects – logical units grouping authorization fields together with values allocated thereto;
- Authorizations – combinations of authorization objects and values detailed in the fields.

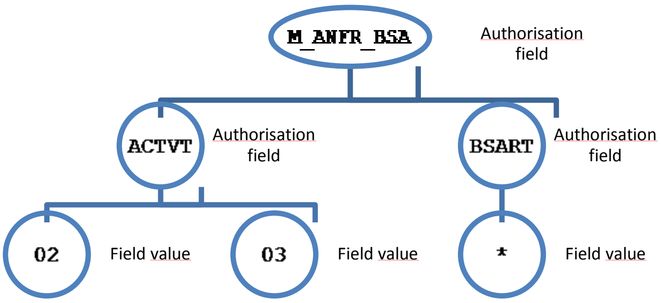


Fig. 1. Authorization concept in SAP based on an M_ANFR_BSA object. Source: own work.

SoD CONFLICT

In enterprises, duly qualified staff are allocated to each business process and then permissions are assigned to the employees' accounts enabling them to perform their tasks. Compared to other complex and complicated processes in the enterprise, this process seems to be relatively simple. It often transpires, however, that increasing dependence of the implementation of business processes on their complex supporting IT systems reveals threats which result from the allocation of too wide permissions in the IT system, which often do not correspond to their employee responsibilities, and from the lack of due segregation of duties (SoD). Challenges of this type are identified in each area of the enterprise, including finance, manufacturing, human resources management or logistics [Cieplik 2018].

A SoD conflict occurs when a user who is an enterprise's employee holds excessive permissions in the IT system to be able to perform activities which, from the viewpoint of:

- internal control,
- security of processes in the firm,
- good business practices,
- legal regulations,
- should be segregated and performed by at least two staff members.

Excessive permissions in ERP systems may lead to:

- abuse,
- unintentional mistake or incorrect feeding of data,
- use of excessive access by third parties (the liability rests with the holder of the account in the IT system).

It is to be borne in mind, however, that segregation of duties does not resolve the issue of potential abuse completely. It minimizes the probability that an event will occur which has a negative effect on the enterprise’s operations. After successful segregation of duties, an abuse requires an agreement between two or more employees. Since it is difficult to establish such an agreement and keep it secret, segregation of duties increases the chances for identifying such abuses within the organization [Dudek 2018].

An example of a SoD abuse may be a recent situation in one of US corporations whose IT Vice-President developed a fraud method to generate false invoices and approve payments for the enterprise’s services. That resulted in the generation of losses of more than USD 8 million. Had the duties within the system been duly segregated, the user would not have been able to perform both actions and hence would not have committed the fraud [www.casewareanalytics.com].

Another example of failure to follow appropriate procedures and control permissions in an enterprise is the situation which occurred in 2018 in Poland. Cenzin, a company of Polska Grupa Zbrojeniowa, operating in the international market of trade in armaments and special equipment, transferred, in several tranches, PLN 4 million to a fake bank account. The fraud was probably committed by phishing which involves sending out emails using an address “similar” to an address known to the business partners. Having received the email, the persons in charge introduced changes in the system of payments for goods from a Czech supplier and made the payment to a new account. The lack of confirmation of the bank account and a two-level approval of the information (additional verification of the change), so important from the viewpoint of the enterprise, enabled a theft of PLN 4 million [www.rp.pl].

The situations described above demonstrate that the granting of the appropriate permissions to IT system users and their monitoring is necessary today for correct, effective and secure performance of business processes.

IDENTIFICATION OF BUSINESS ACTIVITIES IN THE SAP SYSTEM

Brzeziński Ł. et al. (Eds.), Modern solutions in production and warehousing, Spatium, Radom 2019.
https://doi.org/10.17270/B.M.978-83-66017-87-0.8

In order to proactively identify threats involved in the allocation of too wide permissions to system users, it is necessary to analyze the enterprise's business processes. The first stage in this analysis is to identify the business activities (business functions) which may give rise to SoD conflicts. Business activities performed by the staff in an organization may depend on its type, i.e. logistic tasks a in telecom service provider may differ from those performed by manufacturing companies.

