KPMG LLP
Suite 750
Las Olas Centre
450 East Las Olas Boulevard
Fort Lauderdale, FL 33301-3105

January 26, 2011

Mr. Jose Montes De Oca
Chief Internal Auditor
Miami-Dade County Public Schools
1450 N.E. 2nd Avenue
Miami, FL 33132

Dear Mr. De Oca:

As outlined in the addendum dated April 27, 2010 to the Services Agreement letter between Miami-Dade County Public Schools (M-DCPS) and KPMG LLP (KPMG), dated July 15, 2008 and executed on August 15, 2008, KPMG has completed the *SAP Security and User Access Assessment*. This letter transmits our final report that includes observations and recommendations through August 19, 2010.

The data included in these reports were obtained through interviews, meetings, and inspection of documentation, performed from June 09, 2010 (our first day of fieldwork) through August 19, 2010 for the *SAP Security and User Access Assessment* report. In addition, it includes management comments through January 20, 2011. We have no obligation to update this report or to revise the information contained therein to reflect events and transactions occurring subsequent to these dates. M-DCPS may request KPMG to send this report electronically for the client's convenience. However, only the final hard-copy report should be viewed as our work product.

This report is solely for your information and is not to be referred to in communications with or distributed for any other purpose to anyone who is not a member of management or board of directors of Miami-Dade County Public Schools, except as required to comply with Florida laws.

Please contact Mike Costello at 678-350-3627 or Jay Patel at 954-798-3654 if you have any questions or comments. We look forward to continuing to provide services to Miami-Dade County Public Schools.

Sincerely,

KPMG LLP

KPMG LLP, is Delaware limited liability partnership, the U.S. member firm of KPMG International Cooperative ("KPMG International"), a Swiss entity.

ADVISORY

Miami Dade County Public Schools

SAP Security and User Access Assessment

January 20, 2011

KPMG LLP

AUDIT • TAX • ADVISORY

Table of Contents

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

SAP Security and User Access Assessment – Overview

Overview

SAP Security and User Access Assessment – Overview

Prior to the deployment of SAP, each business process was typically automated in separate systems, 'owned' by a department or division of the business such as procurement. It was relatively easy for each business owner to know who had access to their system and who did what. It was important to control which systems a person had access to but not so important to control what they could do in each system. With SAP, all business processes are combined into one system, so with access to that system a person could affect any part of the company's activities.

As a result of the SAP rollout, it has become exceedingly important to have a defined process for the creation, maintenance, dissemination, and review of SAP security roles to help ensure roles are designed in such away to limit segregation of duties and validate that user's access rights are in-line with their job responsibilities. Recognizing the importance of adequate security controls, Miami – Dade County Public Schools ('M-DCPS') has requested that KPMG assess it's SAP authorization concept and provide observations and recommendations related to their current SAP security environment and processes.

More specifically, M-DCPS has requested KPMG perform the following to assess their SAP Security and User Access:

- Gain an understanding of the overall Authorization Concept (including policies and procedures).
- Review the M-DCPS Business Controls Catalog for inappropriate security roles and user access segregation of duties conflicts based on KPMG's standard segregation of duty and sensitive transaction rules.
- Develop observations and recommendations on M-DCPS' security strategy , SAP security roles and segregation of duties.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Overview (Continued…)

SAP Security and User Access Assessment – Overview (Continued…)

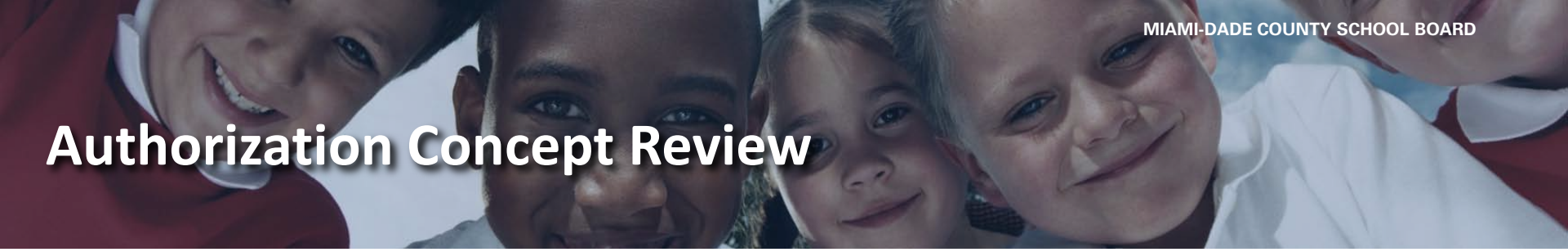
KPMG's review has been divided into two main sections: **Authorization Concept Review** & **Segregation of Duties Analysis**; observations and recommendations have been provided for each respective section.

- **Authorization Concept Review:** Review of security processes, policies, and procedures related to role creation and maintenance, access provisioning / de-provisioning, and monitoring of sensitive access.
- **Segregation of Duty Analysis:** Analysis of segregation of duties conflicts currently present within M-DCPS' SAP environment based upon KPMG's standard segregation of duty rules.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Authorization Concept Review



Authorization Concept Review

Overview

An organizations authorization concept establishes the rationale for how roles are designed, maintained, and outlines specific rules for how the roles will be granted to users. An adequately designed authorization concept and maintenance of the concept is exceedingly important as it provides the framework for establishing a segregation of duty free environment.

