Внедрение СУИБ в соответствии с требованиями ISO/IEC 27001:2005 в международном банке

Перминов Владимир Сергеевич
CISM
Начальник отдела консалтинга и поддержки продаж ЗАО «РНТ»

Магнитогорск, 2011 г.

Внедрение СУИБ в международном банке

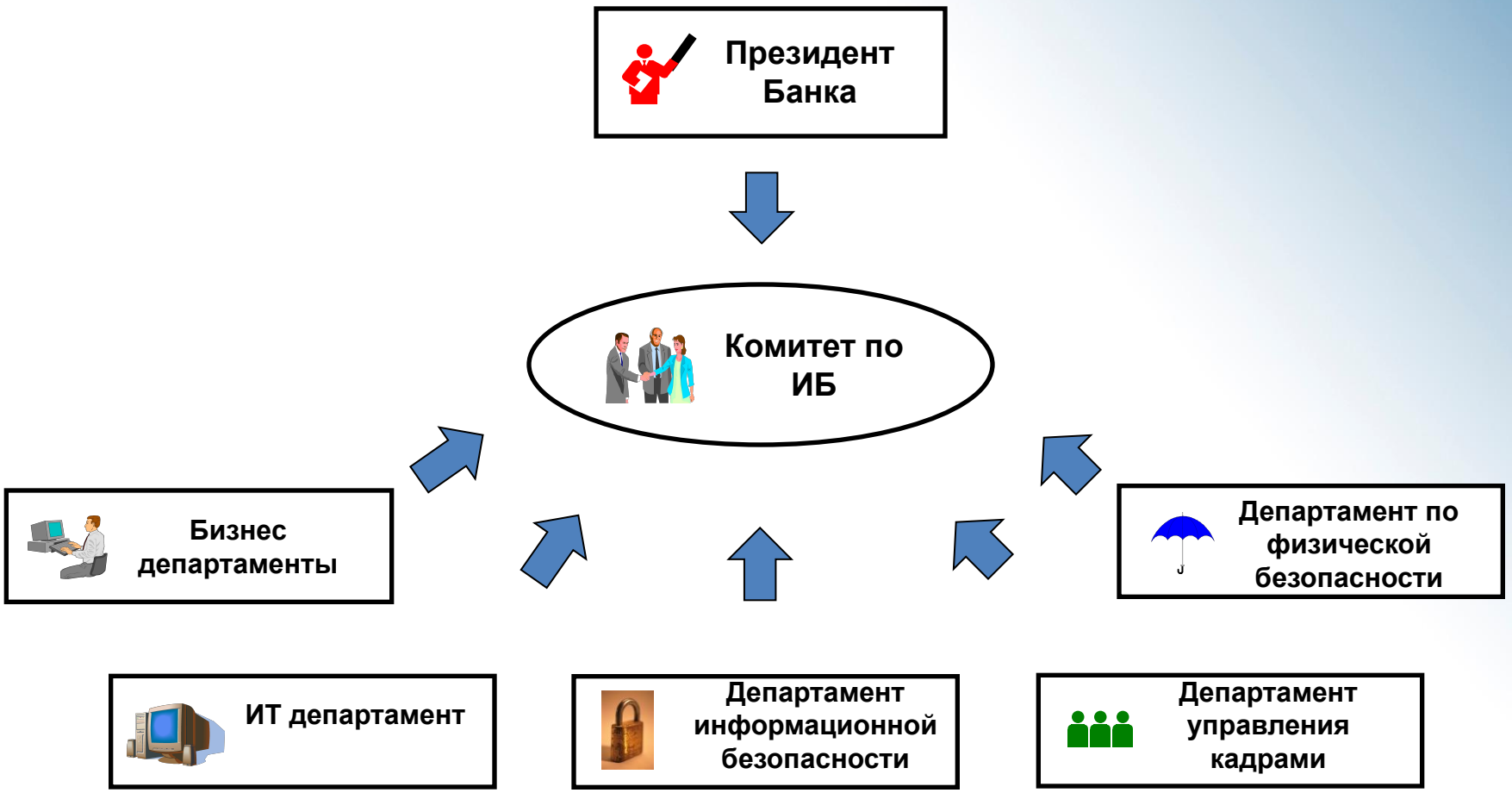
- Информация о банке
- Комитет по ИБ
- Этапы проекта
- Область деятельности СУИБ
- Сертификационный аудит

Информация о банке

- Крупный ритэйл банк в Азии
- 4 региональных офиса
- 125 дополнительных офисов
- 5000 сотрудников