Identification of business activities which are mapped in the SAP system requires the involvement of all of the enterprise's departments. Each of them should specify what tasks it performs, with what frequency and which of them are done through SAP. It is also a good practice to include activities which, due to the firm's policy or internal arrangements, are not mapped in the ERP system (hardcopy documentation). Useful in the identification are all specifications and instructions helping staff perform their daily duties. These often include processes with transaction codes used by the SAP system end users. The table presents examples of business logistic activities performed in the SAP ERP system.

Table 1. Examples of business logistic activities performed in the SAP ERP system

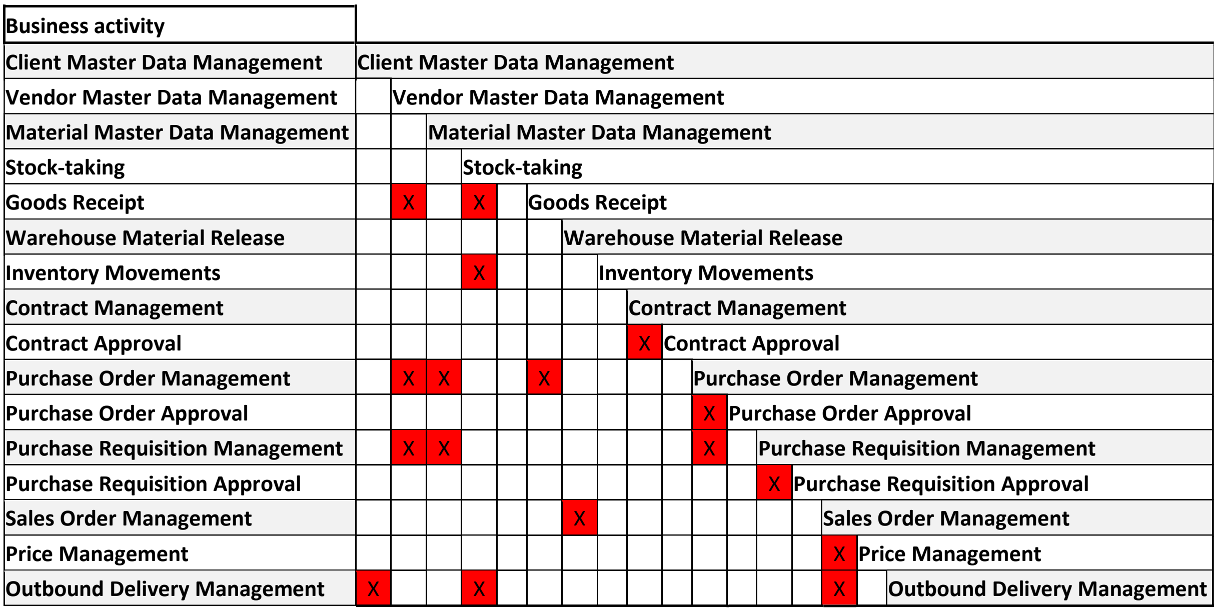
Client Master Data Management	Warehouse Material Release	Purchase Order Approval
Vendor Master Data Management	Inventory Movements	Purchase Requisition Management and Purchase Requisition Approval
Material Master Data Management	Contract Management	Sales Order Management
Stock-taking	Contract Approval	Price Management
Goods Receipt	Purchase Order Management	Outbound Delivery Management

Source: own work based on [Szkoda 2010, Szkoda M 2014].

Based on the activities presented in the table 1, a SoD matrix can be built which provides a graphic representation of all key business process elements for which combined access for the user (and, as a result, the potential of the user performing activities) will have a real impact on the enterprise's operations. In practice, for each combination (this is usually a matrix in the form of parallel access to two activities within the system), the risk level and the number are defined, the person in charge is identified and a description is provided to indicate the impact of this combination of permissions on the organization [Dudek 2018].