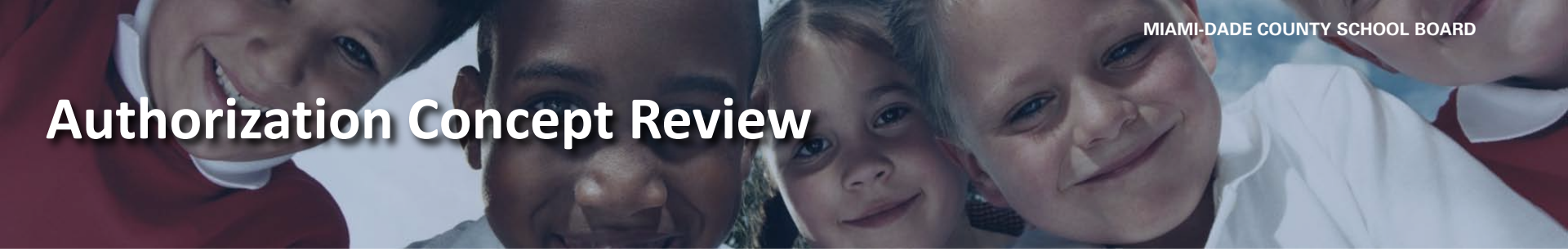
The KPMG team, working with relevant M-DCPS personnel conducted targeted meetings and reviewed specific process documentation to gain a detailed understanding of the SAP authorization concept, currently in place at M-DCPS. The review was conducted to analyze the authorization concept within the following areas:

- Development of roles & on-going role maintenance;
- Access provisioning, modification, and de-provisioning;
- Monitoring of access to sensitive transactions.

The results of this initial review were then mapped against a set of industry leading authorization concept practices to identify any deviations. Any deviations, noted within the report as 'observations', were reviewed and validated with relevant M-DCPS staff. M-DCPS staff comments were utilized by KPMG to generate targeted recommendations specific to M-DCPS' authorization concept. As of September 1, 2010, all KPMG observations were discussed with M-DCPS management. Through these discussions, KPMG has determined that M-DCPS management has accepted the observations and was in the process of implementing the resulting recommendation or had an appropriate response to any deviations from the resulting recommendation. These actions are documented next to each recommendation throughout the document.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



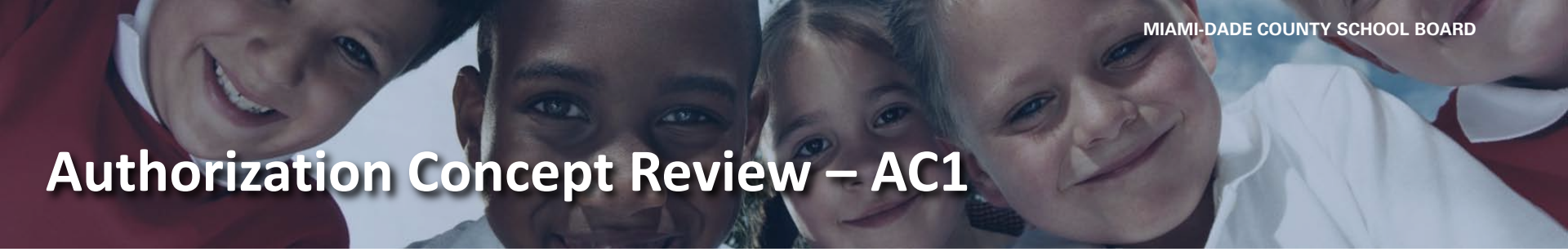
Authorization Concept Review

Observations

Overall, the authorization concept and supporting processes in place at M-DCPS incorporate many of the industry leading practices. Also, many of the general IT controls (access provisioning, de-provisioning, etc.) are well thought out and appear to be designed effectively.

The following tables provide a process overview, observations, and recommendations for each area reviewed:

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.



Authorization Concept Review – AC1

Area & High-Level Overview	Observation	Recommendation
AC1 - Role Development & Maintenance • Task based roles have been created for each process and assigned to a position within SAP-OM. • Roles are granted to users based upon position assignment within SAP-OM. • Security is de-centralized, where supervisors are able to assign specific access to users based upon job responsibility utilizing the AAAA application. • Roles have been created utilizing a three-tiered concept display, reporting, task based. Where the task based roles have parent child relationships to incorporate org level restrictions. • Creation of roles is requested, and approved, once approved they are developed and tested prior to being promoted to production. Promotion or transport of the role is conducted by someone other than the security group. • As roles are developed they are reviewed for inherent SoD conflicts.	Overall, KPMG noted that the role design approach utilized by M-DCPS appears to be in-line with leading practices, specifically as it relates to the use of a bottom-up approach to developing security and incorporating a three-tiered role concept (display, reporting, task based roles). KPMG did note the following observations: 1. The authorization concept and supporting security processes have been documented and outline: role architecture; naming conventions; maintenance process; provisioning / de-provisioning procedures; security analysis reporting, etc. However, the document was last updated March 6, 2008, and does not in all cases document current M-DCPS roles design and supporting processes.	1. KPMG recommends that M-DCPS review their authorization concept documentation and update relevant sections to reflect current architecture and processes. Additionally, the documentation should be reviewed at least yearly and updated on an as-needed basis to keep the document current.

Management Response
We concur with the recommendation. The current ERP security strategy (commonly known as MD-23) was meant to guide M-DCPS in the development / implementation phases of ERP. With the final phase of project of nearing its completion, it is the intent of M-DCPS to address ERP security documentation within the scope of its existing Policies and Procedure for Information Security. We intend to conduct an annual review of the Policies and Procedures on an ongoing basis, but will start the first review before Payroll Go-Live and finish after the Go-Live so that any lessons learned can be included. **Estimated start: July 1, 2011; Completion: January 1, 2012.**

KPMG

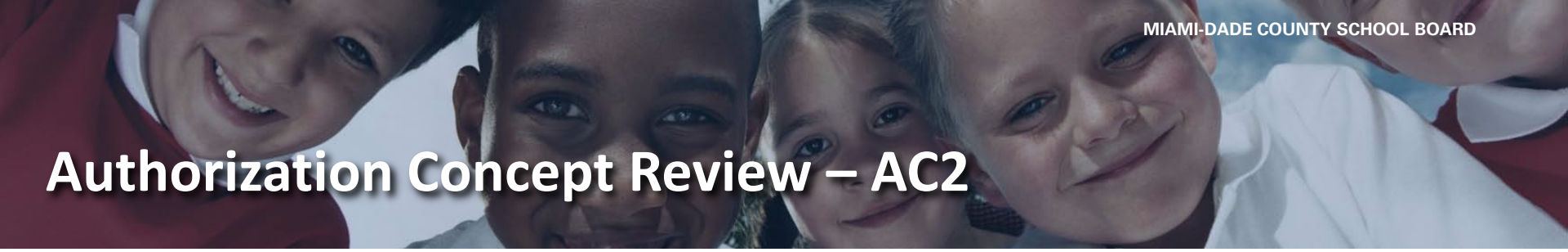
©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Authorization Concept Review – AC2