Комитет по ИБ

Комитет по ИБ



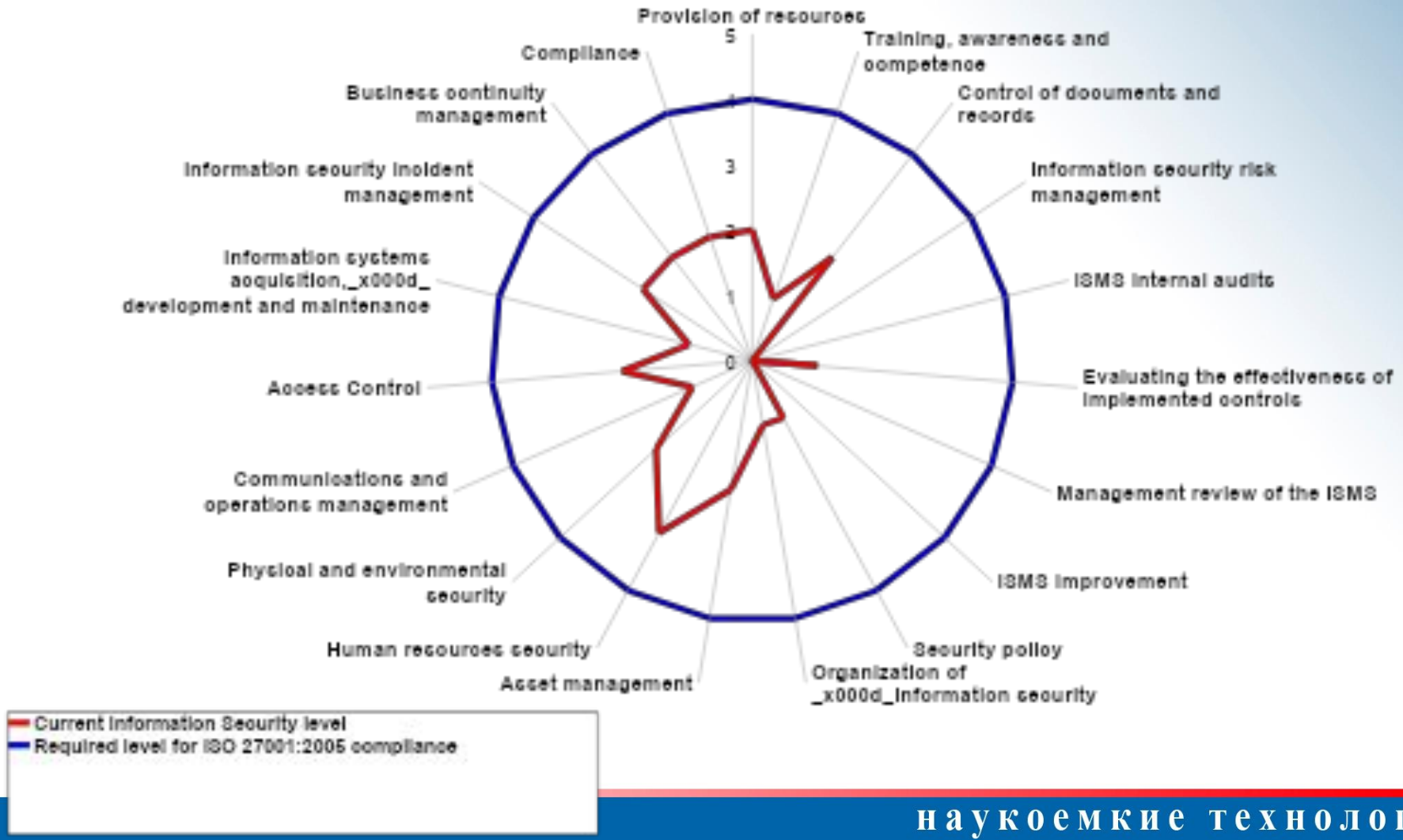
Этапы проекта

- Оценка текущего соответствия требованиям ISO/IEC 27001:2005
- Внедрение СУИБ
  - Выбор Области деятельности
  - Разработка ОРД
  - Оценка рисков
  - Внедрение процессов
- Сертификационный аудит

Оценка текущего соответствия требованиям ISO/IEC 27001:2005

- Документация по ИБ
- Основные системы
  - АБС
  - Система выпуска пластиковых карт
  - Терадата
  - Система хранения данных
- Локальная вычислительная сеть
  - Анализ конфигураций
  - Анализ уязвимостей

