INFORMATION
MANAGEMENT
&TECHNOLOGY

Информационные технологии риск и контроль для финансовых систем

Семинар Казначейского Сообщества PEMPAL

2011 г.

Кристин Ладо Туфан

THE WORLD BANK GROUP

Введение

- Офицер по вопросам риска и соответствия ИТ в области управления информацией и информационных технологий (IMT) Всемирного банка, сертификаты CISA, CRISC
- Руководство отделом внутреннего контроля банка в области финансовой отчетности (ICFR) общий контроль ИТ с 2007 года по настоящее время
- В 2000 – 2005 гг. консультации Development Gateway Grantees в Монголии, Шри-Ланке и Восточно-Карибском регионе (с Румынией) по Интернет бизнес планам и внедрению в поддержку министерств и доноров

- Всемирный банк добровольно соблюдает требования ICFR (сходные с US Sarbanes-Oxley) в качестве хорошей практики
- Приложения, входящие в компетенцию Банка, включают SAP, PeopleSoft и многочисленные казначейские приложения
- Соответствие ICFR – это не одноразовое событие, это метод ведения дел

План

- Общие средства и методы внутреннего контроля для обеспечения разумной гарантии относительно компетентности, точности и целостности вашего FMIS для финансовой отчетности
- Основы для оказания помощи в реализации процессов и мер контроля
- Конкретные операционные и информационные меры контроля безопасности для каждого уровня вашего FMIS
- Пример Всемирного банка – безопасный веб-портал
    - «Доверие – это не контроль»
    - Делайте то, что документируете, и документируйте то, что делаете»

Контекст Банка …

- **SAP**: Global ERP с 24 000 пользователей; 12+ крупных приложений, включая стандартные модули, такие как AP/AR и самостоятельно разработанные приложения для выплаты ссуд и для поездок; приблизительно 8,6 млн. операций в месяц
- **PeopleSoft**: Global ERP приблизительно с 18 500 динамичными ролями/пользователями и 1 033 статическими ролями; всего приписано 3 756 операций; поддерживает процессы отдела кадров, выплату зарплат, пенсий
- Банк самостоятельно разработал **безопасный веб-сайт (соединение с клиентом),** который предлагает правительственным чиновникам и агентствам по реализации проектов более быстрый доступ к информации об их портфеле и аналитической работе Банка по стране
- У Банка также имеется множество **казначейских приложений** для поддержки казначейских операций
- **Удаленный доступ**: У Банка имеется несколько вариантов для удаленного доступа, все активируются двухфакторной аутентификацией
- В настоящее время всего тестируется **148 основных мер контроля** каждый год по всем финансовым системам на предмет мер внутреннего контроля над финансовой отчетностью (ICFR)

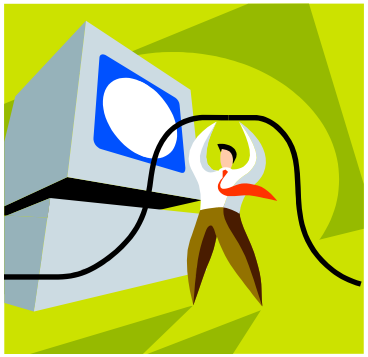
Некоторые риски информационных технологий для финансовых систем

- **Несанкционированный доступ:** доступ пользователя/разработчика не был одобрен для определенного уровня или действия; Пример: позаботиться о том, чтобы привилегированный доступ был должным образом ограничен.
- **Избыточный доступ:** Уровень доступа пользователя/разработчика выходит за рамки должности и обязанностей; Пример: Позаботиться о том, чтобы имелся принцип наименьших привилегий – чтобы у людей был доступ только к той информации и транзакциям, которые необходимы для выполнения их работы и служебных обязанностей
- **Несанкционированные изменения:** Изменение программы не было одобрено до передачи в производство; Пример:
- **Мошенничество –** это потенциальный результат этих рисков, если действия преднамеренные
- **Отсутствие контроля** за приобретением и внедрением новых приложений и обслуживанием существующих приложений
- **Отсутствие контроля** за приобретением, установкой, конфигурацией, интеграцией и обслуживанием инфраструктуры ИТ.