Area & High-Level Overview	Observation	Recommendation
AC2 - Access provisioning, modification & de-provisioning: • To access SAP a user must be granted both Active Directory ('AD") and SAP accounts due to the use of single sign-on. Additionally, most users are required to access SAP via the portal. Only certain IT users are allowed access through the GUI (Graphical User Interface). • Access to SAP is granted through a HEAT ticket request from the individuals supervisor. Once received an Active Directory ('AD') account and SAP-OM account is created for the user. The AD account initiates the creation of an SAP user ID which is then assigned to the SAP-OM account, which grants the position based roles. • Should a user transfer positions all roles associated with their current position remain with the position and new roles are granted only when a new position is assigned to the user. • Upon termination a user's AD account is automatically disabled / deleted once the action is entered within the PERS (HR) application due to batch job connection between PERS an AD. The removal of the AD account prevents a user from accessing SAP.	Based upon the process discussions, KPMG notes that overall M-DCPS' access provisioning, modification and de-provisioning processes appear to have been designed according to leading practices. KPMG noted the following observations through review: 1. Segregation of duties ('SoD') reviews are currently not conducted prior to granting access to users. This may lead to the granting of unnecessary SoD conflicts. However, through discussions with M-DCPS staff, KPMG noted that the district plans to implement SAP's Risk Analysis & Remediation tool (formerly Compliance Calibrator) to handle SoD reporting in the future. Due to other projects, this implementation has been put on hold until these other projects have been completed. 2. Security administration is de-centralized and access is granted by department heads. This could potentially lead to granting inappropriate access and / or SoD conflicts at the user level. 3. The current and planned user termination process require the HR department to both change a users employment status and remove them from an active position within SAP. Due to the human intervention component of the process, there is a risk of terminated user SAP accounts not being deleted, disabled, and / or revoked timely.	Based upon the noted recommendations, KPMG recommends the following: 1. Once the Risk Analysis & Remediation (formerly Compliance Calibrator) application is implemented the district should consider utilizing the tool to perform what-if analyses prior to granting access to identify SoD conflicts prior to granting access to users or positions (Refer to the Access & Security monitoring area to see additional recommendations related to the use of Risk Analysis & Remediation). 2. Roles granted to department heads and principals should be reviewed for SoD conflicts to validate these users are not granting SoD conflicts to their staff. 3. While the overall termination process is designed according to leading practices there is a risk of SAP user access not being timely revoked for terminated users. Therefore, as an added layer of control the district may want to consider reviewing terminated user access at least on a monthly basis to validate all terminated users SAP access has been adequately revoked.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Authorization Concept Review – AC2

MDCPS Management Response

Response to Recommendation 1
The Security team plans to complete the installation of Compliance Calibrator and Firefighter shortly after the payroll Go-Live is complete.
Estimated Start: November 1, 2011 Completion: December 7, 2011.
Note the following:

Currently, Compliance Calibrator is being used in the backend ECC to check roles for SOD conflicts. While the Security team can run Compliance Calibrator in this manner, it would prefer to have the application completely installed in both the backend and in the portal.

User level SOD checks will be impossible implement prior to granting user access because the district has implemented a decentralized method of granting access .To mitigate this factor, the security team is planning to provide chief s with reports detailing SOD conflicts.

Response to Recommendation 2
The School District has decided to implement decentralize user administration through the AAAA (Quad-A) application. Therefore, department heads will be able grant SoD conflicts to their staff. To mitigate this risk the security plans to create SOD conflict reports that the will notify the department head of pending SOD conflicts. Note that this is consistent with the current MDCPS process of providing RACF reports once the user has been provisioned.
Pre GO-live we will create a listing for BPOs of all role assignment for their respective areas. In addition we will look into creating a report for department heads list all role assignments for their departments. Post GO-live we will be issuing SOD conflict reports to the all department heads.
Report of all User Role Assignments by functional area - Start: February 1, 2011 Completion: March 31, 2011.

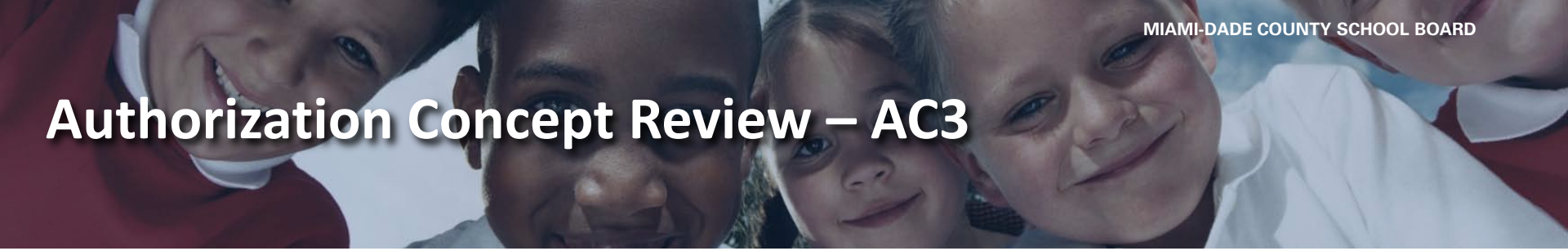
Report of Critical Roles – Start: April 1, 2011 Completion: May 31, 2011

Report of all roles by department (RACF type report) – Start: July 1, 2011 Completion: August 31, 2011