Результаты оценки соответствия требованиям ISO/IEC 27001:2005



Выбор Области деятельности

- Процессы
  - Обслуживание счетов клиентов
  - Формирование финансовой отчетности
  - Торговля на валютной бирже (Forex)
  - Выпуск пластиковых кредитных карт
  - Поддерживающие ИТ-процессы
- 13 дополнительных офисов
- 35 систем
- 250 сотрудников

Разработка ОРД

Уровень 1
Политики ИБ
Область деятельности СУИБ
Описание бизнес процессов
Положение о применимости контролей
Роли и ответственность по ИБ

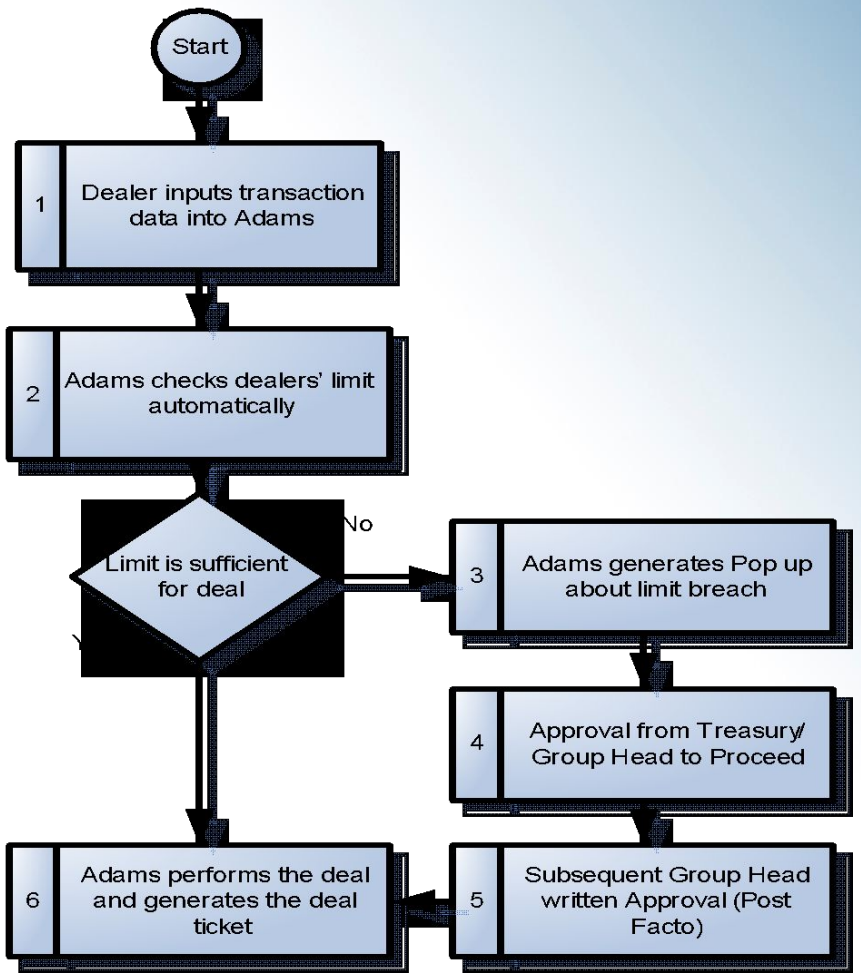
Уровень 2
Процедуры по информационной безопасности, необходимые для соответствия требованиям ISO/IEC 27001:2005

Уровень 3
Внешние нормативные документы

Уровень 4
Записи. Положения о подразделениях. Должностные инструкции. Рабочие инструкции. Приказы по ИБ. Протоколы решений по результатам Комитета по ИБ. Отчеты, предусмотренные процедурами ИБ.

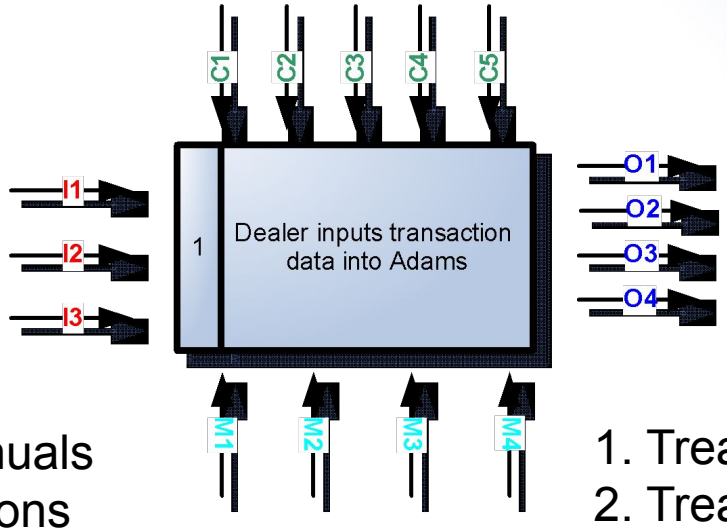
Описание бизнес процессов в области деятельности СУИБ

