

SAP Fraud Management & GRC

Алексей Бабиченко
2013



Основные функции SAP GRC Risk Management

Планирование

- Определение целей, объектов, категорий рисков,
- Определение орг.структуры, риск- аппетита, КРИ
- Присвоение ответственных

Выявление и анализ

- Ведение карточек риска (причин, последствий, владельцев)
- Качественный и/или количественный анализ
- Автоматические уведомления по анализу/переоценке риска
- Обработка сообщений о потенциальных рисках

Обработка риска

- Управление мероприятиями по снижению риска
- Автоматическая оценка остаточного риска

Мониторинг

- Динамическая карта,
- Стандартные параметрические отчеты
- Мониторинг текущих значений КРИ

Основные функции SAP GRC Process Control

Планирование СВК

- Описание среды ВК (политик, рисков, процессов, орг.структуры контролей)
- Ведение каталогов опросных листов, планов тестирования, автоматических контролей
- Присвоение ответственных

Тестирование, выявление отклонений

- Определение объема, проведение тестирования
- Выполнение автоматических контролей бизнес приложений
- Регистрация результатов, эскалация выявляемых отклонений

Обработка отклонений

- Разработка и контроль мероприятий по обработке выявленных отклонений
- Делегирование, эскалация исключений

Мониторинг

- Мониторинг выявленных отклонений
- Отчетность по результатам проверок
- Подтверждение эффективности СВК

Основные функции SAP GRC Access Control

Контроль распределения полномочий

- Ведение встроенной SoD матрицы
- Анализ профилей полномочий пользователей
- Контроль доступа к наиболее значимым операциям
- Моделирования изменений профилей полномочий

Предоставление полномочий

- Обработка запросов на предоставление полномочий сотрудникам
- Документирование подтверждений запросов, моделирование, анализ рисков нарушения SoD
- Контроль фактического использования предоставленных полномочий

Управление ролями

- Ведение централизованного каталога ERP ролей
- Формирование, анализ, подтверждение новых ролей

Управление расширенными полномочиями

- Ведение регламентов расширения полномочий
- Автоматическое предоставление расширенных полномочий в экстренных случаях
- Контроль фактических действий



Обзор решений

SAP Fraud Management on HANA

На сколько велика проблема?

5%

Среднестатистическая
компания теряет около
5% прибыли из-за
мошенничества

Размер потерь от
мошенничества в
2011 году

\$3.5
trillion

Source: 2012 Report to the Nations on Occupational Fraud and Abuse,
Association of Certified Fraud Examiners

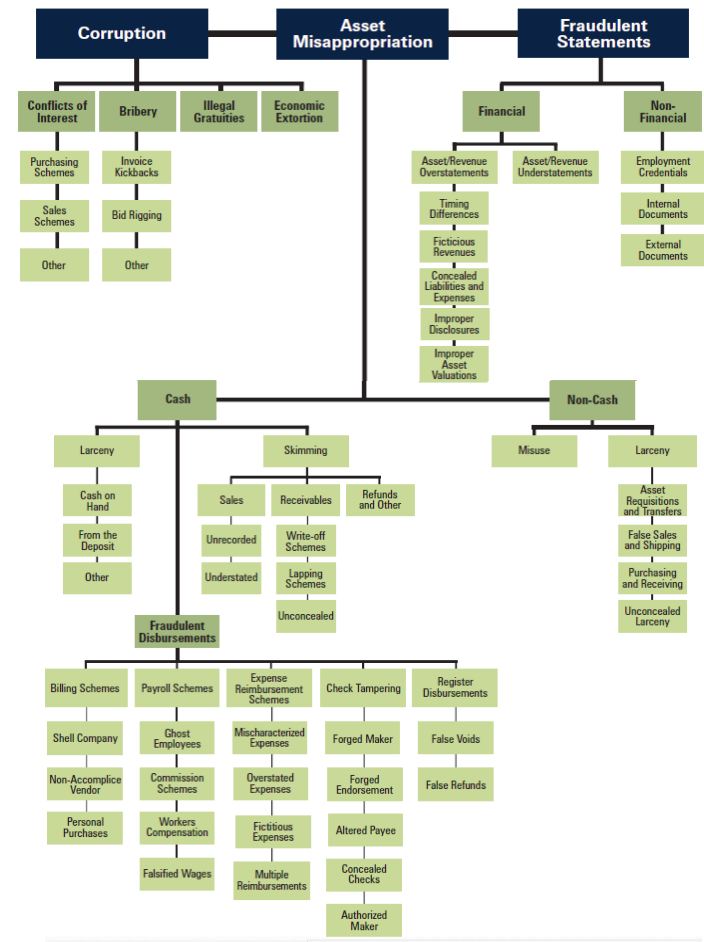
Где Риски?