Response to Recommendation 3
An added layer of controls will not be needed if the user is terminated in a timely fashion and in the past, this has been the District's normal procedure. Accordingly, a user's access will automatically be revoked once they are terminated. Additionally, based on the position level security implemented by MDCPS, terminated users will be placed in another position that does not contain roles, which effectively terminates their access.
We would also point out that District administrative staff always have the option of terminating access themselves through the Quad A application, or can request the Security Department do it at any time.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

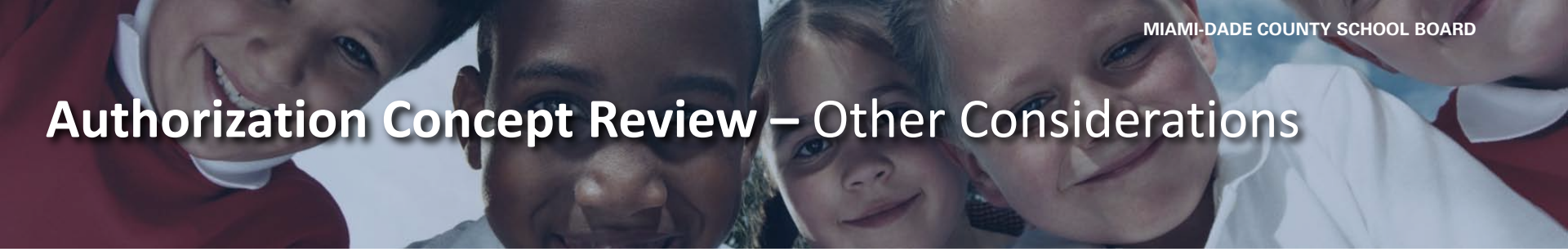


Authorization Concept Review – AC3

Area & High-Level Overview	Observation	Recommendation
AC3 - Access & Security Monitoring • M-DCPS is currently planning to implement SAP's Compliance Calibrator and FireFighter applications to review SoD's, sensitive access and log use of sensitive transaction usage. • Department heads and Principals are provided process specific super user access.	1. Reviews of sensitive access and SoDs are not being conducted on an on-going basis to identify inappropriate access and SoD violations. However, based upon discussion with M-DCPS, KPMG noted that M-DCPS plans to implement Compliance Calibrator to report SoDs and take necessary action. This implementation while planned was said to be on hold until other SAP modules were implemented.	1. KPMG agrees with M-DCPS' decision to implement tools, which will be utilized to report SoDs and log sensitive transaction usage. These tools will allow the district greater ability to understand their security risks and provide a means for addressing each risk, either through role / access modification strategies or mitigating controls. Additional considerations related to the use of these tools have been provided in the 'Other Considerations' section on the next page.

Management Response
We concur with this observation and we are in process of implementing the GRC tools. We will request funding for training, as this will also be needed. Since SAP security staff is down to two, full GRC implementation is planned after PY go-live. **Estimated start: January 1, 2012 Completion: February 15, 2012.**

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Authorization Concept Review – Other Considerations

Other Consideration	Recommendation
GRC Access Controls – Risk Analysis & Remediation (formerly Compliance Calibrator):	1. The SoD and access to sensitive transaction reporting is only as good as the rule book. It is important to modify the standard rulebook to be specific to the district's process. This would include a rationalization of process tasks, authorizations, and risk ratings for each SoD rule. If detailed attention is not paid to updating the rule book the probability of inaccurate reporting of SoDs and false-positives increases substantially. 2. Once the application is implemented and the rule set is updated, detailed procedural documents should be established outlining the frequency with which the analysis are conducted, reviewed and followed-up upon.

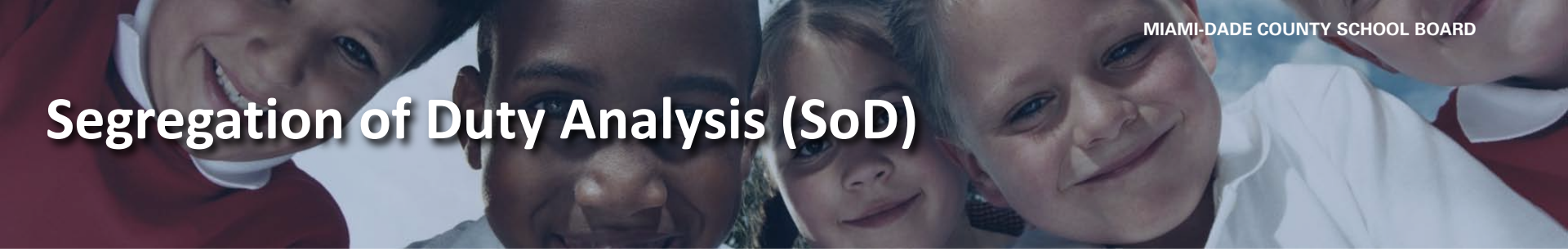
Management Response
1. We concur with this observation. Once GRC is implemented we believe that SOD rule book should be tailored to MDCPS business practices. Estimated start: March 1, 2012 Completion: June 30, 2012. 2. We concur with this observation. Once GRC is implemented, procedural documents should be established. Estimated Start: July 1, 2012 Completion: August 31, 2012.

Other Consideration	Recommendation
GRC Access Controls – Super User Privileged Management (formerly FireFighter):	KPMG understands that the district plans to utilize the Super User Privileged Management application to log use of key transactional usage to validate it's appropriate use. KPMG notes the following recommendation: 1. In order for the logging to be most effective the logs should be extracted on an on-going basis and reviewed for appropriateness. The review of these logs should be completed in a timely manner after the extract occurs and evidence of the review should be retained as this control is only as good as the review that is performed.

Management Response
We concur with this observation. Once GRC is implemented, a schedule will be developed for timely review of firefighter logs. Post Go-live, once firefighter has been implemented, a report will be issued to firefighter owners detailing firefighter usage. Estimated start: September 1, 2012 Completion: October 31, 2012.