For the purposes of this chapter, an example of a SoD matrix has been defined which illustrates potential SoD conflicts in logistics (Fig. 2).

https://doi.org/10.17270/B.M.978-83-66017-87-0.8



Business activity																	
Client Master Data Management	Client Master Data Management																
Vendor Master Data Management		Vendor Master Data Management															
Material Master Data Management			Material Master Data Management														
Stock-taking				Stock-taking													
Goods Receipt		X		X		Goods Receipt											
Warehouse Material Release							Warehouse Material Release										
Inventory Movements				X				Inventory Movements									
Contract Management									Contract Management								
Contract Approval									X	Contract Approval							
Purchase Order Management		X	X			X					Purchase Order Management						
Purchase Order Approval											X	Purchase Order Approval					
Purchase Requisition Management		X	X								X		Purchase Requisition Management				
Purchase Requisition Approval													X	Purchase Requisition Approval			
Sales Order Management							X								Sales Order Management		
Price Management															X	Price Management	
Outbound Delivery Management	X			X											X		Outbound Delivery Management

Fig. 2. Authorization concept in SAP based on an M_ANFR_BSA object. Source: own work.

A parallel access of a user to both activities (marked red at the intersection in the matrix) may result in:

- generation of fictitious orders in the system,
- organization of supplies to a wrong recipient's address,
- execution of payments to wrong bank accounts,
- payments for supplies / services which in fact did not exist,
- unfounded release of goods from the warehouse,
- sale of products at understated prices,
- uncontrolled manipulation of stock levels,
- errors in warehousing operations,
- actions contrary to the firm's policy or without the authorized persons being aware thereof,
- actions contrary to the organization's business objectives.

In order to prevent infringements, tools should be implemented to enable automated identification of existing and new conflicts. The challenge is considerable since the process of granting and cancelling permissions must function on a continuous basis in the enterprise, and hence the users' permissions are continuously modified. Newly hired staff often need an account in the system to perform their duties. Each new user account means new specific permissions which may involve new access risks. Likewise, when an employee leaves, his or her permissions are passed on to others which requires increased permissions for system users so that then can freely perform their new tasks until a new employee is recruited.

Brzeziński Ł. et al. (Eds.), Modern solutions in production and warehousing, Spatium, Radom 2019.
https://doi.org/10.17270/B.M.978-83-66017-87-0.8

Minimization of the risk of an abuse requires a tool which ensures proactive monitoring to inform administrators about new threats and enable regular comparative analyses to be made of potential SoD conflicts in the system.

SAP GRC ACCESS CONTROL APPLICATION

The analysis of users' permissions in SAP ERP and identification of SoD conflicts, if any, is performed automatically in practice, with the use of analytical tools matching the task. Manual analysis, through manual checks of users' permissions by means of SAP transactions (e.g. SU01, PFCG, SUIM) or tables (e.g. AGR*) and identification thereof with the conflicts found before would be very time consuming due to the complexity and variety of the roles assigned to the users.

In order to get full control over the process of conflict identification and resolution, managing staff decide to implement the appropriate tool of the GRC class. In July 2011, SAP launched its new product, SAP GRC 10.0, consisting of the main components Process Control (PC), Risk Management (RM), and **Access Control (AC)** [Chuprunov 2011]

Five integrated modules are be distinguished in the SAP Access Control application. These are:

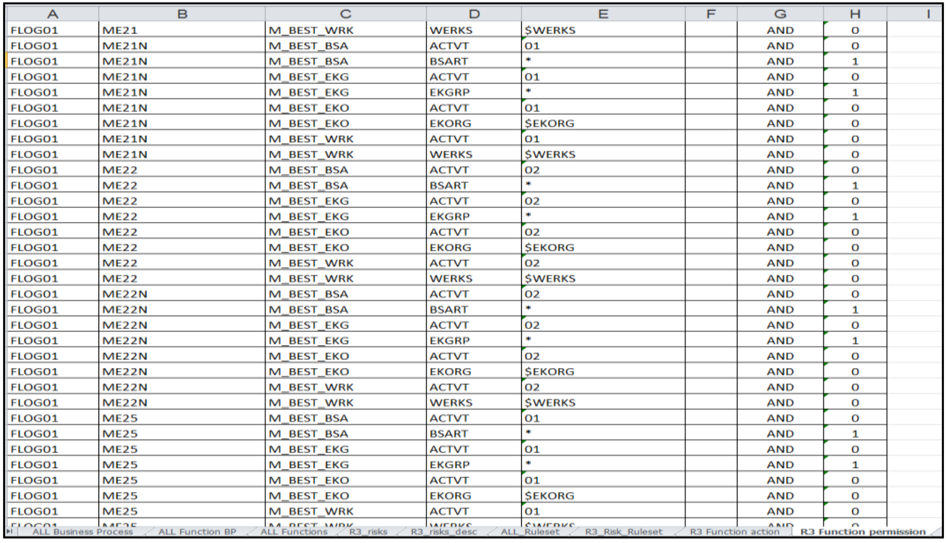
- Emergency Access Management (EAM) – enabling privileged access to SAP systems. It is often used in emergency situations in which quick access is required to an account with wide permissions and in the work of IT consultants. Each action in the dedicated account is monitored and verified by the designated person (Controller).
- Business Role Management (BRM) – supporting the process of managing the catalogue of roles in a manner which is friendly to business users. It facilitates the activities relating to role design, creation, definition and testing.
- Access Request Management (ARM) – automating request-based process of managing users and their permissions. It offers a possibility of designing unique approval paths for particular types of requests (New account, Granting and withdrawing permissions, Blocking the account, Access to privileged accounts).
- User Access Review (UAR) – enabling the automation of periodical reviews of users' access to regularly cancel excessive permissions (e.g. wrongly assigned roles or accesses remaining after change of position within the firm).
- Access Risk Analysis (ARA) – dedicated module enabling identification of threats involved in incorrect segregation of tasks (SoD) in the enterprise.

APPLICATION OF THE ARA MODULE OF THE SAP GRC ACCESS CONTROL SYSTEM IN SoD CONFLICT RESOLUTION IN LOGISTICS

The SoD conflict matrix identified in the analysis is translated into so-called Rulebook written in the form of a specialist scheme integrated with the SAP GRC application. The set contains information about the business processes going on in the enterprise (e.g. materials management or purchases), identified business functions (e.g. acceptance of orders or stock taking exercises) and conflicts. It also includes, *inter alia*, identifiers of conflict creating functions, their level and type as well as the status of activity in the system (on / off).

In order to draft such a Rulebook (Table 2), a list of transactions and authorisations should be allocated to each identified activity (combinations of authorisation objects and values detailed in the fields) which, technically speaking, enable the performance of the business activity in the system. The source of mapping the functions from the SoD Matrix to the activities / transactions and authorisation objects may be, initially, a set of best practices for the selected environment. It is to be borne in mind, however, that it should be adapted to the specific requirements [Dudek 2018].