- Наиболее подвержены хищениям следующие индустрии:

- Government
- Manufacturing (Oil&Gas, Mining, etc)
- Banking/financial services

- 80% хищений выявлены в следующих департаментах:

- Accounting
- Executive
- Operations
- Customer service
- Sales
- Purchasing



SAP Fraud Management

Быстрое и точное выявление и предотвращение мошенничества.

Раннее выявление мошенничества

Использование скоростных характеристик SAP HANA

Интеграция в бизнес-процессы

Нотификация и управление



Увеличение точности обнаружения

Уменьшение количества ложных сигналов благодаря управлению и моделированию в режиме реального времени

Возможность оперировать сверхбольшими объемами данных благодаря SAP HANA



Предотвращение

Обнаружение признаков мошенничества происходит с использованием моделирования и предиктивной аналитики



SAP Fraud Management

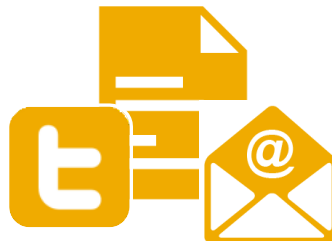
Перекрестный анализ связанный и интегрированный с SAP HANA

Big Data



- Терабайты обработанные со скоростью мысли
- Загрузка большого объема данных в память

Текстовой поиск



- Полнотекстовый поиск
- Графическое моделирование поиска

Предиктивная аналитика



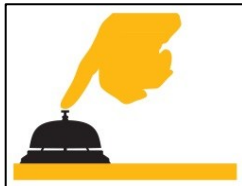
- Раскрытие потенциала большого объема данных
- Построение и визуализация комплекса предиктивных индикаторов
- Возможность использования предиктивной аналитики всеми сторонами бизнеса

SAP Fraud Management

Предупредить – Обнаружить – Расследовать - Отслеживать



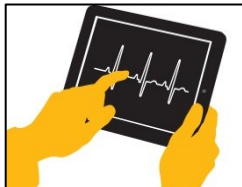
Предупредить мошенничества используя гибридные стратегии, как комбинацию правил и предиктивных индикаторов



Обнаруживать мошенничество в режиме реального времени в любой момент, тогда, когда это необходимо с помощью SAP HANA



Расследовать подозрительные транзакции используя весь доступный инструментарий



Мониторинг процесса обнаружения мошенничества в режиме онлайн с возможностью моделирования и калибровки