Средства и методы внутреннего контроля

- **Контроль на уровне организаций**
  - Тон со стороны руководства и соответствующая культура в организации
  - Руководство заботится о том, чтобы имелись политики и процедуры, и чтобы все сотрудники были осведомлены о них и следовали им
- **Управление приложениями**
  - Разработка и обслуживание приложений
  - Доступ к программам и данным/информации

Контроль безопасности (применяется на всех уровнях



- **Общие меры контроля информационных технологий**
  - Управление инфраструктурными изменениями: база данных, системное программное обеспечение, сеть
  - Операции информационных систем: пакетная обработка заданий, создание резервных копий и восстановление

Люди, процесс, технология

Полезные принципы, в качестве основы для средств и методов внутреннего контроля

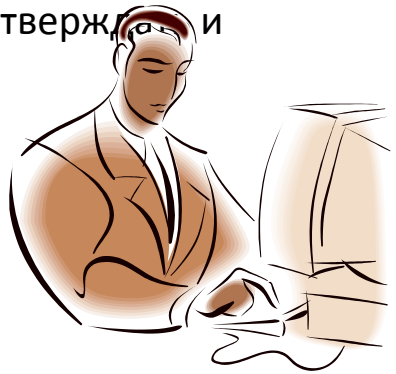
- **COSO/COSO ERM** (Комитет спонсорских организаций Комиссии Тредуэя): Интегрированные принципы для внутреннего контроля, фокусирующиеся на средствах и методах контроля, на оценке риска, контрольной деятельности, информации, коммуникации и мониторинге
- **COBIT** (ISACA): Задачи контроля для информационной технологии, которые фокусируются на четырех основных областях: Планировать и организовать, Приобретать и внедрять, Доставлять и поддерживать, Проводить мониторинг и оценивать
- **ITIL** (Библиотека инфраструктуры информационных технологий) Принципы практики руководства службой ИТ, такие как управление изменениями, управление инцидентами, управление проблемами, управление конфигурацией, управление уровнем сервиса
- **CMMi** (Институт по разработке программного обеспечения): Интегрированная модель зрелости процессов программного обеспечения для цикла разработки программного обеспечения
- **ISO20000**: Принципы и сертификация для руководства ИТ службы
- **ISO27001**: Принципы и сертификация для информационной безопасности
- **RiskIT** (ISACA): Бизнес риски, связанные с ИТ, фокусирующиеся на оценке риска, также на мониторинге риска/отчетности

Разработка и обслуживание приложений

- **Основные риски:** Несанкционированный доступ/изменения, Избыточный доступ, Мошенничество; Не действенные меры контроля в работе
- **Документация** процесса и идентификация основных мер контроля; поддерживается инструментом рабочего цикла
- **Разделение обязанностей** (для бизнеса и ИТ)
  - Разделение между средствами и методами разработки и производства; например, у разработчиков не должно быть обновленного доступа к средствам и методам производства
  - Все изменения в производственном приложении должны быть документально оформлены и одобрены; лицо, которое инициировало изменения, должно быть отличным от того, кто утвердил изменения, и отличным от того, кто перенес изменения в производство
- **Доступ**
  - Доступ пользователя: на основании должностных обязанностей
  - Привилегированный доступ: четкая авторизация, сильная аутентификация;
  - Правило наименьших привилегий – доступ, необходимый для выполнения работы

Управление инфраструктурными изменениями

- **Основные риски**: Несанкционированный доступ/изменения, Избыточный доступ, Мошенничество;
- **Документация** политики управления изменениями, Процессы и меры контроля; поддерживается инструментом рабочего цикла
- Использование основанного на рисках подхода к изменениям: от чрезвычайных до крупных изменений; требуются различные уровни документации и утверждений
- **Разделение обязанностей**: лицо, которое инициировало изменения, должно быть отличным от того, кто утвердил изменения, и отличным от того, кто перенес изменения в производство
- Обеспечить четкое обозначение ролей и обязанностей относительно того, кто может инициировать изменения, тестировать изменения, утверждать и переводить в производство
- Позаботиться о том, чтобы все свидетельства изменений были документированы, утверждены и хранились так, чтобы их можно было легко извлечь



Меры контроля информационной безопасности: доступ

- **Аутентификация и авторизация**: Как достигается доступ, и кто одобрен – новый пользователь и перевод
- **Привилегированный доступ:** системные администраторы
  - Позаботиться о том, чтобы права доступа уволенных сотрудников своевременно аннулировались
  - Индивидуальные счета в сравнении с сервисными – возможность отслеживания
- **Безопасность и целостность данных** – безопасная передача данных; шифрование данных при передаче (Протокол безопасных соединений/SSL и Безопасный протокол передачи гипертекста/HTTPS)



- **Брандмауэры сети и веб-приложений**: Журнал обзоров, ограничение доступа
- **Пароли для всех типов пользователей**: Сложные, принудительное изменение, блокирование счета
- **Физическая безопасность** в вашем центре данных – у кого имеется доступ к чему; это периодически утверждается и пересматривается?