- Высокоуровневое описание процессов



Описание бизнес процессов в области деятельности СУИБ

- Детальное описание каждой активности



I1 – Deals Input

O1 – Command for Adams for Limit checks

C1 – Limits
C3 – Bank's Policy & Manuals
C4 – State Bank Regulations

Documents
1. Treasury & Investment Policies
2. Treasury Manual
3. Adams Manual
4. Deal Ticket Format

M1 – Reuter's Dealing System
M2 – Brokerage
M3 – Telephone/email
M4 – Dealers

Assets
1. Five PCs
2. One Printer
3. Deal Tickets office copy
4. Five Dealers

Оценка рисков

- Шкала оценки ценности (ущерба)

Оценка ценности (ущерба) актива	Финансовые потери	Потеря репутации	Несоответствие требованиям регуляторов
1	50 000	10	Предупреждение о несоответствии
2	250 000	15	Официальный запрос
3	500 000	150	Внеплановая проверка
4	750 000	250	Принудительные санкции
5	> 750 000	> 250	Отзыв лицензии

Оценка рисков

- Идентификация и классификация

N п/п	Актив	Владелец	Расположение	Тип актива	Оценка ценности
1	Customer account details & data	Manager Operations	Unibank Server at Computer Room	Soft Copy	5
2	Cheque/ Instruments	Manager Operations	Store Room at Branch	Hard Copy	4
3	Deposit Slip (Pay in Slip)	Manager Operations	Store Room at Branch	Hard Copy	4
4	Clearing Schedule	Manager Operations	Store Room at Branch	Hard Copy	2

Оценка рисков

Asset	Threats	Vulnera-bilities	Potential Impact	Existing Counter-measures	Likeli-hood	Analysis	Consequences				Impact level	Risk level	Risk Strategy
							Financial Loss	Loss of Reputation	Recovery Cost	Non - compliance with regulations			
A1	T1	V1											
	T2	V1											
		V2											
	T3	V1											
A2	Ti	V1											
		V2											
		…											
		Vn											
An	Tn	V1											
		V2											
		…											

Оценка рисков

Вероятность

very high	medium risk	high risk	high risk	very high risk	very high risk
high	low risk	medium risk	high risk	high risk	very high risk
medium	low risk	low risk	medium risk	high risk	high risk
low	very low risk	low risk	low risk	medium risk	high risk
very low	very low risk	very low risk	low risk	low risk	medium risk
	very low	low	medium	high	very high

Ущерб

План обработки рисков

Assets	threats	vulnerabilities	Risk Level	Acceptable Risk Level	Required Countermeasures	Linked Controls from Annex A(ISO 27001)	Description of control(Annex A)	Deadline of implementation	Responsible Person	Educed Risk Level
Building (Saima Trade Centre Branch, I.I. Chundriger Road, Karachi)	Fire (FIRE)	Non fire-fighting organization (description of roles and responsibilities)	Very High (Level 5)	Level 4 (high)	Employees should be given proper fire fighting trainings/drills on the bank level and responsibilities are assigned	9.1.4	Physical protection against damage from fire, flood, earthquake, explosions, civil unrest and other forms of natural or man-made disaster shall be designed and applied			
Unibank main Server	Tampering with software (IDS)	The operating system can be booted from any peripheral (e.g. floppy disc, CDROM)	Very High (Level 5)	Level 4 (high)	All external booting devices should be disabled	11.5.4	Use of utilities			
Unibank (Core banking software)	Forging of rights(FGR)	The password base of the operating system is decipherable (not encrypted)	Very High (Level 5)	Level 4 (high)	Password base should be made deciphered to ensure non-repudiation	11.5.3	Password management system			

Внедрение процессов

- Аудит ИБ
- Корректирующие и предупреждающие действия
- Управление инцидентами ИБ
- Обучение и повышение осведомленности по ИБ
- Анализ эффективности процессов по установленным метрикам
- Анализ СУИБ со стороны руководства

Сертификационный аудит

- Предсертификационный аудит
- Сертификационный аудит
  - Аудит документации
  - Аудит внедрения СУИБ

СПАСИБО ЗА ВНИМАНИЕ