Table 2. Example of a fragment of an access rule set



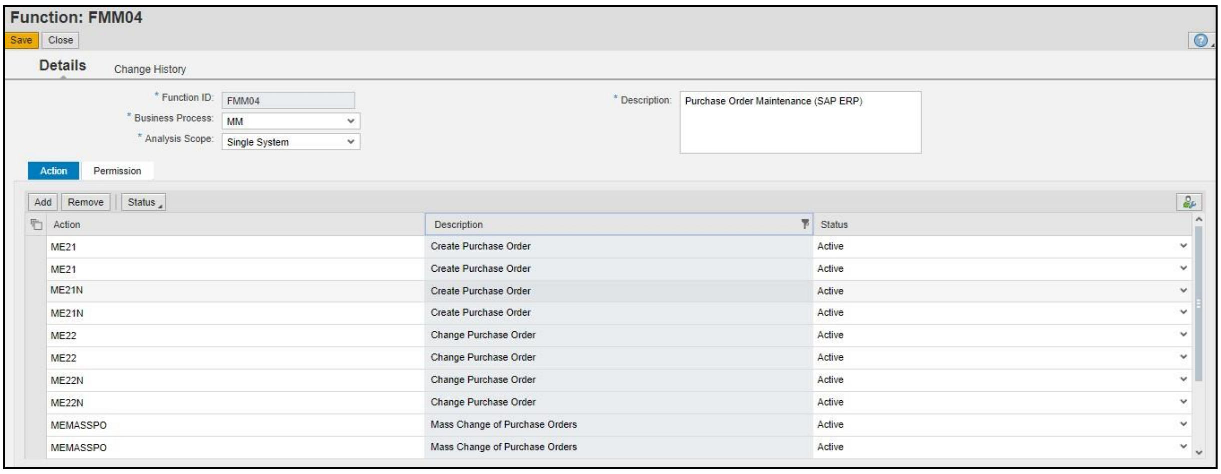
A	B	C	D	E	F	G	H	I
FLOG01	ME21	M_BEST_WRK	WERKS	$WERKS		AND	0	
FLOG01	ME21N	M_BEST_BSA	ACTVT	01		AND	0	
FLOG01	ME21N	M_BEST_BSA	BSART	*		AND	1	
FLOG01	ME21N	M_BEST_EKG	ACTVT	01		AND	0	
FLOG01	ME21N	M_BEST_EKG	EKGRP	*		AND	1	
FLOG01	ME21N	M_BEST_EKO	ACTVT	01		AND	0	
FLOG01	ME21N	M_BEST_EKO	EKORG	$EKORG		AND	0	
FLOG01	ME21N	M_BEST_WRK	ACTVT	01		AND	0	
FLOG01	ME21N	M_BEST_WRK	WERKS	$WERKS		AND	0	
FLOG01	ME22	M_BEST_BSA	ACTVT	02		AND	0	
FLOG01	ME22	M_BEST_BSA	BSART	*		AND	1	
FLOG01	ME22	M_BEST_EKG	ACTVT	02		AND	0	
FLOG01	ME22	M_BEST_EKG	EKGRP	*		AND	1	
FLOG01	ME22	M_BEST_EKO	ACTVT	02		AND	0	
FLOG01	ME22	M_BEST_EKO	EKORG	$EKORG		AND	0	
FLOG01	ME22	M_BEST_WRK	ACTVT	02		AND	0	
FLOG01	ME22	M_BEST_WRK	WERKS	$WERKS		AND	0	
FLOG01	ME22N	M_BEST_BSA	ACTVT	02		AND	0	
FLOG01	ME22N	M_BEST_BSA	BSART	*		AND	1	
FLOG01	ME22N	M_BEST_EKG	ACTVT	02		AND	0	
FLOG01	ME22N	M_BEST_EKG	EKGRP	*		AND	1	
FLOG01	ME22N	M_BEST_EKO	ACTVT	02		AND	0	
FLOG01	ME22N	M_BEST_EKO	EKORG	$EKORG		AND	0	
FLOG01	ME22N	M_BEST_WRK	ACTVT	02		AND	0	
FLOG01	ME22N	M_BEST_WRK	WERKS	$WERKS		AND	0	
FLOG01	ME25	M_BEST_BSA	ACTVT	01		AND	0	
FLOG01	ME25	M_BEST_BSA	BSART	*		AND	1	
FLOG01	ME25	M_BEST_EKG	ACTVT	01		AND	0	
FLOG01	ME25	M_BEST_EKG	EKGRP	*		AND	1	
FLOG01	ME25	M_BEST_EKO	ACTVT	01		AND	0	
FLOG01	ME25	M_BEST_EKO	EKORG	$EKORG		AND	0	
FLOG01	ME25	M_BEST_WRK	ACTVT	01		AND	0	
FLOG01	ME25	M_BEST_WRK	WERKS	$WERKS		AND	0	

Source: own work

Next, the file with the set of rules is imported to the SAP GRC system. Then, rules are generated meaning that the business functions, risks and their respective authorisations are related. After the access rules are generated, the information recorded in the Rulebook becomes more transparent to the business user.

Brzeziński Ł. et al. (Eds.), Modern solutions in production and warehousing, Spatium, Radom 2019.
https://doi.org/10.17270/B.M.978-83-66017-87-0.8

The set of rules, as fed in, is the foundation for the analyses. After it is imported and re-generated, analyses for users, roles and authorisation profiles may be performed (Fig. 3).



