

A Maturity Model for Segregation of Duties in Standard Business Software

Jan Omland, Nick Gehrke, Niels Müller-Wickop

▶ **To cite this version:**

Jan Omland, Nick Gehrke, Niels Müller-Wickop. A Maturity Model for Segregation of Duties in Standard Business Software. Governance and Sustainability in Information Systems: Managing the Transfer and Diffusion of IT (Working conference), Sep 2011, Hamburg, Germany. pp.288-294, 10.1007/978-3-642-24148-2_20 . hal-01571735

HAL Id: hal-01571735

https://inria.hal.science/hal-01571735

Submitted on 3 Aug 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

A maturity model for segregation of duties in standard business software

Jan Omland

Benrather Schlossallee 99, 40597 Düsseldorf, Germany
jan.omland@bfcs.de

Nick Gehrke

Köllner Chaussee 11, 25337 Elmshorn, Germany
nick.gehrke@nordakademie.de

Niels Müller-Wickop

Max-Brauer-Allee 60, 22765 Hamburg, Germany
niels.mueller-wickop@wiso.uni-hamburg.de

Abstract. Maturity models are widespread used in several domains ranging from business processes to complete management frameworks like CMMI, ITIL or Cobit. In the paper on hand we develop a detailed maturity model for the management of segregation of duties in ERP systems. Our model includes several aspects starting with simple access rights management of individual systems and leading to comprehensive organizational aspects of multiple systems environments. Applying this model, organizations are enabled to improve compliance regarding access rights using a step by step approach. The approach described can also be used to assess existing segregation of duties processes of an organization in order to reveal further improvement opportunities.

Keywords: Maturity Model, Segregation of Duties, SoD, Authorization Process, Authorization/Access Controls, Rule Set

1 Introduction

When it comes to business process implementation and integration of business data throughout all value chain activities, a lot of companies rely on standard business software (for definition cf. Staud 2006, p.33). This is only justified, if the software is sufficiently secured. (Hendrawirawan et al. 2007, p.46). It seems necessary to provide an authorization concept for system security, which incorporates thoroughly implemented segregation of duties (SoD). Many Companies have problems implementing segregation of duties accurately (Krell 2007, p.18). One significant

reason is the inherent complexity of ERP systems. Due to the comprehensive application range and the high grade of process integration it is not only necessary to have business process skills, but to have technical knowledge as well. The high complexity of SoD, the growing quality awareness and the claim for an efficient approach underline the need for SoD standards and maturity models (Chandra und Beard 2007, p.2). The application of maturity models facilitates the quality measurement of SoD.

2 Conceptual design of the maturity model

In general, maturity models range from three to six maturity degrees (Fraser et al. 2002, p.246). We decided to use five maturity levels. In a second step rating criteria were developed, these are used to determine maturity levels. The number of complexity level ranges from two to five. Altogether 31 questions have been developed to determine maturity level for SoD in standard business software. For the purpose of giving a structured overview to the developed maturity model, rating criteria are assigned to the following 4 categories*: rule set, control processing, SoD reporting and organizational framework* (COSO 2004, pp.3-4). For our maturity model we use the staged representation (In this context ”staged” means that every maturity level fulfills all criteria of maturity levels below (Fraser et al. 2002, p.246)) Following the four categories and their assigned rating criteria are specified in more detail.

Category *“rule set“:* A rule set is the foundation of every SoD analysis. All relevant SoDs are defined here (Little und Best 2003, p.421). First of all, the quality of SoD in standard business software depends on the applied rule set. Thereby certain rule set characteristics are relevant which are usable as rating criteria for the maturity model (Hendrawirawan et al. 2007, p.3). When analyzing SoD it is only possible to detect those conflicts that have been defined in advance. Apart from completeness, being up-to-date is another important criterion. Based on the risk identification the rule set has to be updated continuously to achieve a high quality SoD process (Chandra und Beard 2007, p.11). For the category “rule set“ altogether four questions are posed to determine the maturity level (cp. figure 1 in appendix). Existence resp. complexity level (cl) is used as unit of measurement (um) (cp. figure 2 in appendix).

