



**Опыт внедрения SAP GRC AC.
Организация разграничения полномочий в SAP.**

**Ряжкина Ирина
9.04.2015**

Цели выступления

Поделиться опытом по организации разделения полномочий в SAP в части:

- результатов проекта по внедрению SAP GRC AC;
- подхода к организации разделения полномочий в SAP Группе Северсталь.

Причины возникновения конфликтов полномочий в ИС

- Сжатые сроки внедрения ИС. Отсутствие внимания к ролям и полномочиям пользователей на стадии внедрения ИС;
- Массовое присвоение полномочий пользователям на этапе старта ИС;
- Неконтролируемое изменение ролей;
- Неконтролируемое расширение полномочий пользователя в ИС.
Предоставление пользователю полномочий в обход установленных процедур и контролей;
- Неограниченный доступ разработчиков и консультантов в ИС;
- Неэффективные коммуникации в процессе внесения изменений в ИС.

Решение по организации разделения полномочий в ИС Северсталь.

- ✓ Внедрение SAP GRC Access Control 10.0;
- ✓ Реализованы разработки для модулей:
 - CUP – Workflow согласования запросов расширения полномочий. Настройка интеграции с SAP HCM и MS Active Directory;
 - RAR – Настройка правил распределения полномочий. Настройка Библиотеки компенсирующих контролей;
 - SPM – Настройка правил предоставления расширенных полномочий. Роли FireFighter;

Система	Процесс
SAP ERP SAP BW SAP HCM	1. Управление персоналом 2. Закупки и Управление материальными потоками 3. Сбыт 4. Финансы, контроллинг 5. Консолидация и отчетность 6. Производство 7. Техническое обслуживание и ремонт оборудования

Объем реализации:

Цели проекта:

- Управление доступом пользователей;
- Снижение рисков мошенничества и порчи данных;
- Эффективное управление рисками разделения полномочий;
- Адаптация лучших практик по повышению эффективности СВК;

Задачи проекта:

- Настройка процедуры предоставления полномочий пользователям (WF);
- Разработка матрицы рисков по бизнес-процессам в РС;
- Разрешение SoD-конфликтов с учетом утвержденной матрицы рисков;

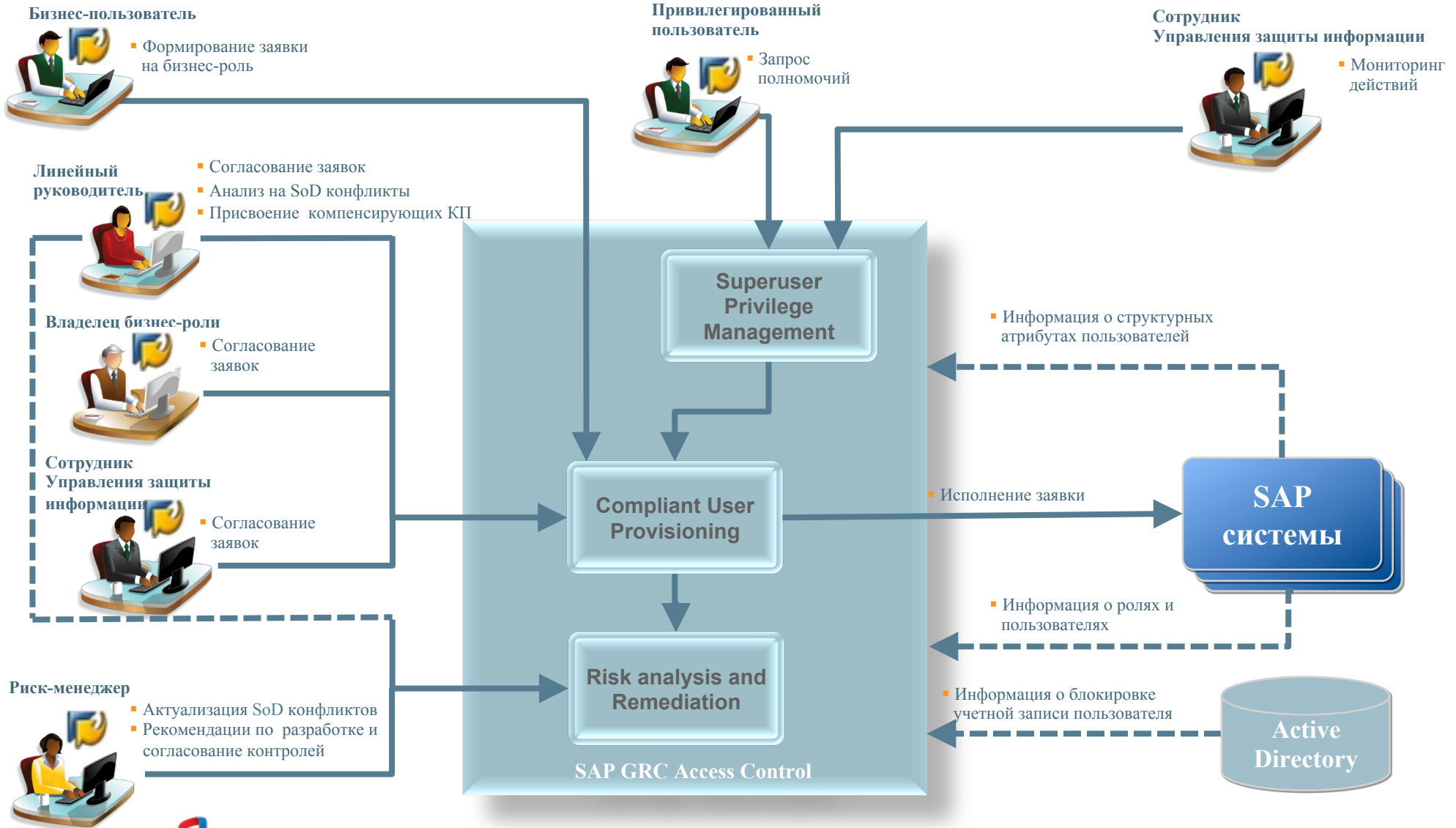
Участники проекта:

- УВАиРМ; Бизнес; ИТ департамент; СБ
- Внешний консультанты: Компания «Делойт» (CUP)
Компания «ПрайсвотерхаусКуперс Раша Б.В.» (RAR)

Реализация:

Год	Мероприятия
2011-2012	<ul style="list-style-type: none">— Внедрение модуля CUP в Северсталь ЧерМК• Workflow согласования запросов расширения полномочий;• Настройка интеграции с SAP HCM и MS Active Directory;• Запуск SAP GRC для согласования запросов пользователей Северсталь ЧерМК— Пилот RAR по бизнес-процессу HCM и P2P в Северсталь ЧерМК
2013	<ul style="list-style-type: none">— Тиражирование модуля CUP на предприятиях Российской стали— Внедрение модуля RAR:<ul style="list-style-type: none">• Разработка и согласование матриц рисков с бизнесом;• Разработка и загрузка правил в матрицу правил GRC;• Очистка ролей от SoD конфликтов;• Очистка профилей пользователей от SoD конфликтов;— Запуск RAR при запросе на расширение полномочий пользователя (по бизнес-процессам)— Настройка процессов по анализу рисков при создании/ изменении ролей
2014	<ul style="list-style-type: none">— Тиражирование модуля CUP на предприятиях Ресурса— Тиражирование модуля RAR на оставшихся предприятиях Российской стали— Настройка процедуры по блокировке полномочий пользователя при проведении HR-мероприятий— Внедрение модуля RAR на предприятиях Ресурса (разработка матриц, правил, очистка ролей и профилей пользователей)— Внедрение модуля SPM
2015	<ul style="list-style-type: none">— Поддержка модуля RAR проектной командой, документирование и подготовка обучающих материалов— Настройка процедур по актуализации матриц, поддержки библиотеки контролей— Передача модуля RAR в поддержку— Разработка автоматизированных средств контроля в SAP GRC PC

Работа пользователей в SAP GRC Access Control

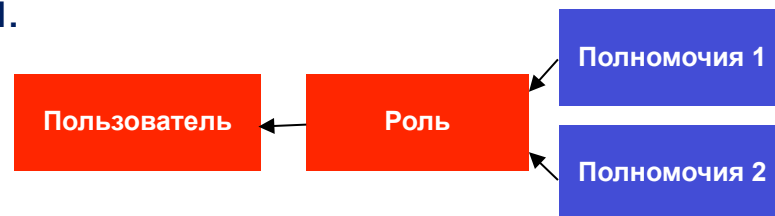


Подход к разграничению полномочий в рамках проекта

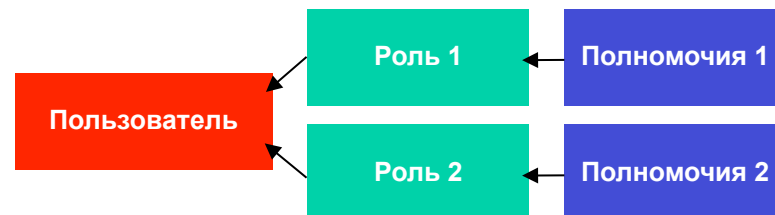
- Разработка матриц правил разделения полномочий с учетом специфики бизнес-процессов Северсталь
- Фокус на устранении рисков разделения полномочий высокого уровня
- Правила распределения полномочий утверждаются владельцами бизнес-процессов

- Устранение рисков на уровне технических ролей.