Function: FMM04

* Function ID: FMM04
* Business Process: MM
* Analysis Scope: Single System
* Description: Purchase Order Maintenance (SAP ERP)

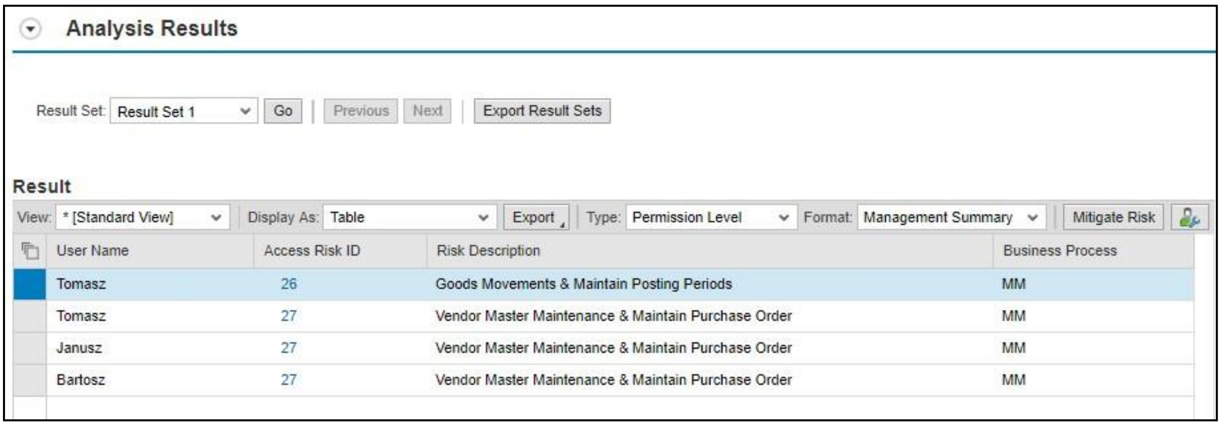
Action	Description	Status
ME21	Create Purchase Order	Active
ME21	Create Purchase Order	Active
ME21N	Create Purchase Order	Active
ME21N	Create Purchase Order	Active
ME22	Change Purchase Order	Active
ME22	Change Purchase Order	Active
ME22N	Change Purchase Order	Active
ME22N	Change Purchase Order	Active
MEMASSPO	Mass Change of Purchase Orders	Active
MEMASSPO	Mass Change of Purchase Orders	Active

Fig. 3. Definition of FMM04 function (Purchase Order Maintenance) in the SAP GRC AC system (laboratory environment). Source: own work

Following the imported set of rules based on the pre-prepared SoD matrix, analyses are carried out to identify users with excessive permissions in the SAP system.

The analysis may pertain to all staff having accounts in the SAP ERP system (global analysis) and selected users, conflicts or business areas. It can be done manually or automatically, i.e. regularly, daily at the same time. It facilitates considerably the monitoring of threats involved in the access to particular system functions, e.g. by designating persons responsible for inspections in the different departaments of the enterprise.

The results of detailed analyses help the persons in charge resolve SoD conflicts, e.g. make decisions on taking specific rules away from users (which provide access to one the parties to the SoD conflict). They indicate what transactions and authorisation objects produce the conflict resulted from and which role enables access thereto (Fig. 4).



Analysis Results

Result Set: Result Set 1

Result

View: * [Standard View]
Display As: Table
Type: Permission Level
Format: Management Summary

User Name	Access Risk ID	Risk Description	Business Process
Tomasz	26	Goods Movements & Maintain Posting Periods	MM
Tomasz	27	Vendor Master Maintenance & Maintain Purchase Order	MM
Janusz	27	Vendor Master Maintenance & Maintain Purchase Order	MM
Bartosz	27	Vendor Master Maintenance & Maintain Purchase Order	MM

Fig. 4. Analysis of user-level risk in the SAP GRC system (laboratory environment) – risks of access from the MM area resulting from too wide permissions for users of the SAP ERP system. Source: own work