Category *“control procedure“:* This category summarizes those criteria which deal with guidelines and procedures to mitigate relevant risks. Following the stages of the SoD process (Wolf und Gehrke 2009, p.3) it is possible by means of these criteria to control the before defined compliance of rule sets (COSO 2004, p.4). Basically three different criteria are pointed out which can be used for control procedure maturity level assessment: point of time, character of control and frequency (Debreceny 2006, p.4). Regarding the time of control procedure preventive and detective controls can be classified. Thus by means of a control risk occurrence can be avoided (ex ante) or retrospectively discovered (ex post).

Another criterion is the type of control execution. A differentiation is made between manual and automatically executed controls. Especially SoD controls

provide a strong link to automated approaches. It is crucial for the sustainable implementation of SoD that the control activities are carried out regularly (Taiariol 2009, p.23). Before mentioned questions of control activity assessments are presented in the appendix (see Figure 1).

Category *"SoD Reporting"*: This category includes SoD reporting criteria describing the preparation of the analysis results as well as criteria that address the clean-up of identified SoD conflicts. Hence the sustainable implementation of the defined rules is also subject to this category. For example, the comparison of the last SoD analysis results reveals the success or failure of the SOD activities over time (also taking the timely removal of identified conflicts into account) (Taiariol 2009, p.25). Thus indicators of possible process improvements can be identified. A structured approach to eliminate the weak points we pointed out is also useful to prioritize the individual SoD conflicts. This can ideally be done by a risk assessment of the different SoD conflicts (Krell 2007, p.19). Thereby it is important to question risks according to the risk management process to challenge the rule set and adjust it if necessary. In accordance with the determined risks, escalation mechanisms should be implemented for the purpose of eliminating assessed conflicts. A differentiation of escalation mechanisms, considering the calculated risks and temporal evolution, is worth taking into account.

Category *"Organizational Environment":* Criteria grouped under this category are primarily concerned with the assessment of process safety consciousness within the company. This category is essential for the quality of SoD processes executions. Although so-called Computer Assisted Audit Techniques (CAAT) are used to support the automation of SoD activities, the employment of employees in many areas is still essential (Hendrawirawan et al. 2007, p.3).

From an organizational perspective a criterion for assessing the maturity level is the definition of responsibilities (Herbsleb et al. 1997, p.38). Usually, the IT department is responsible for ERP security-related issues. The business departments employees - as business process owners - typically lack the technical knowledge for the maintenance, allocation and testing of permissions. Therefore, the separation of duties within standard business software should be an inter-divisional anchored task (Taiariol 2009, p.23). The integrative character is also reflected in properly implemented authorization assignment processes (Chandra and Beard 2007, p.14). Because of the far-reaching consequences approval by the line manager is not sufficient, a so-called “role owner” must be defined.

Further criteria include the involvement of senior management and the definition of target values. Assuming the management is informed regularly about the development of SoD conflicts a high priority of the issue within the company can be assumed (Herbsleb et al. 1997, p.38).

Maturity Level 0: The maturity level 0 is present if a company carries out its authorization management for business standard software, but does not consider SoD issues. The perception of SoD issues within the company does not exist. The purpose of the authorization management is only to allow employees access the ERP system.

Maturity Level 1 - Initial: Similar to known maturity models such as CMMI and BPMM SoD projects in standard business software have the degree of "initial" if they

are assigned to the lowest possible maturity. In this stage, processes are executed in an unplanned and unstructured way, thus the quality of SoD analysis is difficult to assess (OMG 2008, p.20). This is mainly due to the lack of formalization of the rule sets, which complicates the traceability of activities regarding completeness and correctness. Rules are defined on an ad hoc basis by the participating employees, creating a company-wide heterogeneous landscape. In addition, the definition of rules is not based on risk assessments within the meaning of the risk management process. Therefore a full consideration of all high-risk business processes is not given. This also implies a lack of dynamism of rules. Adjustments based on risk assessments are not made.

Maturity Level 2 - Repeatable: In comparison to the maturity level "Initial " a formalized rule set - defining SoD conflicts - is existent. This increases the transparency of SOD activities within the company and facilitates the formalization of a re-implementation of SoD analysis. From an organizational perspective on this level of maturity the department is more involved in the SoD process. On the one hand, this increases the quality of the rule set. On the other hand, departments as recipients of reports are enabled to identify and evaluate SoD conflicts as well as assisting with their removal. The successful elimination of SoD conflicts is reflected in passed follow up audits. The results are documented and reported.