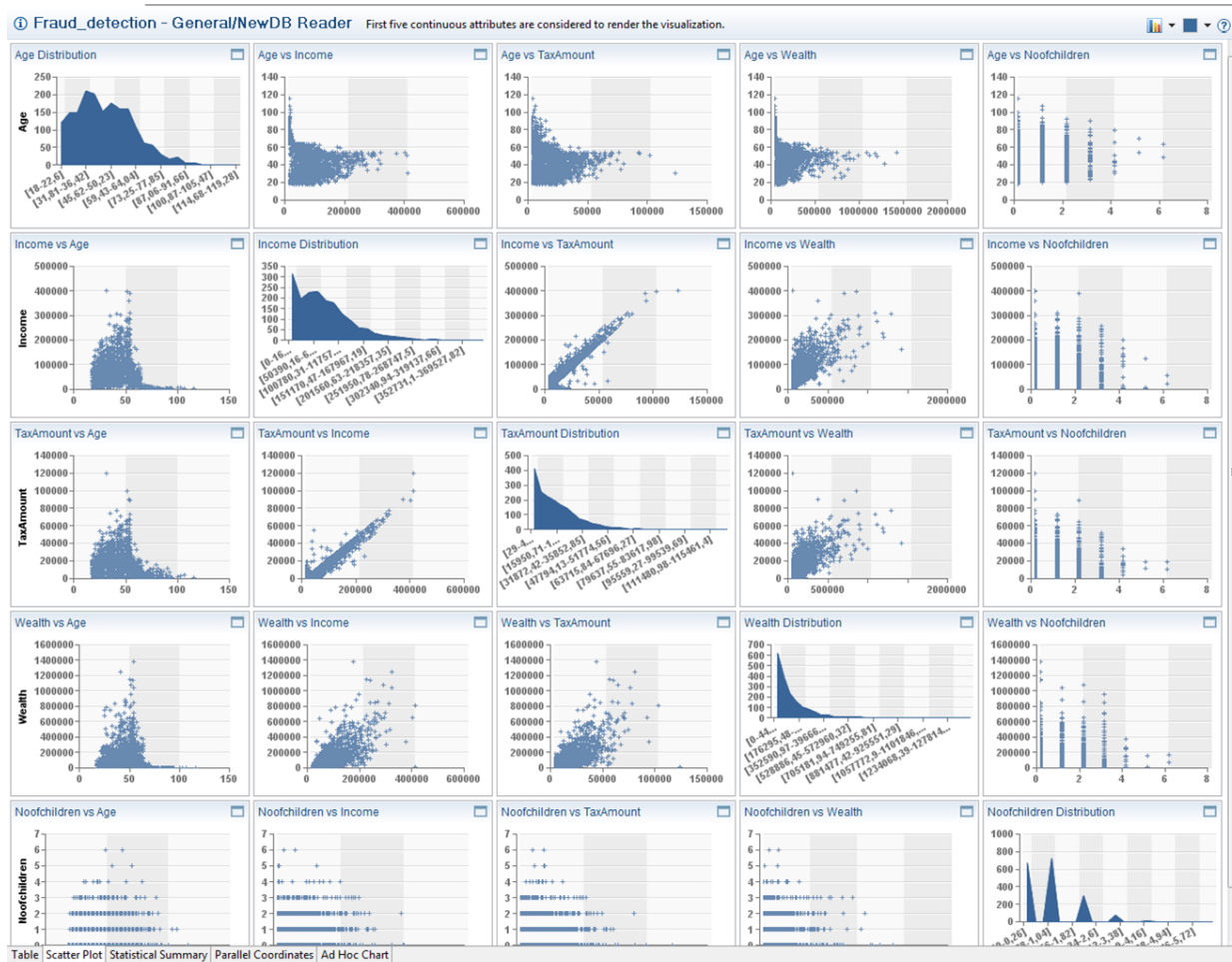


SAP HANA – высокопроизводительная, настраиваемая стандартная платформа

Панель управления Fraud Management



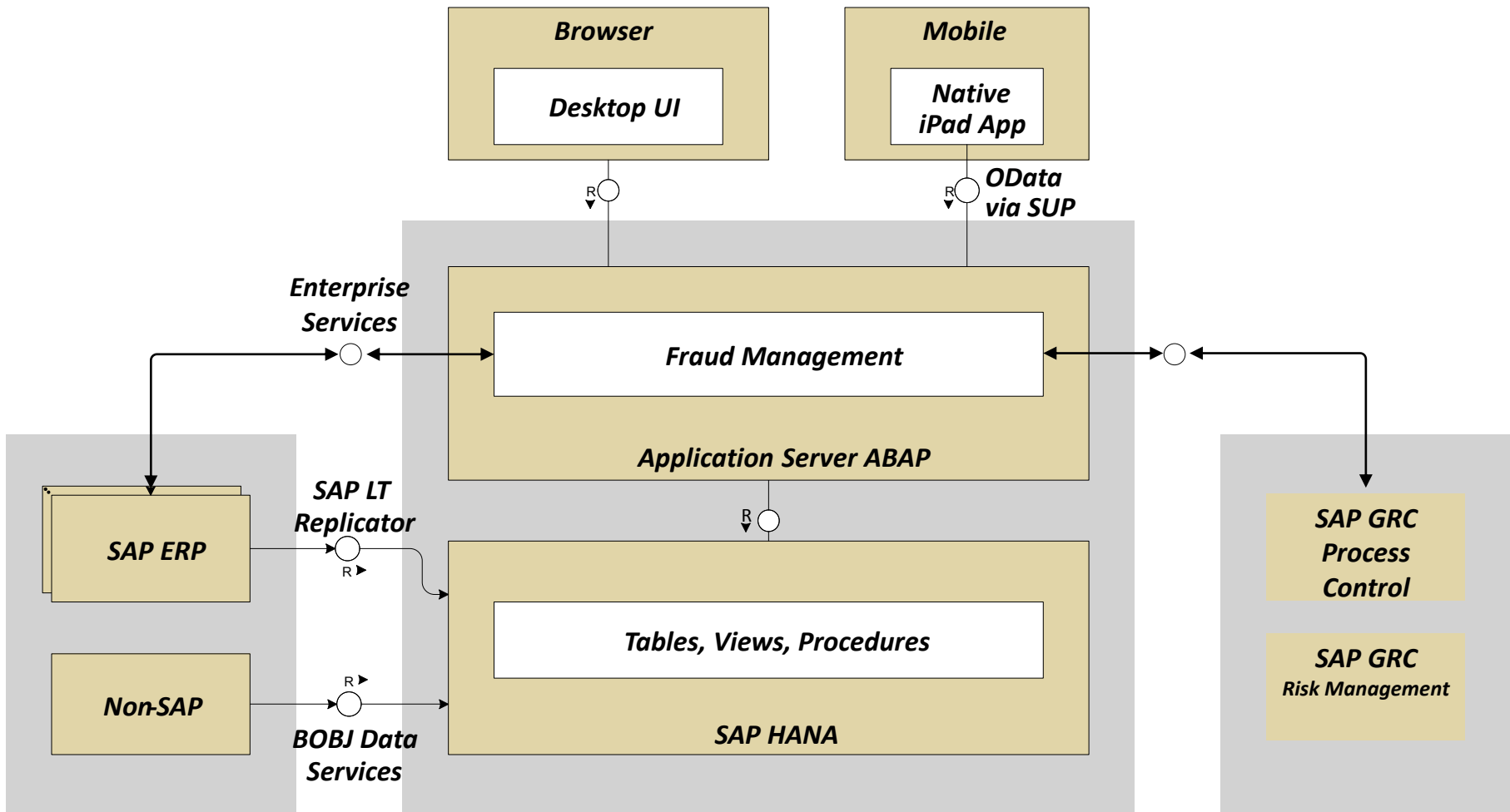
Перекрестный анализ



Scatter Plot

SAP Fraud Management

Архитектура



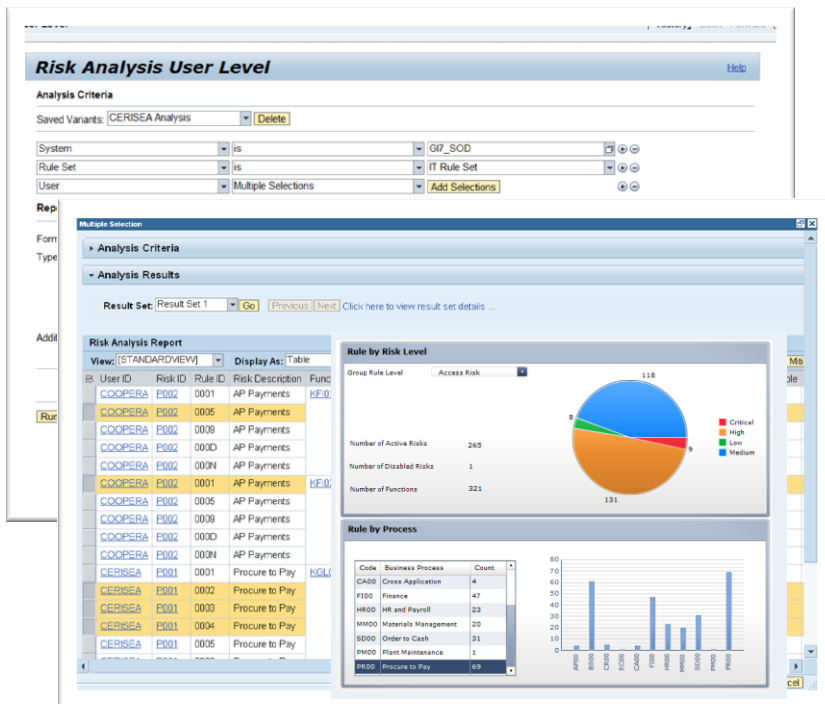


Обзор решений

SAP GRC Access Control

Анализ рисков доступа

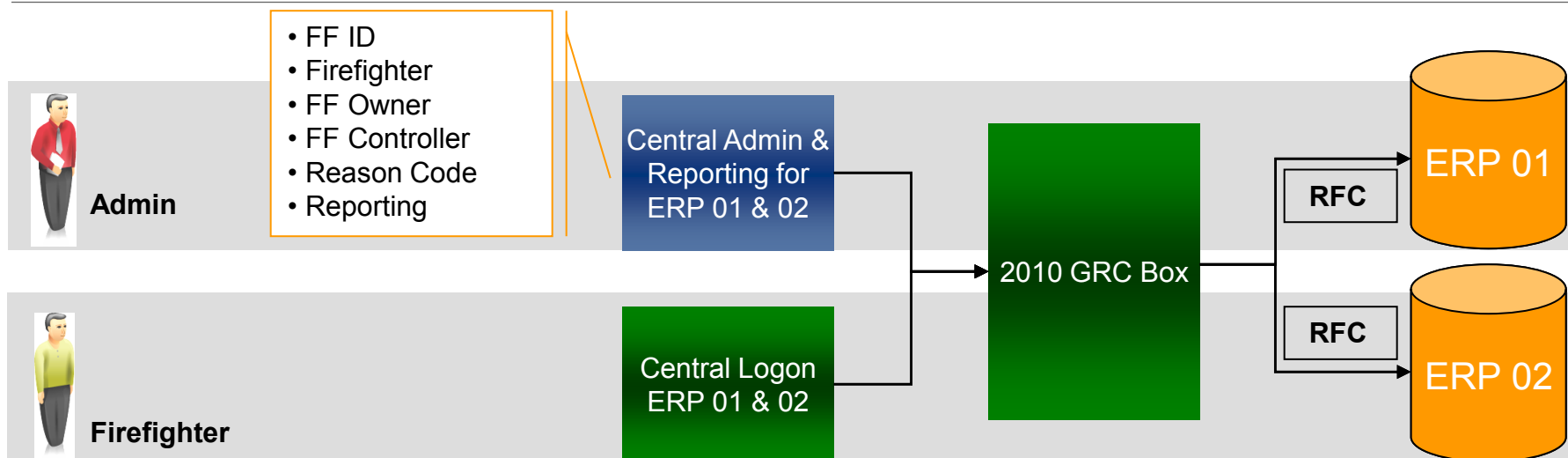
Среда для анализа рисков доступа с интуитивным интерфейсом, который поддерживает настройку бизнес-пользователей (персонализацию). Поддерживает массовые операции, генерирует данные аудита, предлагает возможности для смягчения рисков.



- Библиотека правил для определения рисков доступа в контексте SoD.
- Формализованное представление правил упрощает совместную работу бизнеса и IT.
- Позволяет выполнить детальный анализ рисков по пользователям и ролям.