Снижение количества бизнес-ролей, содержащих SoD-риски



- Устранение рисков у пользователей через удаление излишних полномочий или применение контрольных процедур



Основные этапы работы по бизнес-процессу.

1. Разработка SOD правил, загрузка правил в GRC

- ✓ Знакомство с текущим процессом на предприятиях. Выявление рисков процесса
- ✓ Разработка библиотеки SoD-рисков. Согласование библиотеки внутри проектной команды и с бизнес-экспертами
- ✓ Утверждение библиотеки владельцем бизнес-процесса
- ✓ Составление технических правил с учетом специфики системы. Согласование правил внутри проектной команды. Загрузка правил в GRC

Критические факторы успеха:

- Наличие актуальной документации по внедренному функционалу SAP
- Поддержка и вовлечение владельца бизнес-процесса
- Эффективные коммуникации с бизнес-экспертами и ключевыми пользователями
- Подробное описание рисков, которое понятно бизнес пользователям.

Основные этапы работы по бизнес-процессу.

1. Разработка библиотеки рисков, загрузка правил в GRC

✓ Риск критичной операции:

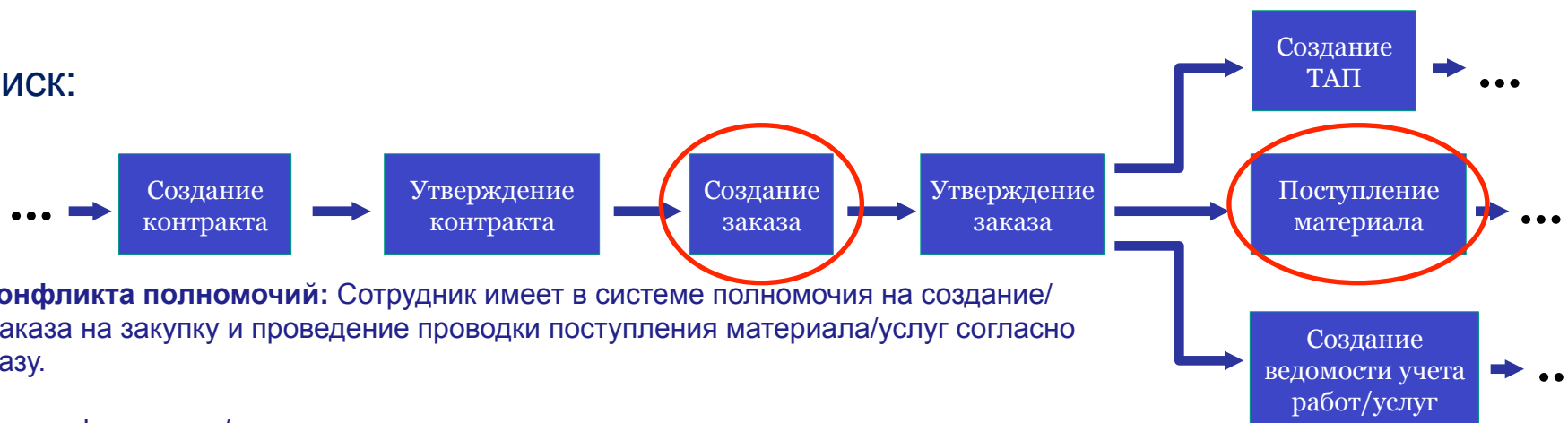


Описание критичной операции: Сотрудник имеет в системе полномочия на изменение основной записи материала (вид материала, тип планирования потребности в материале, код управления ценой и т.д.), тем самым изменяя алгоритм учета материала в информационной системе.

Риск

- Риск искажения статьи запасов в финансовой отчетности.
- Риск неэффективного планирования потребности в материале.

✓ SoD-риск:



Описание конфликта полномочий: Сотрудник имеет в системе полномочия на создание/изменение заказа на закупку и проведение проводки поступления материала/услуг согласно данному заказу.

Риск

- Риск отражения фиктивных/несуществующих запасов.
- Риск ошибочного увеличения складских запасов.
- Риск искажения статьи запасов в финансовой отчетности.