Maturity Level 3 - Defined: At this maturity level rules for multiple risk prone business processes and supporting application systems are existent. Rule sets are updated as soon as relevant changes are made to the business processes. To increase the effectiveness of the control system the rule set includes both - detective and preventive - controls. In the case of inapplicable rules, decentralized local controls are executed in order to minimize potential risks. To support a company-wide process improvement, conflicts are tagged with “risk values” in the regular reporting. Based on the risk values managers can derive a prioritization of follow-up activities to ensure effective use of their resources. The communication of conflicts is integrated in the escalation management to ensure timely processing. Overall, the SoD approach at this level is structured. Responsibility for SoD processes lies with the departments. Departments develop rule sets in cooperation with IT staff and remove identified conflicts. The increased awareness of SoD is also reflected in the further development of the authorization management.

Maturity Level 4 - Managed: At this maturity level a generic rule set is used. Based on the risk assessment SoD are defined for all relevant business processes. These SoD are defined independently of the (IT-) system. Before deriving controls from the rule sets transactions are mapped to relevant application systems. In this way it is easier to maintain a company-wide uniform rule set. In case of process changes only one rule set needs to be adapted. Vice versa the rule set is still usable if IT systems are replaced. Only system-specific transformations need to be adapted. All control activities are automatically carried out on a regular basis. This enables responsible personal to make a statement about compliance regarding SoD aspects in the short term. The sustainable elimination of conflicts is supported by an automatic escalation management. Furnished with a priority conflicts are communicated to corresponding

departments depending on age and risk assessment. Reports also include figures about process improvements.

Maturity level 5 - Optimizing: The maturity level "Optimizing" describes the highest level of SoD projects in standard business software. At this level SoD processes are constantly being developed and improved. A process to update the rule set in the case of relevant processes changes is in place. Also included is the systems specific rule set transformation, linked control activities, the risk assessment and the reporting as well as the escalation management. At this maturity level the company-wide uniform rule set is characterized by its completeness. It includes not only all high risk classified processes and the linked application systems, but also SoD aspects across different systems. To ensure uniform implementation of all control activities compensating controls are defined and rolled out centrally. An autonomous approach by departments is precluded. Compared to maturity level 4 there are not only set targets for the elimination of SoD conflicts, but the management also designs an incentive system. Thereby incremental and innovative process and technology improvements are encouraged.

3 Conclusion

In this paper a maturity model for segregation of duties in standard business software is presented. Both the complexity of the issue and the lack of research in this area illustrate the need of such a model. In the categories rule set, control activities, reporting and organizational environment we developed 31 questions that can help assess the current state of SOD activities. Furthermore, based on the results improvement opportunities can possibly be identified and prioritized accordingly. In comparison to other maturity models the relatively simple structure should provide high user friendliness. In order to aggregate important information a future graphical presentation of results is possible (Carbonel, 2008, p.4).

REFERENCES

Carbonel J (2008) Case Study: Assessing IT Security Governance Through a Maturity Model and the Definition of a Governance Profile. INFORMATION SYSTEMS CONTROL JOURNAL 2(2008):29–32.

Chandra A, Beard M (2007) Towards a Framework for Achieving Effective Segregation of Duties. http://artsms.uwaterloo.ca/accounting/UWCISA-new/symposiums/symposium_2007/Chandra-SOD.pdf. Retrieved 2009-08-25.

COSO Committee of Sponsoring Organizations of the Treadway Commission (2004) Enterprise Risk Management - Integrated Framework - Executive Summmary 2004. www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf. Retrieved 2009-09-15.

Debreceny RS (2006) Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls. In: System Sciences, 2006. HICSS ‘06. Proceedings of the 39th Annual Hawaii International Conference on, (8):196c-196c.

Fraser P, Moultrie J, Gregory M (2002) The use of maturity models/grids as a tool in assessing product development capability. In: Managing technology for the new economy, St John's

College, Cambridge, UK, 18 - 20 August 2002; proceedings. Piscataway, NJ: IEEE Service Center:244–249.