- При работе использует данные, полученные в реальном времени из SAP, Oracle, JD Edwards, PeopleSoft и разработанных приложений (при наличии коннектора).
- Быстрое устранение конфликтов.
- Проактивное управление проверками для смягчения рисков.
- Периодическое подтверждение назначенных проверок для смягчения рисков.
- Симуляция изменений в составе ролей пользователя для анализа риска.
- Мониторинг конфликтов в рамках периодического анализа на риски SoD.

Централизованный доступ для пользователей с чрезвычайными полномочиями

2



- Согласование и отслеживание заявок на предоставление чрезвычайных полномочий в рамках документированного и аудируемого процесса.
- Предоставление временного доступа с заданными сроками действия.
- Автоматическое присвоение идентификатора чрезвычайного доступа после согласования.
- Все действия, предпринимаемые в рамках сессий пользователя с чрезвычайными полномочиями записываются в лог и отчеты об использовании.
- Связанный workflow процесс обеспечивает своевременный анализ таких отчетов.
- Управление исключениями между ожидаемыми и фактическими действиями через запросы workflow.

Автоматизированное присвоение ролей пользователям

Access Control использует стандартную функциональность SAP Business workflow и обеспечивает гибкие и настраиваемые процессы по обработке заявок на доступ.

The screenshot displays two SAP web interfaces. The top interface is an 'Access Request :80567' showing details like Request Type (Change Account), Due Date (13.02.2011), Priority (High), User (ZERNALNEWS), and Requestor (ZERNALNEWS). Below this is a 'Reason for Request' section and an 'Attachments Preview' section with a message: 'The table does not contain any data'.