Библиотека рисков по бизнес-процессу Закупки и управление материальными потоками. Формат для согласования с бизнесом

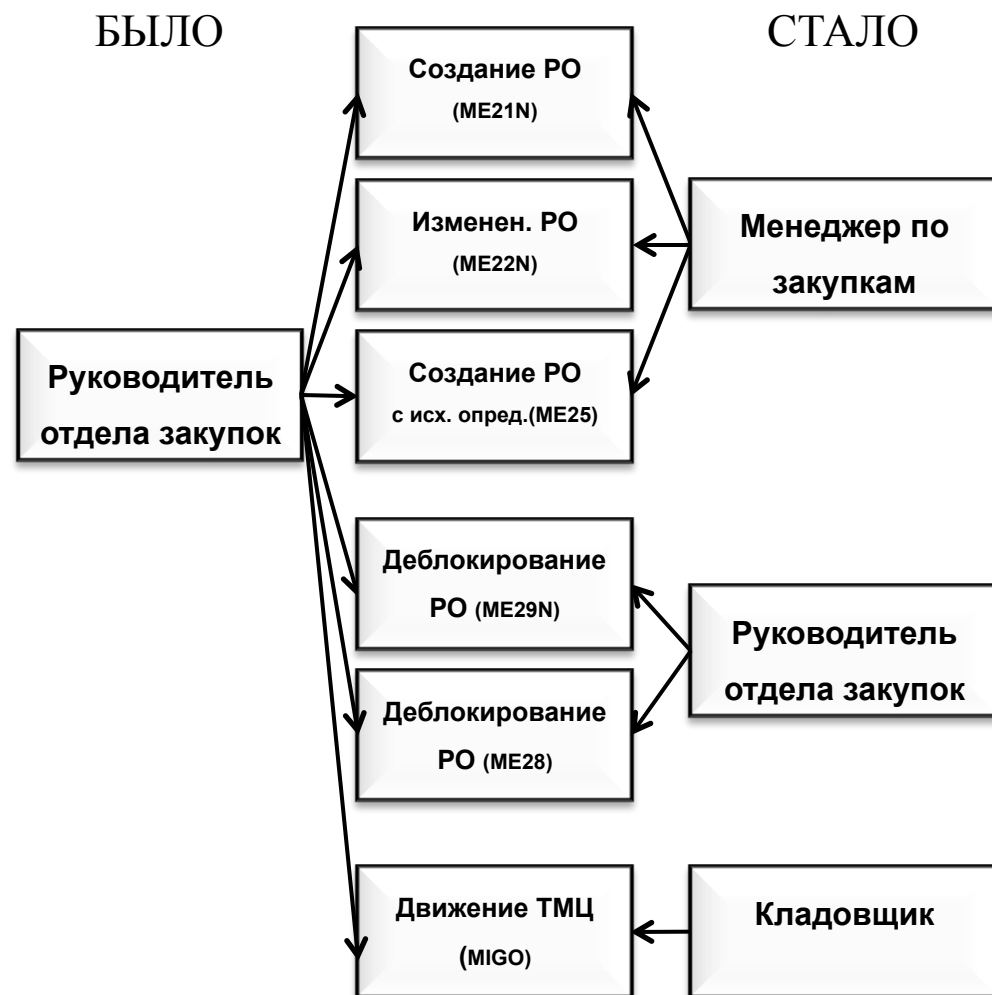
Код риска	Тип риска	Уровень риска	Полное описание конфликта полномочий	Риск	Влияние на бизнес	Ид. Ф1	Описании функции 1	Ид. Ф2	Описании функции 2	Пример
S-P005	Разделение полномочий	Высокий	Сотрудник имеет в системе полномочия на создание/изменение заказа на закупку и проведение проводки поступления материала/услуг согласно данному заказу.	Риск отражения фиктивных/ несуществующих запасов Риск ошибочного увеличения складских запасов Риск искажения статьи запасов в финансовой отчетности	- проведение неавторизованной закупки материалов/услуг - увеличение складских расходов вследствие закупки избыточного количества МТР - срыв графика производства продукции вследствие недостаточной закупки материалов/услуг - отражение в учете неавторизованных/ несуществующих запасов	S-PR02	Создание/изменение заказа на закупку	S-MM07	Поступления материала к заказу на закупку	1. Сотрудник создал фиктивный/ошибочный заказ на закупку (изменил номенклатурные позиции, количество, цены или условия оплаты в разрез существующему договору). 2. Сотрудник выполнил поступление материала в соответствии с фиктивным/ошибочным заказом. 3. Сотрудник изменил заказ на закупку в соответствии с существующим договором для сокрытия факта фиктивной/ошибочной закупки материала. Пример: С поставщиком был заключен договор на закупку 100 тонн титано-магнетитовой руды. Договор был отражен в информационной системе. В системе был создан заказ на закупку соответствующего материала. 1. Сотрудник изменил в заказе на закупку номенклатуру материала (с титано-магнетитовой руды на маритовую). Сумма заказа на закупку осталась без изменений. 2. Сотрудник выполнил поступление материала в соответствии с фиктивным/ошибочным заказом. 3. Сотрудник изменил номенклатуру материала в заказе на поставку для сокрытия мошеннических действий.
S-M006	Разделение полномочий	Высокий	Сотрудник имеет в системе полномочия на проведение поступления/движение материала и ввод результатов инвентаризации.	Риск сокрытия некорректно проведенного поступления материалов Риск финансовых потерь вследствие списания материалов, которые числятся на статье запасов	- скрывание факта хищения/ошибки при поступлении материалов	S-MM05	Поступления материала к заказу на закупку и Движения материалов	S-MM02	Ввод результатов инвентаризации	1. Сотрудник отразил в системе фиктивное/ошибочное поступление материала. 2. Во время инвентаризации сотрудник ввел фиктивные/ошибочные результаты инвентаризации. Пример: Сотрудник имеет договоренность с поставщиком на сокрытие фактов недопоставки продукции. С поставщиком был заключен договор на закупку 100 кг. руды. Договор был отражен в информационной системе. В системе был создан заказ на закупку. Поставщик поставил фактически 90 кг. руды. 1. Сотрудник отразил в системе поступление материала в количестве 100 кг. 2. Во время проведения инвентаризации сотрудник отразил в системе фиктивный результат подсчета материала - 100 кг. Таким образом был скрыт факт физической недостачи в размере 10 кг.

