Deloitte.

Подход к выявлению конфликтов и реализации разграничения полномочий

Петр Михеев, Ведущий консультант

15 декабря 2010

Масштаб проблемы

Методология разграничения полномочий

Выявление конфликтов разграничения полномочий

Выявление ключевых операций

- Анализ проектных решений и описаний бизнес-процессов, реализованных/ планируемых к реализации в системе.
- Проведение интервью с функциональными консультантами и пользователями бизнес-процессов.

Определение требований к разграничению полномочий

- Классификация ключевых операций (Авторизация, Отражение в учете, Сохранность ценностей).
- Выявление рисков, конфликтующих ключевых операций и построение матрицы разграничения полномочий.

Сопоставление ключевых операций с транзакциями

- Анализ проектных решений, описаний бизнес-процессов и выявление используемых транзакций.
- Определение используемых стандартных и нестандартных (Z) транзакций, детализация на уровне объектов авторизации.

Определение и выявление конфликтов

- Выявление конфликтов стандартных и нестандартных (Z) транзакций на уровне ключевой операции, с учетом объектов авторизации.

Устранение конфликтов разграничения полномочий

Устранение конфликтов в одиночных ролях

- Корректировка одиночных ролей, в том числе исключение конфликтующих транзакций, разделение одиночных ролей и изменений соответствующих объектов авторизации.

Устранение конфликтов в композитных ролях

- Корректировка композитных ролей, в том числе исключение конфликтующих одиночных ролей, разделение композитных ролей.
- Разработка и внедрение компенсирующих контрольных процедур — контрольных процедур, снижающих риск конфликта полномочий.

Устранение конфликтов на уровне пользователя

- Корректировка перечня композитных ролей, назначенных пользователю.
- Разработка и внедрение компенсирующих контрольных процедур.

Процессы с учетом разграничения полномочий

- Постановка процесса обеспечения разграничения полномочий.
- Интеграция с процессами предоставления доступа и управления изменениями.

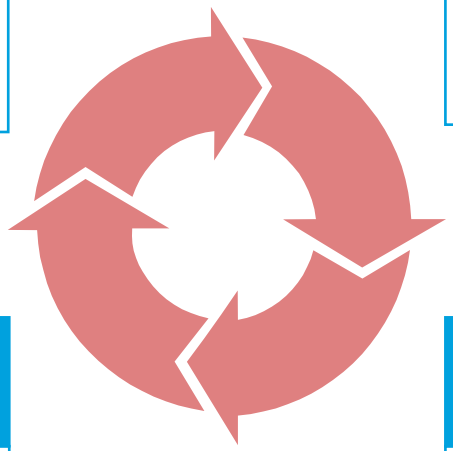
Процессы с учетом разграничения полномочий

Предоставление доступа

Проверка, анализ и согласование разграничения полномочий в рамках процесса предоставления доступа.

Изменения бизнес-процессов и бизнес операций

Актуализация списка ключевых операций, рисков, конфликтующих ключевых операций, определение и выявление конфликтов.



Управление изменениями

Определение используемых транзакций, объектов авторизации, определение и выявление конфликтов.

Регулярные проверки

Выполнение регулярных проверок соблюдения принципов разграничения полномочий с участием внутреннего контроля и аудита.

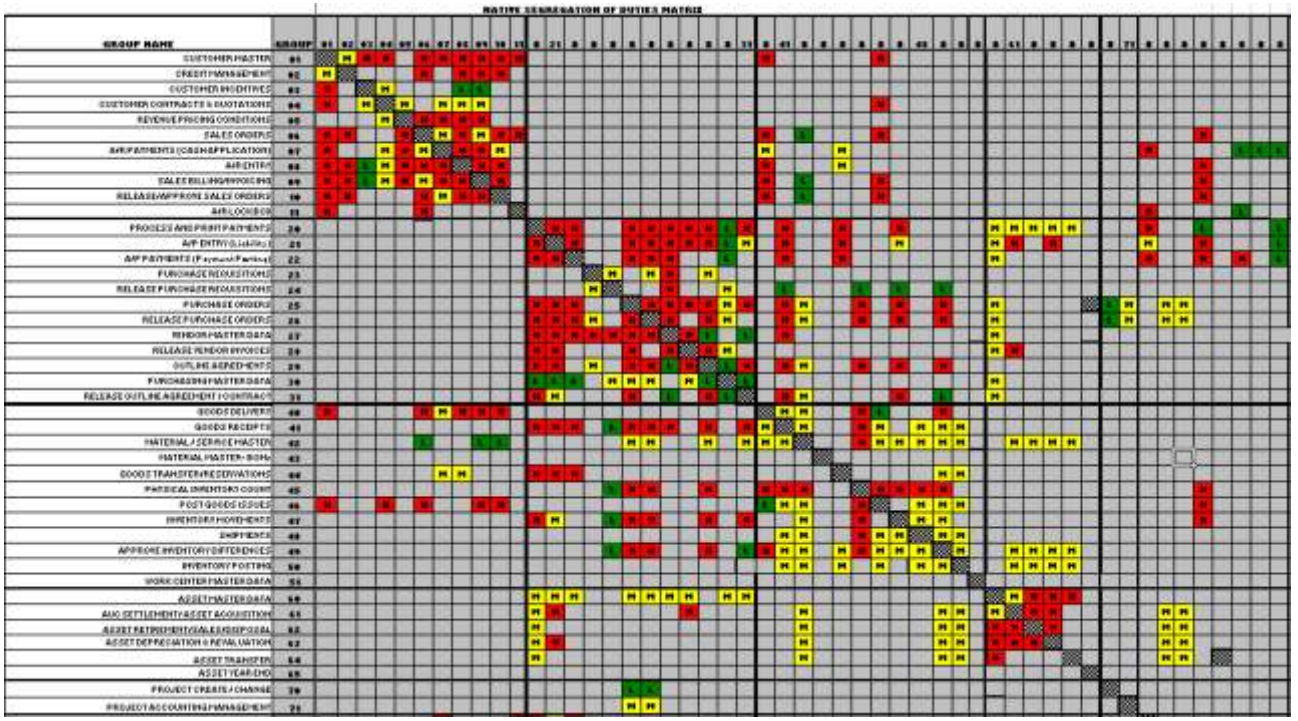
Результаты применения методологии

Концепция разграничения полномочий	• Концепция обеспечения разграничения полномочий – основные принципы и подход.
Матрица разграничения полномочий	• Формирование матрицы разграничения полномочий для выявления и разрешения возможных конфликтов, включая настройку автоматизированных инструментов.
Роли и ответственность	• Определение ролей и ответственности за разграничение полномочий, включая управление доступом, внесение изменений и аудит. Обучение персонала.
Регламентирующие документы	• Подготовка и доработка регламентирующих документов (политики, регламенты, инструкции).

Пример. Выявление конфликтующих транзакций

Пользователь	Код транзакции	Описание транзакции	Группа транзакций	Название группы
USER1	FB70	Enter Outgoing (A/R) Invoices	8	A/R ENTRY
USER1	VL01	Create Delivery	40	GOODS DELIVERY

Стандартная матрица разграничения полномочий содержит основные процессы и соответствующие группы транзакций (внутри группы конфликты отсутствуют) и соответствующие риски, конфликты между группами.



Пример. Конфликты разграничения полномочий

Спасибо за внимание.