https://doi.org/10.17270/B.M.978-83-66017-87-0.8

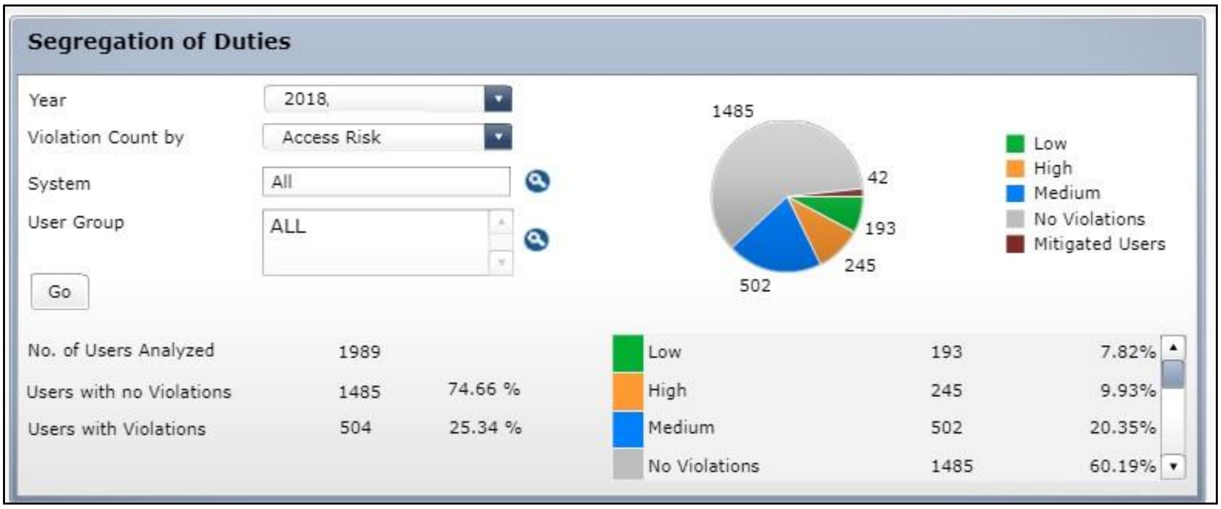
Sometimes duties cannot be segregated properly because of a small or remote staff. Such cases require management oversight to ensure that SoD violations are not occurring. Instead of segregation of duties through access control, a compensating control needs to be put in place so that a manager reviews the transactions entered by such employees [Vu Broady and Holly 2008]. If it does not discourage the user from committing an infringement, such an action may successfully reveal thefts which have already taken place and protect the organisation against more.

After the assignment of control, tolerance to risk for the user concerned is increased. Subsequent analyses done for the user will display the relevant information about mitigation control.

Mitigation controls are detective in their nature, i.e. are designed to identify errors or irregularities after they occur. An example of a detective control may be a verification of purchase documents which have been created for products not included in the purchase request before (so-called PO with no demand reference) or warehouse stocktaking [Cieplik 2019]. Automation of such controls is offered by another tool from the GRC segment – SAP GRC Process Control.

The SAP GRC Access Control application enables an analysis for system roles and authorisation profiles. This helps determine whether the roles that have been built take account of the SoD conflict, i.e. whether the allocation of one role to a user enables such user to perform two conflicting activities. Theoretically, each role in the system should be SoD conflict free. Otherwise each time it is allocated to the user, it generates a new SoD conflict in the enterprise.

A graphic equivalent of the analyses are in-built access panels. An example of such a panel is shown in the figure 5. Their graphic representation which supports the monitoring of the number of SoD conflicts. They present, *inter alia*, analyses for groups of users and roles in graphic form, a comparison of the number of conflicts in the organisation for selected periods (quarterly, monthly), the progress of remedial actions as well as the statistics relating to the use of conflicting transactions by system users.



Segregation of Duties

Year 2018

Violation Count by Access Risk

System All

User Group ALL

Go

No. of Users Analyzed	1989	
Users with no Violations	1485	74.66 %
Users with Violations	504	25.34 %

🟩	Low	193	7.82%
🟧	High	245	9.93%
🟦	Medium	502	20.35%
⬜	No Violations	1485	60.19%

Fig. 5. Analysis of all SoD conflicts in an example of an enterprise broken down by risk level including mitigated (compensated) risks in the SAP GRC AC system (laboratory environment). Source: own work

CONCLUSIVE REMARKS

In order to perform the various activities in the SAP system, users need permissions to enable them to execute their daily business tasks. In SAP systems, users' permissions are role-based. The assignment of a role to a user in SAP offers the possibility of performing specific activities in the system, i.e. using a transaction, generating a report or getting information from a data table. The management of permissions from the perspective of IT administrators may be very bothersome. The point is to assign roles to users so that the resulting permissions minimise the possibility of abuses involved in the use of too wide an access in the system. The challenge is considerable enough for a major part of enterprises using the SAP system to have hundreds and even thousands of users and roles assigned to each of them with various durations, and various access sets. As a result, manual analysis and matching permissions with the actual responsibilities of employees becomes impossible.