.....
Важно:

- Быть в курсе текущего бизнес-процесса
- Описать риски на языке бизнеса
- Иллюстрировать риски примерами реализации

Основные этапы работы по бизнес-процессу.

2. Выполнение анализа рисков. Мероприятия по снижению рисков



- ✓ Анализ ролевой структуры и профилей пользователей на предмет наличия рисков (SAP GRC)
- ✓ Разработка рекомендаций по устранению рисков на уровне ролей и пользователей
- ✓ Обсуждение рекомендаций со всеми участниками проекта
- ✓ Согласование мероприятий по устранению рисков и изменению ролевой структуры с бизнес-экспертами и владельцами ролей
- ✓ Запрос на изменение роли в соответствии с регламентом

Критические факторы успеха:

- Поддержка и вовлечение владельца бизнес-процесса
- Поддержка ИТ-специалистов в оптимизации ролей в том числе ими же созданных
- Устоявшийся бизнес-процесс

Основные этапы работы по бизнес-процессу.

3. Разработка и согласование контролей для снижения рисков

- ✓ Опрос бизнес-экспертов, пользователей о действующих контролях по выявленным рискам бизнес-процесса. Описание существующих контролей
- ✓ Разработка и обсуждение возможных контрольных процедур внутри проектной команды. Обсуждение предложений с бизнес-экспертами
- ✓ Дизайн контрольных процедур
- ✓ Формирование библиотеки контролей и загрузка контролей в GRC
- ✓ Создание контролей для снижения рисков на уровне пользователей в процессе обработки заявок на расширение полномочий в GRC

Критические факторы успеха:

- Поддержка и вовлечение владельца бизнес-процесса
- Эффективные коммуникации с бизнес-экспертами и ключевыми пользователями
- Максимально «чистые» роли и профили пользователей от SoD-конфликтов
- Устоявшийся бизнес-процесс

Снижение рисков при согласовании запросов пользователей

Запрос доступа: 9000071277 - Windows Internet Explorer предоставлен компанией ОАО Северсталь-инфоком

Запрос доступа: 9000071277

Согласовать Прочие операции Закреть Обновить

Тип запроса Изменить учетную запись Срок исполнения 07.04.2015 Приоритет Средний Ид. пользователя 10378756 Имя пользователя Наталья Борисовна Зернова Автор запроса Наталья Борисовна Зернова Этап Согласование со стороны владельца роли

Утверждающий должен проверить содержимое запроса и выполнить операции согласно политикам компании. Доступ к системе находится на закладке "Доступ пользователя", а подробные данные пользователя — на закладке "Подробная информация пользователя". Также можно выполнить анализ риска и снизить риски на закладке "Нарушения риска". На других доступных закладках представлена дополнительная информация, релевантная для обработки запроса. Скрыть быструю справку