The bottom interface is a 'User Access Review :10378344' showing details like Request Type (UAR_Review), Due Date (00.00.0000), Priority (UAR_HIGH), and Coordinator (UAR_MAN1). It includes a 'Review Instructions' section with detailed text about the review process. Below the instructions is a 'Review Status' section showing 'Total Users: 1', 'Approved: 1', and 'Rejected: 0'. There are tabs for 'User Access', 'Audit Log', 'Attachments', and 'Comments'. The 'User Access' tab is active, showing a table with columns: View By, User, Type, Description, System, Usage, Action, Comments, and Reason. The table lists three roles for user Vandana Maini: 'SAP_GAP_CUST_CC' (cross client customizing), 'SAP_GAP_ROLES_ADMIN' (Authorization for Roles), and 'SAP_GAP_ROLES_ADMIN_AC_TS' (Authorization for Roles). Each role has a status of 'Approved' or 'Remove' with a corresponding 'Add Comments' link.

- Сервисы самообслуживания обеспечивают простой и быстрый способ подачи заявок на доступ.
- Автоматизированные workflow обеспечивают эффективное согласование заявок.
- Встроенный анализ рисков (в реальном времени) препятствует появлению конфликтов, не обеспеченных средствами контроля.
- В логах аудита и отчетах сохраняется всеобъемлющая информация для поддержки внутреннего или внешнего аудита.
- Автоматизированные процессы для перепроверки полномочий доступа у пользователей.

Бизнес-ориентированное управление ролями

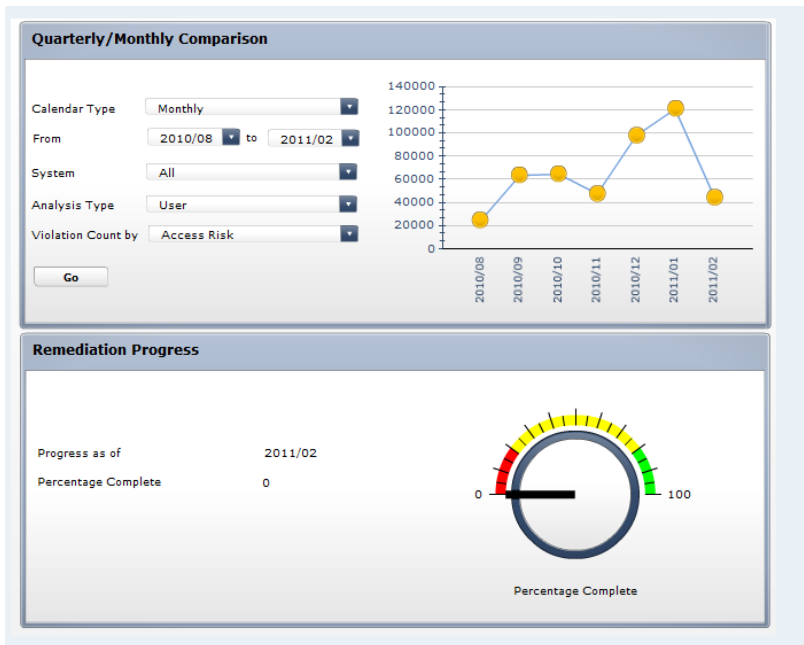
Access Control предоставляет функции для организации процесса совместной разработки бизнес-ролей со встроенной проверкой на риски (симуляции).



- Документирование изменений в составе ролей и обеспечение соответствующих процессов согласования в рамках интегрированного workflow.
- Поддержка как технических, так и бизнес-пользователей для установки соответствия между техническими авторизациями и бизнес-функциями.
- Кросс-системный анализ рисков для анализа состава ролей в SAP и non-SAP ландшафте.
- Анализ параметров фактического использования ролей для обеспечения оптимального присвоения ролей пользователям или своевременной актуализации ролей.
- Автоматическое обновление присвоений роли пользователям в случае, внесения изменений в роль.
- Периодическая проверка присвоений роли, авторизаций в составе роли.