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Segregation of Duty Analysis (SoD)



Segregation of Duty Analysis (SoD)

SoD Analysis Process Overview

The KPMG team, utilizing KPMG's proprietary baseline SoD rules matrix, performed an SoD analysis of SAP user access to determine M-DCPS overall risk exposure due to the number of SoD conflicts that exist in the production environment. The SoD analysis was conducted in the following manner:

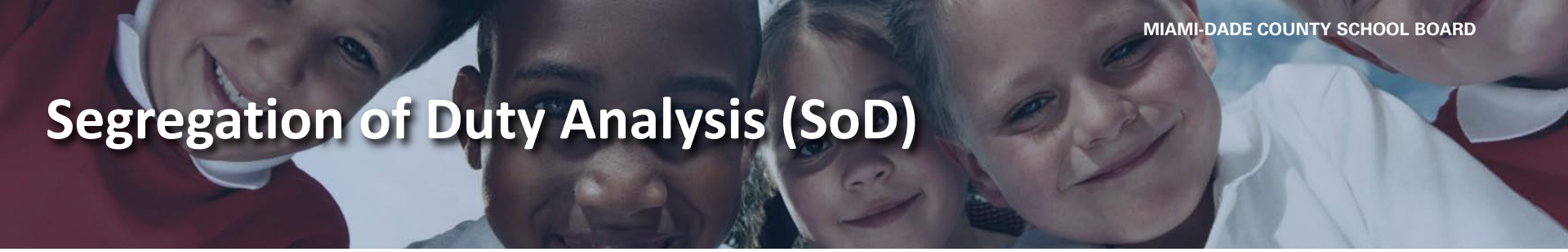
- Obtained relevant SAP security tables
- Security tables were mapped against the SoD rule set to identify SoD conflicts
- Resulting conflicts were analyzed and validated
- Results were reviewed with relevant M-DCPS staff and recommendations provided

The SoD results were reported at the risk level as opposed to the transaction conflict level. In so doing, KPMG is able to produce a robust SoD report that easily reviewed and understood by stakeholders at all levels. However, it should be noted that this report only reports an SoD for user one time, where in actuality the one SoD conflict may have been granted in multiple ways through a number of transactions. Within a GRC environment, the total SoD conflicts reported for each user may be much larger if there are multiple transactions on each side of the rule causing a conflict to exist.

NOTE: Due to time and budget *constraints, the SoD rules matrix utilized to conduct the analysis was not modified to be specific to M-DCPS' processes. Thus, KPMG recognizes the possibility that false positives may be identified which do not necessarily pose a specific financial or operational risk to the organization. However, these risks do exist within the environment and should be evaluated further to validate the appropriateness of this access.*

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Segregation of Duty Analysis (SoD)

SoD Example

Segregation of duties (SoD) is defined as the separation of duties and responsibilities of a business process to prevent individuals from being in a position to both perpetrate and conceal an error or irregularity. To create a SoD conflict from an SAP perspective, a user must have access to two transactions that are in conflict of each other.

An SoD rule is made of two conflicting tasks (Task 1 vs Task 2), each task having their own set of transactions (T-codes) which allow a user to execute the task. When a single transaction from both tasks are granted to a single user or within a single role the result is an SoD conflict. See below for an example:

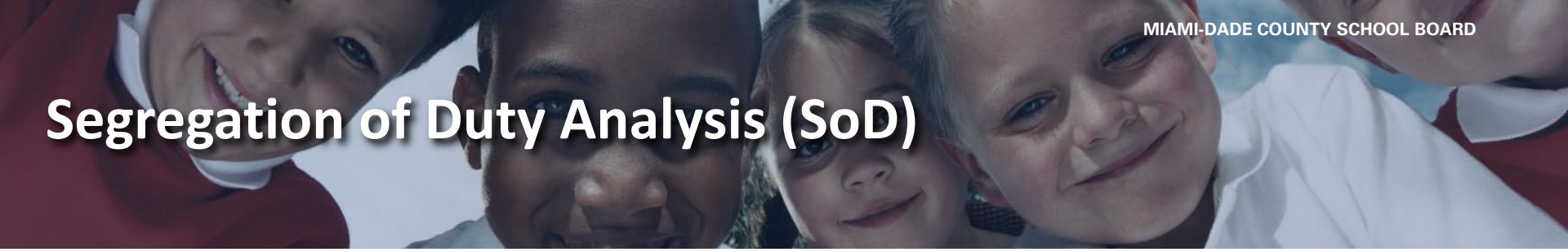
Conflicting Tasks: Maintain Purchase Order (Task 1) vs AP Payments (Task 2)

	Task 1: Maintain PO	Task 2: AP Payments	Conflict Description
Transactions	ME21, ME21N, ME22, ME22N, ME25, ME59, ME59N, MEMASSPO	F.13, F-04, F-07, F110, F-18, F-31, F-44, F-48, F-51, F-53, FB05, FB1K, FBA7, FBAB, FBZ0, FBZ2, FBZ4	Enter a ficticious purchase order and enter the covering payment.

Within GRC, an SoD conflict is created by having access to a single transaction within Task 1 versus a single transaction within Task2. Based on the example above, there are 136 possible transaction combinations which would result in an SoD within the example above.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.



Segregation of Duty Analysis (SoD)

SoD Rule Book Overview

An SoD Rule Book, is a set of segregation of duties risks that have been identified by an organization. This rule book is compared to the organizations security environment to determine whether the rules have been violated and segregation of duties conflicts granted.

An SoD rule book is comprised of 3 major components: Risks, Tasks, and Authorizations.

- **Risk:** Combination of two tasks when granted to a single user cause an SoD conflict (ex. Maintain PO vs AP Payments).
- **Task:** A single step in a process (ex. The ability to create a PO would be a task within the Procure to Pay process).
- **Authorizations:** The specific transactions and associated authorization objects a user must have to perform the process task.