Gehrke N, Wolf P (2009) Continuous Compliance Monitoring in ERP-Systems – A Method for Identifying Segregation of Duties Conflicts. In: Wirtschaftsinformatik 2009:347-356.

Hendrawirawan D, Tanriverdi H, Zetterlund C, Hakam H, Kim HH, Paik H, Yoon Y (2007) ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution. INFORMATION SYSTEMS CONTROL JOURNAL 2(2007):46–50.

OMG (2008), Business Process Maturity Model (BPMM), Object Management Group (OMG), http://www.omg.org/spec/BPMM/1.0/PDF/ Abgerufen am 08.02.2011

Herbsleb J, Zubrow D, Goldenson D, Hayes W, Paulk M (1997) Software Quality and the Capability Maturity Model. COMMUNICATIONS OF THE ACM 6(40):30–40.

International Federation of Accountants (IFAC) (2008) Handbook of international quality control, auditing, review, other assurance and related services pronouncements. 2010 Edition. New York. ISBN: 978-1-60815-052-6

Krell E (2007) ERP System Controls. Business Finance 4(13):18–22.

Little A, Best PJ. (2003) A framework for separation of duties in an SAP R/3 environment. MANAGERIAL AUDITING JOURNAL 5(18):419–430.

OMG Object Management Group (2008) Business Process Maturity Model (BPMM). http://www.omg.org/spec/BPMM/1.0/PDF/. Retrieved 2009-09-09.

Staud JL (2006) Geschäftsprozessanalyse. Ereignisgesteuerte Prozessketten und objektorientierte Geschäftsprozessmodellierung für Betriebswirtschaftliche Standardsoftware. Dritte Auflage. Berlin, Heidelberg, Springer-Verlag (Springer-11775 /Dig. Serial]).

Taiariol R (2009) Segregated Duties in Fashion. INTERNAL AUDITOR 1(66):23–25.

AUTHOR BIOGRAPHIES:

Nick Gehrke is full professor at the Nordakademie (Private University of Applied Sciences) in Elmshorn. After his Ph.D. he worked for PricewaterhouseCoopers for 5 years. During this time he did his CISA exam. His interests lie in the area of assurance and business process outsourcing.

Niels Mueller-Wickop is Ph.D. Student at the University of Hamburg. After his master studies he worked for PricewaterhouseCoopers for two years. His interests lie in the area of assurance and business process management.

Jan Omland is currently working for BFCS (Business & Finance Consulting Services GmbH). Before he joined BFCS he worked for PricewaterhouseCoopers. His interest lie in the area of assurance and financial consulting.