Обновление запроса

Описание: Прошу присвоить мне роли PMN.13.937 и PMN.25.362 для создания сообщений МЗ

Предпросмотр приложений

Таблица не содержит данных

Подр. информ. по запросу

Доступ пользователя Нарушения риска Подробная информация пользователя Параметры Журнал аудита Подробная информация о пользовательской системе Комментарии Приложения

Включить сниженные риски

Выполнить анализ риска

Критерии анализа

Результат

Ракурс: Стандартный ракурс Просмотреть как: Таблица Версия для печати Экспорт Тип: Критичная операция Формат: Итоговый отчет об управл

Ид. пользователя	Имя пользователя	Группа пользователей	Ид. риска доступа	Описание риска	Контролер	Имя контролера	Бизнес-процесс
10378756	Наталья Борисовна Зернова		S-BSCF	Базовые операции по конфигурации			S-BS
10378756	Наталья Борисовна Зернова		S-MNF3	Сотрудник имеет в системе полномочия на корректировку количества списанных материалов			S-MNF
10378756	Наталья Борисовна Зернова		S-MNF5	Сотрудник имеет в системе полномочия на перемещение запаса, проводка переноса материал - материал			S-MNF

Снижение

For org rule analysis when performing mitigation from the risk analysis report do not mitigate the user from management summary report, Only use summary or detail view to mitigate the risk.

Присвоить контроли снижения

Добавить Удалить Статус Срок действия Создать контроль Просм. ПодрИнф

Ид. пользователя	Ид. орг. правила	Ид. риска доступа	Описание	Ид. правила	Система	Ид. контроля	Контролер	Действительно с	Действ. по	Статус
10378756		S-MNF5	Сотрудник имеет в системе полномочия на перемещение запаса, проводка переноса материал - материал	*	*	C-00000934	115006	06.04.2015	05.04.2016	Активно

Ежемесячно ответственный сотрудник производства анализирует в системе SAP движения материалов вида "перенос материала в материал" (отчет MBS1) и выборочно проверяет:
1) наличие авторизованных заявок под каждый вид движений переноса материала в материал
2) соответствие данных в заявке и движений в системе SAP.
Отчет распечатывается и подписывается исполнителем контроля. - Ежемесячно ответственный сотрудник производства анализирует в системе SAP движения материалов вида "перенос материала в материал".

Анализ нарушения рисков в запросах пользователей за период

Моя домашняя страница | Модуль РС | **Отчеты и аналитика** | Модуль RM | УВАИРМ

Инструментальные панели доступа

Исследовать инструментальные панели доступа

Быстрые ссылки

- Библиотека правил доступа
- Библиотека контролей снижения
- Нарушения риска**
- Анализ пользователя
- Анализ роли
- Сравнения нарушений
- Предупреждения
- Библиотека ролей
- Запросы на доступ
- Предоставление полномочий на доступ
- Нарушение риска в запросе на доступ
- Уровень сервиса для запроса на доступ

Отчеты по анализу риска доступа

Просмотреть подробную информацию, связанную с нарушениями

Быстрые ссылки

- Обзор правил доступа
- Правило доступа: подробно
- Отчет по контролю снижения
- Отчет по нарушению риска пользователя
- Отчет по нарушению риска по ролям
- Отчет по нарушению риска для профиля
- Отчет о нарушении риска объекта HR
- Отчет по проверенному объекту
- Уровень пользователя
- Уровень роли
- Моделирование уровня пользователя
- Моделирование уровня роли
- Фоновые задания

Отчеты о запросах на доступ

Просмотреть подробную информацию, связанную с запросами на доступ

Быстрые ссылки

Соотв. назначение пользователей - нарушения риска - Windows Internet Explorer предоставлен компанией OAO Северсталь-инфоком

Нарушения риска доступа

Начальная дата: 04/05/2015
 Конечная дата: 04/06/2015
 Система: STLCINT400
 Тип запроса: All
 Приоритет: All
 Функциональная сфера: All
 Потока операций: Поток операций утверждены

Общее число запросов: 65

■ Снизжение
 ■ Без нарушения
 ■ Нарушение

Нарушения риска доступа подробно

Запрос с нарушениями: 22
 Число нарушений: 265

Критичность	Подсчет
Средн.	0
Высок.	265
Низк.	0
Критич.	0

Общее число запросов: 65

Общие отчеты по управлению доступом

Просмотреть подробную информацию

Быстрые ссылки

Запросы - Windows Internet Explorer предоставлен компанией OAO Северсталь-инфоком