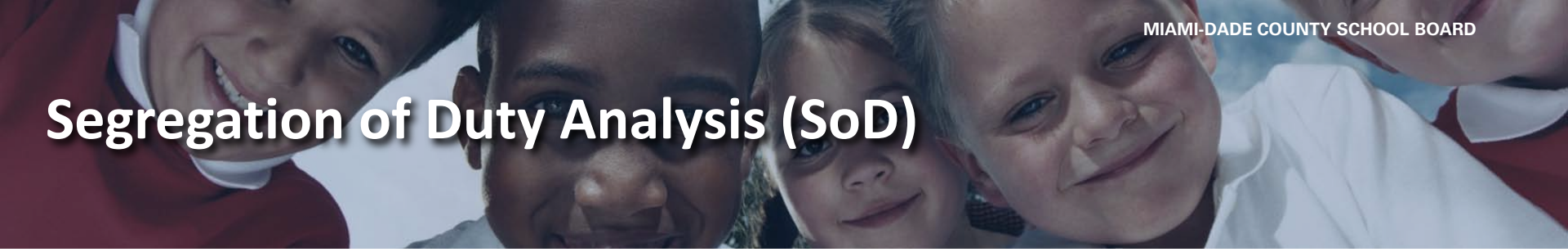
To create a rule, authorizations are assigned to tasks, and tasks assigned to rules. All rules then makeup the overall rulebook.

SoD Rule Book Rationalization

The rule book utilized by KPMG to assess the SoD security risks present within MDCPS' SAP application is a baseline rule book that has not been customized to any single industry or organization. Instead, it has been developed along **standard** SAP processes and transactions that embody industry agnostic leading practices. Therefore, the results of the report should be reviewed to determine overall risk and impact to MDCP's as some false-positives may exist given industry variations in business practices. Additionally, the utilized rule book did not take into account any custom transactions that may exists within MDCPS' environment and this may result in non-reporting of SoD conflicts caused by these custom transactions.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Segregation of Duty Analysis (SoD)

SoD Rule Book Rationalization (Cont'd)

As a result of the Rule Book rationalization process performed by KPMG, as discussed on the previous slide, certain SoD rules were deemed not relevant as they were associated with processes that are not currently utilized or have not been implemented. The relevant (utilized / implemented) processes for this review included:

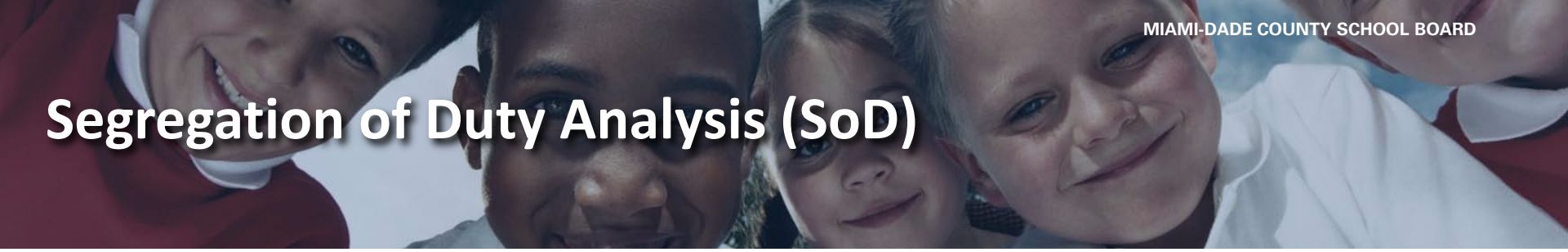
- Procure to Pay
- Materials Management
- Finance
- Basis (IT)

Based on discussions with MDCPS staff it was determined that the following processes are either not utilized or have not been implemented, however, SoD violations were noted within each of these processes. Therefore, the SoD violations for each of the listed processes was included within Appendix-A to provide the District a representative number of violations that may be reported should a standard rule book be utilized to assess SoD violations within their productive system:

- Finance – (certain sub-processes)
- HR & Payroll
- Materials Management – (certain sub-processes)
- Procure to Pay – (certain sub-processes)
- Order to Cash

.

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Segregation of Duty Analysis (SoD)

SoD Results Validation & Reporting Process

Once MDCPS' SAP Security environment was assessed against the modified SoD Rule Book, KPMG reviewed the SoD report and validated the results. The results were validated in the following manner:

- Sampled identified SoD user conflicts across all in scope process at various risk levels.
- Each sampled conflict was then validated by reviewing security tables and the Security User Information System within SAP to determine whether the user was in fact assigned the authorizations for each task within the rule showing as a conflict.

By performing the procedures above, KPMG is able to gain comfort that the results in total are accurate. KPMG performed these procedures for the MDCPS SoD conflict results and noted the SoD results appeared accurate.

Once validated, the SoD report was formatted to show conflicts at the risk level, indicating the number of user violations for each risk. This was done for management reporting purposes. However, it should be noted that the SoD Rule Book utilized, like SAP's Risk Analysis & Remediation tool (formerly Compliance Calibrator), reports conflicts at the transaction conflict level as depicted within the SoD example on slide 9. Therefore, reported SoD's within the technical report could be exponentially higher depending upon the various ways a conflict has been granted to each user.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Segregation of Duty Analysis (SoD)