Единое решение для управления централизованной стратегией GRC на предприятии

5

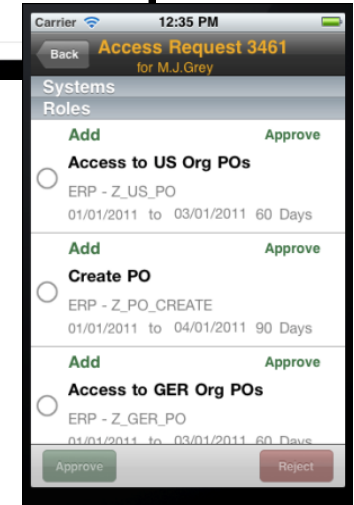
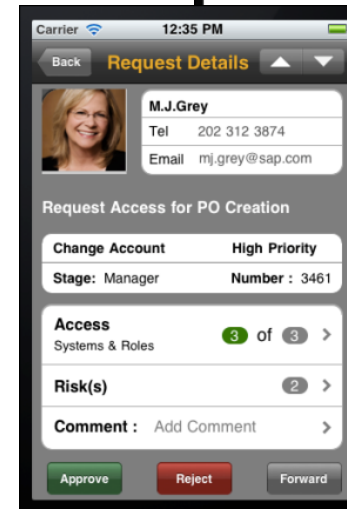
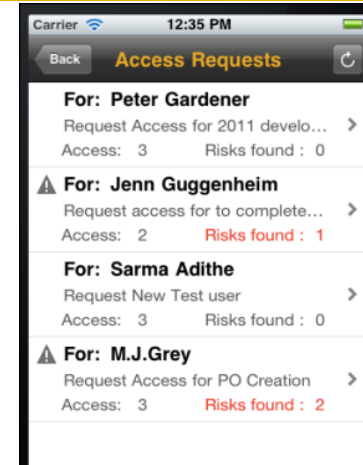


- Встроенные SAP Dashboards и отчеты Crystal reports дают визуальное представление об эффективности в управлении рисками доступа.
- Открытый framework позволяет перенастраивать отчеты при помощи внешних средств анализа и генерации отчетности.
- Тесная интеграция с SAP BusinessObjects Process Control и Risk Management для реализации централизованной стратегии корпоративного GRC.

SAP Access Approver mobile app

Предоставление доступа

- Списки запросов на доступ
- Детализированная информация по запросу
- Анализ рисков доступа
- Запрос дополнительной информации для предоставления доступа
- Комментарии по запросу
- Перенаправление запроса (делегирование)



Экономическая выгода при использовании SAP GRC Access Control



Сокращение затраченного времени на 20% и повышение эффективности управления бизнес ролями на 80% с помощью SAP BusinessObjects Access Control



Автоматизация 92% пользовательских запросов на доступ с SAP BusinessObjects Access Control



Разрешение 91% конфликтов распределения полномочий



Спасибо за внимание!

Контактная информация:

Алексей Бабиченко

Менеджер по развитию бизнеса, GRC

alexei.babichenko@sap.com

+7 926 395 54 44

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, PowerPoint, Silverlight, and Visual Studio are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, z10, z/VM, z/OS, OS/390, zEnterprise, PowerVM, Power Architecture, Power Systems, POWER7, POWER6+, POWER6, POWER, PowerHA, pureScale, PowerPC, BladeCenter, System Storage, Storwize, XIV, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, AIX, Intelligent Miner, WebSphere, Tivoli, Informix, and Smarter Planet are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the United States and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and its affiliates.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems Inc.

HTML, XML, XHTML, and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Apple, App Store, iBooks, iPad, iPhone, iPhoto, iPod, iTunes, Multi-Touch, Objective-C, Retina, Safari, Siri, and Xcode are trademarks or registered trademarks of Apple Inc.

IOS is a registered trademark of Cisco Systems Inc.

RIM, BlackBerry, BBM, BlackBerry Curve, BlackBerry Bold, BlackBerry Pearl, BlackBerry Torch, BlackBerry Storm, BlackBerry Storm2, BlackBerry PlayBook, and BlackBerry App World are trademarks or registered trademarks of Research in Motion Limited.

Google App Engine, Google Apps, Google Checkout, Google Data API, Google Maps, Google Mobile Ads, Google Mobile Updater, Google Mobile, Google Store, Google Sync, Google Updater, Google Voice, Google Mail, Gmail, YouTube, Dalvik and Android are trademarks or registered trademarks of Google Inc.

INTERMEC is a registered trademark of Intermec Technologies Corporation.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

Bluetooth is a registered trademark of Bluetooth SIG Inc.

Motorola is a registered trademark of Motorola Trademark Holdings LLC.

Computop is a registered trademark of Computop Wirtschaftsinformatik GmbH.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, SAP HANA, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase Inc. Sybase is an SAP company.

Crossgate, m@gic EDDY, B2B 360°, and B2B 360° Services are registered trademarks of Crossgate AG in Germany and other countries. Crossgate is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.