Список запросов

Ресурс: [Стандартный ракур] | Просмотреть как: Таблица | Версия для печати | Экспорт

№	Номер запроса	Тип запроса	Приоритет	Дата отправки	Срок	Имя пользователя
1	9000071259	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Роман Сергеевич Барцев
2	9000071268	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Марк Эдуардович Смулако
3	9000071275	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Анна Михайловна Муратов
4	9000071277	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Наталья Борисовна Зерно
5	9000071293	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Любовь Васильевна Башп
6	9000071294	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Алексей Михайлович Коног
7	9000071298	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Елена Николаевна Ражин
8	9000071303	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Елена Николаевна Ражин
9	9000071304	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Елена Николаевна Ражин
10	9000071323	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Эдуард Васильевич Парыг
11	9000071327	Изменить учетную запись	Средний	06.04.2015	07.04.2015	Ольга Сергеевна Мешкова

Анализ риска на уровне роли

Быстрые ссылки
Библиотека правил доступа
Библиотека контролей сни
Нарушения риска
Анализ пользователя
Анализ роли
Сравнения нарушений
Предупреждения
Библиотека ролей
Запросы на доступ
Предоставление полномо
Нарушение риска в запрос
Уровень сервиса для запр

Отчеты по анализу риска,
Просмотреть подробную и

Быстрые ссылки
Обзор правил доступа
Правило доступа: подробн
Отчет по контролю снижен
Отчет по нарушению риска
Отчет по нарушению риска
Отчет о нарушении риска с
Отчет по проверенному об
Уровень пользователя
Уровень роли
Моделирование уровня по
Моделирование уровня ро
Фоновые задания

Отчеты о запросах на дос
Просмотреть подробную и

Быстрые ссылки
Поиск запросов
Уровень сервиса для запр
Запросы с конфликтами и
Запросы по ролям и утверждающим для присвоения роли
Запросы по RD-структурным профилям

Анализ риска: Уровень роли - Windows Internet Explorer предоставлен компанией ОАО Северсталь-инфоком

Многократный выбор

Критерии анализа

Система: - STLCINT400
Ид. объекта: - MNF.26.001 ПЛАНИРОВЩИК ПРОИЗВОДСТВА
Ид. набора правил: - SG
Уровень риска: - Высок.

Тип объекта: Роль
Тип роли: Бизнес-роль
Офлайн-данные: НЕТ
Тип: Критичная операция
Уровень разрешения

Учитывать организационные правила в анализе риска:
Показать все объекты в отчете по анализу риска: X
Тип ракурса формата отчета: Технический ракурс

Результаты анализа

Набор результатов: Набор результатов 1 | Пуск | Назад | Дальше | Экспорт наборов результатов

Результат

Ракурс: [Стандартный ракур] | Просмотреть как: Таблица | Версия для печати | Экспорт | Тип: Критичная операция
Формат: Итоговый отчет | Снизить риск

Имя роли	Ид. риска доступа	Система	Ид. правила	Уровень риска	Операция	Контроль	Контролер	Ид. организационного правила
MNF.26.001 ПЛАНИРОВЩИК ПРОИЗВОДСТВА	S-MNF3	STLCINT400	000D	Высок.	MIGO			
MNF.26.001 ПЛАНИРОВЩИК ПРОИЗВОДСТВА	S-MNF3	STLCINT400	000F	Высок.	MIGO_GO			
MNF.26.001 ПЛАНИРОВЩИК ПРОИЗВОДСТВА	S-MNF5	STLCINT400	0001	Высок.	MIGO			
MNF.26.001 ПЛАНИРОВЩИК ПРОИЗВОДСТВА	S-MNF5	STLCINT400	0003	Высок.	MIGO_GO			
MNF.26.001 ПЛАНИРОВЩИК ПРОИЗВОДСТВА	S-MNF7	STLCINT400	0001	Высок.	MIGO			

OK | Отменить

Результат

Ракурс: [Стандартный ракур] | Просмотреть как: Таблица | Версия для печати | Экспорт | Тип: Уровень разрешения
Формат: Итоговый отчет | Снизить риск

Имя роли	Ид. риска доступа	Система	Ид. правила	Уровень риска	Операция	Контроль	Контролер	Ид. организационного правила
MNF.26.001 ПЛАНИРОВЩИК ПРОИЗВОДСТВА		STLCINT400			Без нарушений			

Анализ риска на уровне пользователя

Анализ риска: Уровень пользователя - Windows Internet Explorer предоставлен компанией ОАО Северсталь-инфоком