Appendix A: Definition of maturity level with associated questioner

Category	Criterion \ Maturity Level	1	2	3	4	5	Question	
Rule Set	1	0	1	1	1	1	Is there a formalized rule set that defines the individual SoD conflicts, for example a SoD-Matrix?	Yes/No
	2	1	1	2	3	4	Does the rule set include all processes classified as "risky" and the relevant associated application systems?	DoC
	3	0	0	0	1	1	Is it a company-wide or group-wide uniform rule set?	Yes/No
	4	1	1	2	2	3	Is a review of the rule set carried out, if changes of underlying processes take place?	DoC
Controls	5	1	1	1	1	1	Are there enough detectives SoD controls implemented?	Yes/No
	6	0	1	1	1	1	Is the regular execution of detective SoD controls adequate?	Yes/No
	7	0	0	1	1	1	Is the execution of detective SoD controls as far as possible automated?	Yes/No
	8	0	0	0	1	1	Are there enough detective controls to review transaction- and master data in order to detect fraud as well as error or abuse of individual authorizations?	Yes/No
	9	0	0	1	1	1	Are there enough preventive SoD controls implemented?	Yes/No
	10	0	0	0	1	1	Is the regular execution of preventive SoD controls adequate?	Yes/No
	11	0	0	0	1	1	Is the execution of preventive SoD controls as far as possible automated?	Yes/No
	12	0	0	1	1	1	Are there enough compensating SoD controls implemented?	Yes/No
	13	0	0	1	2	3	How are compensating controls defined and executed?	DoC
	14	0	0	0	1	1	Is the regular execution of compensating SoD controls adequate?	Yes/No
	15	0	0	0	0	1	Is the execution of compensating SoD controls as far as possible automated?	Yes/No
	16	1	1	2	2	3	Is there a process in place that ensures the adaption of control activities as a result of a rule set changes?	DoC
SoD-Reporting	17	0	1	1	1	1	Is a SoD-Reporting existent?	Yes/No
	18	0	0	1	1	1	Is the regular reporting adequate?	Yes/No
	19	0	0	0	1	1	Does the reporting take the chronological sequence of the identified SoD conflicts removal into account?	Yes/No
	20	0	0	1	1	1	Are there risk values calcualted for each SoD conflict?	Yes/No
	21	0	0	0	1	1	Is the risk value calculation review regularly?	Yes/No
	22	1	1	2	2	3	Are there escalation mechanisms existent that are used to eliminate SoD conflicts?	DoC
	23	0	0	0	1	1	Are escalation mechanisms initiated automatically depending on the reporting results?	Yes/No
	24	1	1	1	2	3	Are there target reviews (e.g. KPIs) included in the reporting?	DoC
	25	0	0	0	1	1	Are there metrics for process improvement included in the reporting (e.g. optimizing the role concept and user administration)?	Yes/No
Organization	26	1	2	3	3	3	Is only the IT-department involved in SoD issues? Are other departments only informed about SoD-analysis results?	DoC
	27	0	1	1	1	1	Is every department responsible for granting authoritzation (is this document in specific work instructions)?	Yes/No
	28	0	0	1	1	1	Is there are seperate process for special user rights like "Super-User/SOS-User"?	Yes/No
	29	1	2	3	4	5	Is a monitoring process for special users like "Super-User/SOS-User" in place (e.g. review of system logs)?	DoC
	30	0	0	0	0	1	Are there incentives for reaching set SoD aims?	Yes/No
	31	0	0	0	1	1	Is the management regularly informed about the development of SoD conflicts?	Yes/No

Appendix B: Degree of complexity for different questions

Degree of Complexity - Question 2

DoC	Characteristic
1	The rule sets are existent per "risk process" and an application system. It is defined system-specific.
2	The rule set is existent for a number of "risk processes" and an application systems. It is system independent (generic) defined.
3	A generic rule set exists for all "risk processes" and was transformed for some application systems.
4	A generic rule set exists for all "risk processes" and was transformed for all application systems. It also includes cross-system SoD.

Degree of Complexity - Question 4

DoC	Characteristic
1	No. The rule set is static.
2	In some cases, the rule set is reviewed. However, there is no systematic review.
3	A process is in place for updating the rule set as soon as relevant process changes occur.

Degree of Complexity - Question 13

DoC	Characteristic
1	Compensating controls are decentrally defined and executed.
2	An approval is centrally given for decentral defined controls.
3	Compensating controls are centrally defined and executed.

Degree of Complexity - Question 16

DoC	Characteristic
1	No.Controls are not reviewed.
2	In some cases a control review is carried out. However, there is no systematic review.
3	There is a process that ensures that controls are checked at each rule set chhnge

Degree of Complexity - Question 22

DoC	Characteristic
1	No. There are no procedures for the elimination of identified SoD conflicts.
2	Yes. Once SoD conflicts were identified, the department manager is prompted to resolve these conflicts.
3	Yes. Depending on the calculated risk value different levels of hierarchy are notified.

Degree of Complexity - Question 24

DoC	Characteristic
1	No. There are no target Values.
2	Yes. There are rudimentary targets, for example the elimination of all conflicts by the end of the year.
3	Yes. There are dedicated targets. These values are determined on risk basis

Degree of Complexity - Question 26

DoC	Characteristic
1	No involvement of the departments.
2	The department is informed of SoD analysis results.
3	The departments are responsible for the SoD process.

Degree of Complexity - Question 29

DoC	Characteristic
1	There is no review Process
2	Activation/Configuration of system log files
3	Random review of system logs
4	Regular manual review of logs
5	Automatic control of system logs