Работа информационных систем/ планирование на случай чрезвычайных ситуаций

- **Основные риски**: сбой системы, потеря данных; неэффективные меры контроля в процессе
- **(Как минимум)** процессы резервного копирования и восстановления **документов**
  - Мониторинг сбоев и принятие соответствующих действий
  - Проведение периодических тестов на восстановление для обеспечения доступности данных с пленки/диска
  - Безопасное хранение, в отдельном месте
- Разработка ИТ политики восстановления после бедствий; тестирование ИТ плана на случай чрезвычайных ситуаций
- Документация процессов пакетных заданий
  - У кого имеется доступ для работы?
  - Знать сферу действия, влияние и частоту задний
  - Предпринять действия по невыполненным заданиям

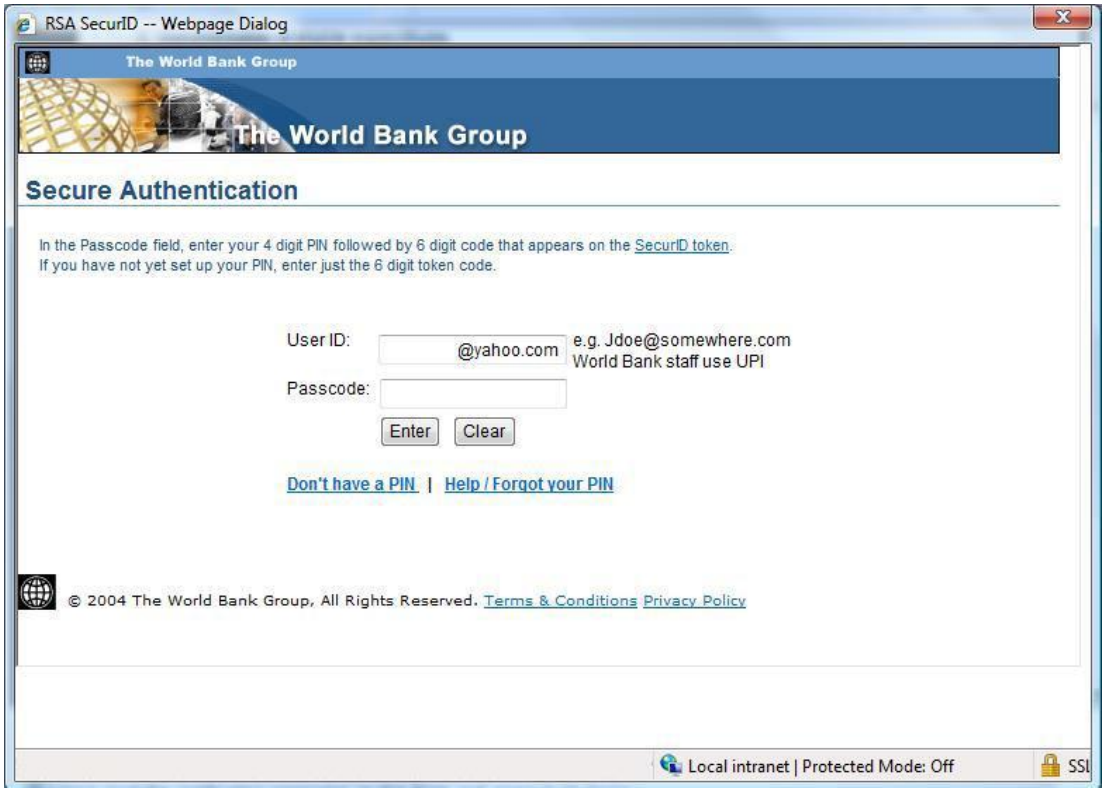
Пример Всемирного банка: Client Connection