Анализ риска: Уровень пользователя

Критерии анализа

Многokrатный выбор

Критерии анализа

Система: - STLCCLNT400
Ид. объекта: - 70000916
Ид. набора правил: - SG
Уровень риска: - **Высок.**

Тип объекта: Пользователь
Офлайн-данные: НЕТ
Тип пользователя: Диалог
Тип: Критичная операция
Уровень разрешения

Учитывать организационные правила в анализе риска:
Показать все объекты в отчете по анализу риска: X
Тип ракурса формата отчета: Технический ракурс

Результаты анализа

Набор результатов: Набор результатов 1 | Пуск | Назад | Дальше | Экспорт наборов результатов

Результат

Ракурс: [Стандартный ракурс] | Просмотреть как: Таблица | Версия для печати | Экспорт | Тип: Уровень разрешения | Формат: Подробная информация | Снизить риск

Ид. пользователя	Ид. риска доступа	Ид. правила	Уровень риска	Функция	Система	Операция	Дата последнего выполнения	Число выполнений	Ресурс	Расширение ресурсов	Значение с	Значение по	Роль/профиль	Групповая роль	Контроль	Контролер	Ид. органа
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400	MIGO		0	M_MSEG_BMB	BWART	101		ZED:02C:5.7.40 &				
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400	MIGO		0	M_MSEG_BMB	BWART	101		ZED:P3P:2.1.10 &				
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												
70000916	S-P005	000J	Высок.	S-MM07	STLCCLNT400												

Риск доступа: S-P005

Закреть | Violation Historic View

Подробные данные | История изменений

Ид. функции	Описание
S-MM07	S-MM07 - Поступления материала к заказу на закупку
S-PR02	S-PR02 - Создание/изменение заказа на закупку

70001313 | 06.04.2015

OK | Отменить

Организация поддержки процедуры контроля над SoD-рисками

Внедрение процедур контроля для снижения вероятности появления SoD-риска:

в ролях:

- Процедура внесения изменений в роли
- Созданные новые роли анализируются на риски до переноса в продуктив

у пользователей:

- Предоставление/ расширение полномочий пользователей только через SAP GRC AC
- Блокировка полномочий пользователей при проведении HR-мероприятий
- Роли FireFighter. Развитие культуры пользователей с расширенными правами

в бизнес-процессах:

- Анализ изменений бизнес-процессов
- Процедура периодической переоценки SoD-рисков владельцами процессов

Преимущества от внедрения SAP GRC

- Комплексное решение для соблюдения требований разграничения полномочий и подтверждения достоверности финансовой отчетности
- Повышение эффективности управления жизненным циклом полномочий пользователей и ролей:
 - Обеспечение корректной обработки запроса пользователя на расширение полномочий в ИС
 - Обзор нарушений SOD и доступа к критическим транзакциям
 - Организация контроля над полномочиями пользователя (снижение рисков)
 - Моделирование ролей и присвоений пользователям
 - Стандартная отчетность по анализу рисков, пользователей
- Минимизация времени и затрат на аудит

Основные проблемы и их решение в рамках проекта

Проблемы	Решение
Трудности в понимании рисков.	Расширение описательной части рисков: 1) Подробное описание риска; 2) Влияние на бизнес; 3) Примеры возможных ошибок и/ или мошеннических действий.
Недостаточно актуальная документация, в том числе из-за изменений бизнес-процессов. Ограниченное описание собственных доработок (Z-транзакции).	Проведение дополнительных интервью с бизнес-пользователями для понимания процесса реализованного в SAP
Изменение текущего каталога ролей = перевнедрение.	Работа с текущим каталогом ролей. Оптимизация текущей ролевой структуры
Обнаружение новых рисков в вычищенных ролях и профилях пользователей.	Внедрение процедур контроля в процессы изменения ролей и расширение полномочий пользователей
Отсутствие возможности применения стандартных контролей (на примере SAP HCM)	Разработка ручных, частично автоматизированных контролей
Оптимизация численности/ Небольшие предприятия. Расширение полномочий пользователей, в т.ч. появление в профиле пользователей SoD-конфликтов	Настройка контролей в модуле SAP GRC PC

Достичь большего вместе

Северсталь 2012. Любое несанкционированное использование, копирование, раскрытие или распространение материалов, содержащихся в данном документе (или приложениях к нему), строго запрещено. Коммерческая тайна ОАО «Северсталь». 162600, Российская Федерация, Вологодская область, г. Череповец, ул.Мира, 30