SoD Conflict Results – Statistics

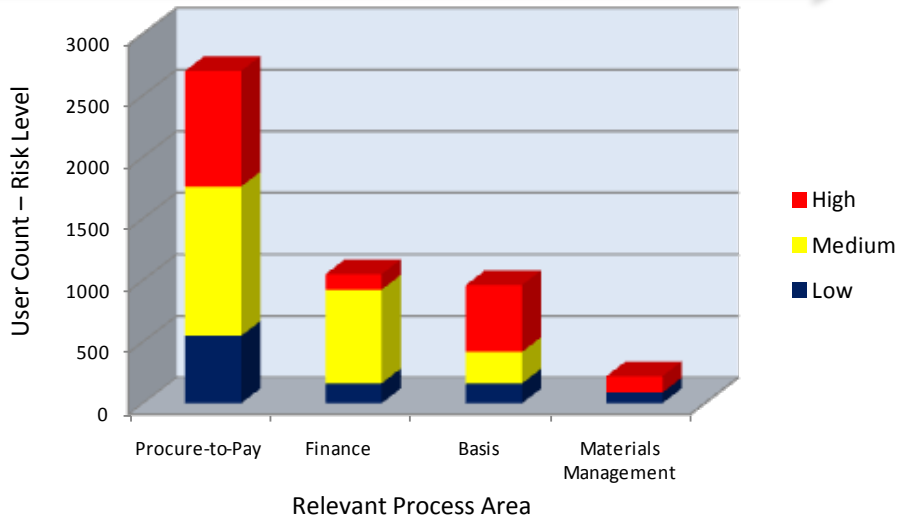
The figures below show an executive view of SoD violations at the risk level for each relevant process, including user counts:

Figure 1 - SoD Conflicts (*Quantitative View*)

Process	Risk Level			Total - By Process
	Low	Medium	High	
Procure-to-Pay	548	1212	939	2699
Finance	162	760	126	1048
Basis	161	256	543	960
Materials Management	87	0	133	220
Total - By Risk	958	2228	1741	**4927**

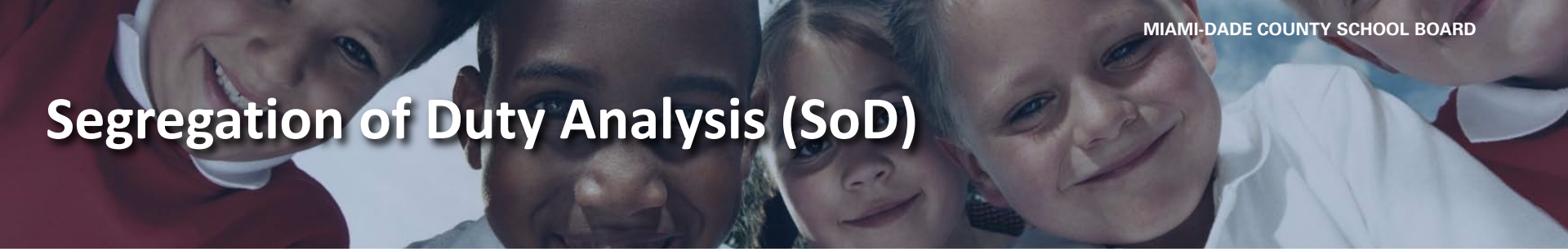
Note: *User count details within Figures 1 & 2, document total users who have been granted an SoD violation at the SoD risk level for each process and associated risk, and do not account for user violations for processes determined to not be utilized or not currently implemented.*

Figure 2 - SoD Conflicts **(***Graphical View*)



The conflicts depicted within the figures above have been further defined by process at the risk level within Appendix-A

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



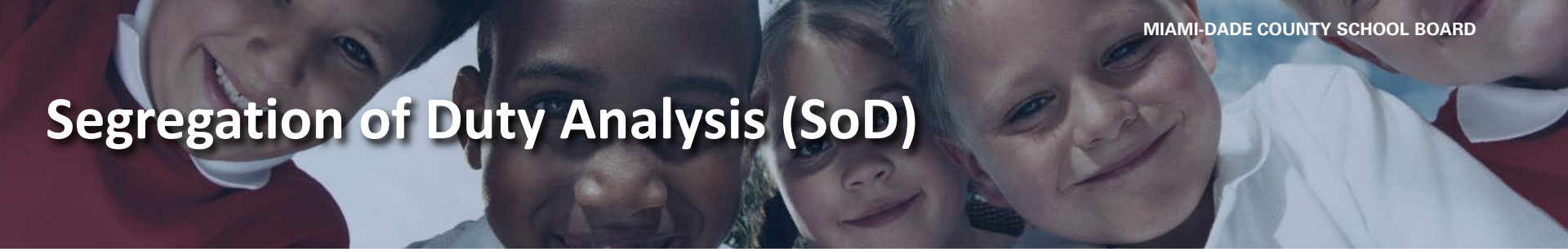
Segregation of Duty Analysis (SoD)

SoD Conflicts Management Responses

Observation Reference	Management Response
Basis SoD Risks	**Utilized** SOD will be reviewed as part of the Segregation of Duty Analysis noted above
Finance SoD Risks **Materials Management SoD Risks** **Procure-to-pay SoD Risks** **Order-to-cash SoD Risks**	**Utilized** SOD will be reviewed as part of the Segregation of Duty Analysis noted above. **Unutilized functionality** Since most of these SODs are for Non-utilized processes their value is limited. Any new process after KPMG analysis should be analyzed using M-DCPS GRC tools. Noting that new processes were in development at the time of this analysis and may have changed.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.



Segregation of Duty Analysis (SoD)

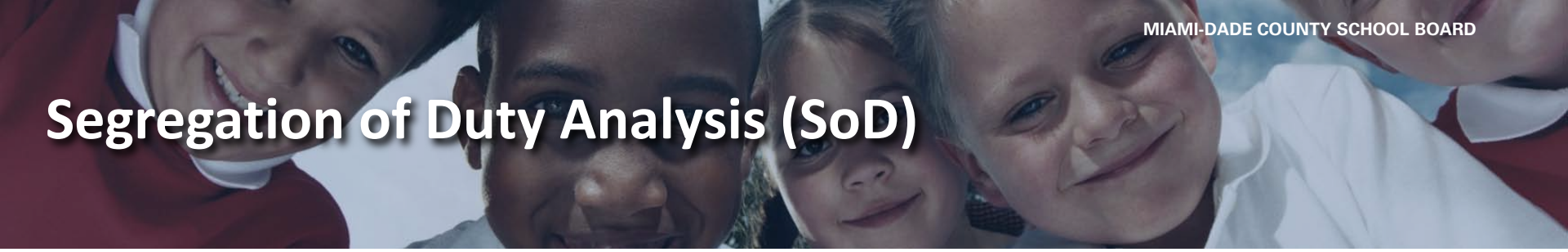
Recommended Next Steps

Based upon the SoD Analysis results and MDCPS' intention to implement SAP's GRC Risk Analysis & Remediation – 'RAR' (formerly Compliance Calibrator) tool, KPMG recommends the following actions to be taken by MDCPS:

Pre-Implementation of RAR

Pre Implementation - Recommended next steps	Management Response
Pre – Implementation of RAR SoD Conflicts Rationalization SoD conflicts identified through this review should be reviewed with appropriate MDCS stakeholders to determine the relevance of each SoD conflict. Appropriate mitigating controls should then be identified for each 'High' risk SoD conflict.	We concur with this observation in that it would be helpful to review the SOD conflicts found by KPMG and GRC. Start: March 5, 2012 Completion: July 3, 2012
Pre – Implementation of RAR Mitigating Control Assessment Each identified mitigating control should then be incorporated to the MDCPS' overall Risk Control Matrix and be identified as a 'key' control. These mitigating controls should be assessed on an on-going basis to determine their operating effectives and their ability to mitigate the risk of the SoD conflict. o These mitigating controls should be assessed on an on-going basis, as the mitigating control does not eliminate the conflict, the SoD conflict and it's associated risk continue to exist. o If mitigating controls are not identified for the 'high' risk conflicts and their operating effectiveness not assessed on and ongoing basis , MDCPS may be exposed to undue IT, Financial, Operational, Fraud, and Audit risks.	We concur with this observation that risks need to be monitored and mitigated on an on-going basis. Once identified, high risk conflicts need to be mitigated. The first risk assessment: February 1, 2012 and ongoing after that.

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



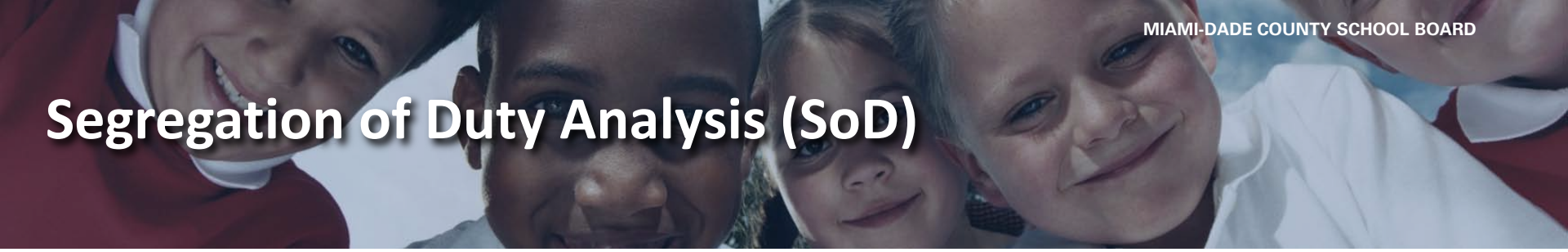
Segregation of Duty Analysis (SoD)

Post-Implementation of RAR

POST Implementation - Recommended next steps	Management Response
1. POST – Implementation of RAR SoD Rulebook Rationalization Once RAR has been successfully implemented , MDCPS should rationalize RAR's global SoD Rulebook to create a rulebook that is specific to MDCPS processes. The Rulebook rationalization process should be a joint effort between IS and Business Process Owners (BPO's). BPO's will validate the appropriateness of process tasks, SoD rules, and risk level. Where IS will be responsible for providing the technical components of the rulebook and loading it into the RAR tool.	We concur with this observation that Rulebook rationalization should take place. In addition, it should be a joint effort between IS and Business Process Owners (BPO's). We expect that this should take place during GRC implementation. Start: March 5, 2012 Completion: July 15, 2012
2. POST – Implementation of RAR SoD Analysis The MDCPS environment should then be assessed against the rationalized rulebook to identify segregation of duties conflicts. o SoD conflicts reporting should then be validated to determine accurate reporting.	We concur with this observation; once GRC has been implemented and the Rulebook has been rationalized, we will develop a schedule of SoD analysis. In addition will be sending SOD reports to the Business Process Owners (BPO). Start: March 5, 2012 Completion: July 15, 2012
3. POST – Implementation of RAR Remediation and Mitigation Each SoD conflict should be evaluated by both business and IT to determine how the conflict is being created/assigned, and remediation strategies identified. o Remediation or access modification to remove the conflict, should be the ultimate goal, however, certain conflicts may be necessary due to various reasons. Only after all remediation options have been evaluated should mitigating controls be applied. The reason for this is that applying mitigating controls do not remove the SoD risk, the risk will continue to exist, the mitigating control only reduces the impact of the SoD risk. o A mitigating control approach, is not recommended as it also increases an organization's 'cost of compliance' as the mitigating control must be assessed on an ongoing basis to determine its operating effectiveness. Where a remediation approach eliminating the SoD risk altogether.	We concur with this observation; once GRC has been implemented, the outcome will be remediation and mitigation. Start: July 15, 2012 and ongoing after that.

KPMG

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.



Segregation of Duty Analysis (SoD)

Post-Implementation of RAR

POST Implementation - Recommended next steps	Management Response
4. POST – Implementation of RAR Governance Process Once all SoD violations have been either remediated and/or mitigated, SoD processes should be incorporated within the MDCPS' overall access provisioning and on-going access verification procedures. o For example, the RAR tool could be utilized to perform 'what-if' analysis reporting to identify potential SoD conflicts prior to access being granted.	We concur with this observation; once GRC has been implemented, a governance process will be created. However, "What if" analysis will prove to be difficult with decentralized user administration. We plan to mitigate these issues by providing BPOs with timely reports (see our response to previous "Access provisioning, modification & de-provisioning: item 2" above). Note that this is consistent with the current MDCPS process of providing RACF reports once the user has been provisioned or de-provisioned.

©2010 KPMG LLP, A Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.