- Client Connection – это безопасный веб портал, позволяющий заемщикам/получателям и донорам получать доступ к информации, связанной с займами, кредитами, грантами и трастовыми фондами
- Сквозная обработка транзакций (STP) – это новейшая фаза проекта eDisbursement (электронные выплаты) – клиенты банка могут подавать он-лайн запросы о выплатах и подписываться электронным образом
- Авторизованные подписанты и бенефициары должны быть одобрены и заранее зарегистрированы
- Должны быть в наличии отдельные профили, такие как Создатель форм (Form Creator) и Сторона, подписывающая формы (Form Signatory)
- У различных профилей – различные уровни доступа или различные виды транзакций, которые они могут выполнять
- Доступ предоставляется по действительному id пользователя и коду-паролю, который включает pin и динамичный маркерный код

http://clientconnection.worldbank.org

Использование двухфакторной аутентификации…

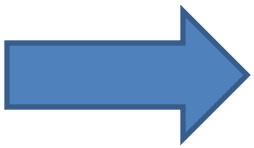
- id пользователя
- 8-значный PIN
- Динамичный 6-значный маркерный код



Пример электронной формы (eForm)

Активирован STP, предстоит поставить подпись…

Подписание формы …



B. Payment instructions

6a. Application currency	6b. Application amount	6c. Equivalent payment currency (if different from application currency)
United States Dollars	5,750,125.79	

6d. Application amount (in words)
United States Dollars FIVE MILLION SEVEN HUNDRED FIFTY THOUSAND ONE HUNDRED TWENTY-FIVE And 79

7. If the application covers more than one loan (as specified in item 2 above), please provide amounts allocated to each financier.

Loan/Financing/Grant No.(s)	Amount	Loan/Financing/Grant No.(s)	Amount
Loan/Financing/Grant No.(s)	Amount	Loan/Financing/Grant No.(s)	Amount

8. Name and address of beneficiary	9. Amount to be paid in installments?	
NATL HIVAIDS CONTROL PROJ III 1234 ANYWHERE IN NEW DELHI	No (if yes, complete "Requested Schedule for Advance Payments" Form 2381)	
10a. Name and address of the beneficiary's bank	10b. Account number (or IBAN for euro payments) of the beneficiary at the beneficiary's bank	10c. SWIFT code of the beneficiary's bank
BANK OF BARODA MADHUBAN: NEW DELHI	CHARITO ACC 123	BARBINBBNND
11a. Name and address of the intermediary bank	11b. Account number (or IBAN for euro payments) of the beneficiary's bank at the intermediary bank	11c. SWIFT code of the intermediary bank
FEDERAL RESERVE BANK OF NEW YORK FLOOR 7: NEW YORK		FRNYUS33XXX
12. Special payment instructions(if any)		

The supporting documentation contains 1 electronic document(s).

1 more signature(s) still needed(to access the eSignatories tab, click here)

☑ I have read the certification appearing on this form and agree to its terms.

Sign **Reject** **Cancel**

Supporting Documents

Documentation Type/Name	Size	Attached By
Statement of Expenditure STP Statement of Expenditures.xls	16KB	STP Create User3 26-OCT-2010 06:02 PM EST

Методы превентивного контроля и контроля обнаружения

- Разделение обязанностей: оперативный и привилегированный доступ
- Двухфакторная или многофакторная аутентификация
- Периодический обзор ролей и доступа на всех уровнях, от доступа к сети до доступа к приложению
  - Осуществляется минимум раз в полгода; документируется обзор и предпринятые действия
- Непрерывный мониторинг контроля – автоматический и ручной
  - Мониторинг доступа к системам – множественные неудачные запросы о регистрации и несанкционированный доступ
  - Мониторинг изменений от источника (приложение/база данных/операционная система) и сравнение с изменениями, внесенными в системы отслеживания ошибок
  - Мониторинг работы брандмауэра
- Зашифрованные данные при перемещении
- Учитывайте брандмауэр приложения

Выгоды аудита

- Аудиторские проверки могут дать достаточную уверенность в том, что подготовка финансовой отчетности поддерживается достаточным и устойчивым соблюдением мер внутреннего контроля
- Аудиторские проверки могут вскрыть недостатки в процессах информационной системы, которые после исправления укрепят средства и методы контроля и целостность системы
- Рассматривайте аудит, как возможность для улучшения процессов и контроля, рационализации контроля и заверения в том, что работа ведется эффективно и действенно
- Рассматривайте аудиторов как  стратегических партнеров!

Вопросы и комментарии?

Спасибо!