In the chapter, 17 examples of SoD conflicts are identified for the logistics of the SAP system which, after a user is given too wide access, may involve the risk of wilful or unintentional abuse having a negative effect on the enterprise. Examples of abuses include:

- generation of fictitious orders in the system,
- organisation of supplies to a wrong recipient's address,
- execution of payments to wrong bank accounts,
- payments for supplies / services which in fact did not exist,
- unfounded release of goods from the warehouse,
- sale of products at understated prices,

- uncontrolled manipulation of stock levels,
- errors in warehousing operations,
- actions contrary to the firm's policy or without the authorised persons being aware thereof,
- actions contrary to the organisation's business objectives.

In order to prevent situations of this type, enterprises use applications which supervise users' permissions. One of such applications is SAP GRC Access Control. This tool supports user- and role-level analyses, enabling automatic support for the process of resolving SoD conflicts, which reduces to the minimum the need to do manual analyses of large quantities of data whilst minimising the probability of committing errors. In addition to supporting SoD conflict resolution, the software improves the overall organisation of the enterprise, e.g. through automation of the process of granting permissions and limits the number of chapter documents in the enterprise.

REFERENCES

Cieplik K., 2018, Identyfikacja i rozwiązywanie konfliktów rozdziału obowiązków i uprawnień w systemie SAP ERP w obszarze logistyki, Master degree dissertation, Cracow University of Technology.

Cieplik K., Kontrole detekcyjne w SAP Process Control, https://grcadvisory.com/blog-ekspertow/kontrole-detekcyjne-w-sap-process-control (dostęp z dnia 10.01.2019).

Dudek Ł., Rozdział obowiązków (SoD) – teoria i praktyka, https://grcadvisory.com/blog-ekspertow/rozdzial-obowiazkow-sod-teoria-i-praktyka (dostęp z dnia 9.10.2018).

Lamotte-Schubert M., Weidenbach Ch., 2009, Analysis of Authorizations in SAP R/3, Proceedings of the 7th International Workshop on First-Order Theorem Proving, FTP 2009, Oslo, Norway, July 6-7, 2009, 92-104.

Vu Broady D., Holly A., 2008, SAP GRC for Dummies, Roland Wiley Publishing, Indianapolis, 87-141.

Chuprunov M., 2011, Auditing and GRC Automation in SAP; Galileo Press, Bonn, 68-72; 118-130,

Juran T., 2016, Beginner's Guide to SAP Security and Authorizations, Espresso Tutorials GmbH, Gleichen, 9-38.

Brzeziński Ł. et al. (Eds.), Modern solutions in production and warehousing, Spatium, Radom 2019.
https://doi.org/10.17270/B.M.978-83-66017-87-0.8

Lorenc A., Szkoda M., 2015, Customer Logistic Service in the Automotive Industry with the Use of the SAP ERP System. Proceedings of: 2015 4th IEEE International Conference on Advanced logistics and Transport (ICALT). 20-22 May 2015, 18-23.

www.casewareanalytics.com/blog/millions-lost-due-segregation-duties-failings

www.rp.pl/Przemysl-Obronny/302089917-Handlujacy-bronia-Cenzin-dal-sie-podejsc-oszustom.html (dostęp z dnia 28.09.2019).

Szkoda M., 2008, Realizacja procesów logistyki dystrybucji z zastosowaniem systemu SAP ERP, Logistyka nr 5/2013, 186-189.

Szkoda M., 2010, Zintegrowane systemy informatyczne w logistyce – SAP R/3. Kraków, ISBN 978-83-7242-564-5.

Szkoda M., 2014, Realizacja procesów logistyki zaopatrzenia z zastosowaniem systemu SAP ERP, Logistyka nr 6/2014, 10343-10351.

Brzeziński Ł. et al. (Eds.), Modern solutions in production and warehousing, Spatium, Radom 2019.
https://doi.org/10.17270/B.M.978-83-66017-87-0.8