

Software Engineering Forum



Внедрение СУИБ, соответствующей ИСО 27001, в ИТ компании

Алексей Евменков. Tieto

План презентации

- Введение
- Теория
- Практика
- Заключение

Введение

Термины и определения

- ИБ = Информационная Безопасность (information security):
 - свойство информации сохранять **конфиденциальность, целостность и доступность**. [Источник: ГОСТ Р ИСО/МЭК 27001:2006]
- СУИБ = Система Управления Информационной Безопасностью:
 - **часть** общей системы менеджмента,
 - основанная на использовании методов оценки **бизнес-рисков**
 - для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения **информационной безопасности**. [Источник: ГОСТ Р ИСО/МЭК 27001:2006]
- Альтернативное определение СУИБ:
 - Система, основанная на управлении **бизнес-рисками**
 - Для защиты **активов** (assets) выбираются и внедряются **соответствующие защитные меры** (security controls)

Зачем необходима СУИБ?

- Бизнес-риски срабатывают, а Вы о них даже не подозревали?
- Ваши партнеры не считают Вас вполне надежными?
- Ваша внутренняя информация не всегда под контролем?
- Ваши процессы не совсем зрелые в области ИБ?
- Вы более пассивны чем проактивны в области ИБ?

- У Вас воруют ноутбуки? ☺

Пора внедрять СУИБ !

Преимущества сертифицированной СУИБ

- Стандарт содержит разумную, выверенную последовательность действий, которую всегда можно подправить под собственные нужды
- Один раз сертифицирован, признан везде!
- Ежегодное подтверждение сертификата поддерживает тонус

Основная причина сертификации СУИБ

- Заказчик требует\повышение конкурентоспособности

Сколько ИСО 27001 сертификатов в мире?

Number of Certificates Per Country

Japan	2999*	France	12	Oman	1
India	441	Iceland	12	Peru	1
UK	395	Pakistan	12	Portugal	1
USA	88	Slovenia	9	Kazakhstan	1
Czech Republic	71	Sweden	9	Morocco	1
Hungary	64	Slovakia	6	Ukraine	1
Italy	59	South Africa	6	Argentina	1
Poland	39	Switzerland	6	Armenia	1
Spain	35	Bahrain	5	Belgium	1
Hong Kong	31	Colombia	5	Kyrgyzstan	1
Austria	30	Croatia	5	Lebanon	1
Australia	29	Indonesia	5	Lithuania	1
Ireland	29	Kuwait	5	Luxembourg	1
Malaysia	26	Bulgaria	4	Macedonia	1
Brazil	21	Gibraltar	4	Belarus	1
Thailand	21	Norway	4	Mauritius	1
Mexico	20	Qatar	4	Moldova	1
UAE	18	Sri Lanka	4	New Zealand	1
Turkey	18	Chile	3	Uruguay	1
Greece	15	Egypt	3	Yemen	1
Romania	15	Iran	3	Relative Total	5333
Netherlands	13	Macau	3	Absolute Total	5314

Macedonia

1

Belarus

1

Uruguay

1

Теория

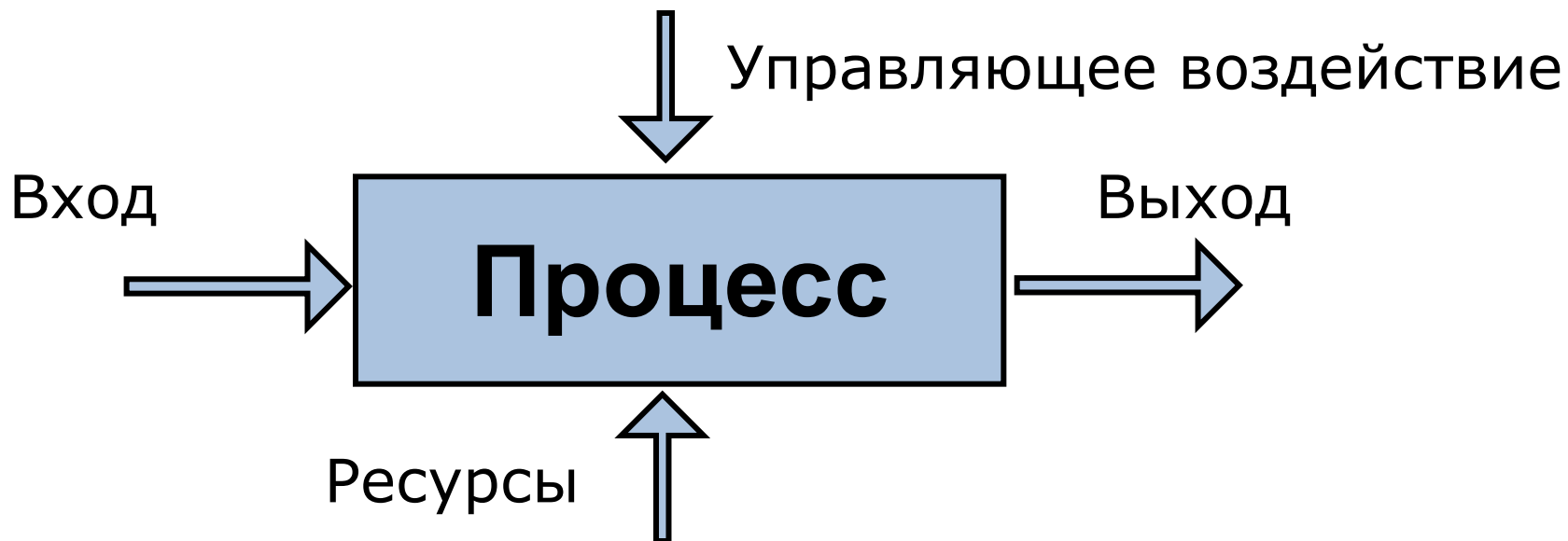
Семейство стандартов ИСО 27000

Terminology	<p>Legend: Under development Published</p>		
	ISO/IEC 27000:2009(?) ISMS fundamentals and vocabulary		
Requirements	ISO/IEC 27001:2005 ISMS requirements		ISO/IEC 27006:2007 Requirements for the accreditation of bodies providing certification of ISMS
	ISO/IEC 27002:2005 Code of practice for information security management		ISO/IEC 27003:2009(?) ISMS implementation Guide
Guidance	ISO/IEC 27005:2008 Risk management		ISO/IEC 27004:2009(?) Measurement and metrics
	ISO/IEC 27007:2010 (?) ISMS Auditor Guidelines		

Принципы ИСО 27001

- Процессный подход
- Цикл PDCA (Plan-Do-Check-Act)

Процесный подход



Процессный подход (пример)

Вход:

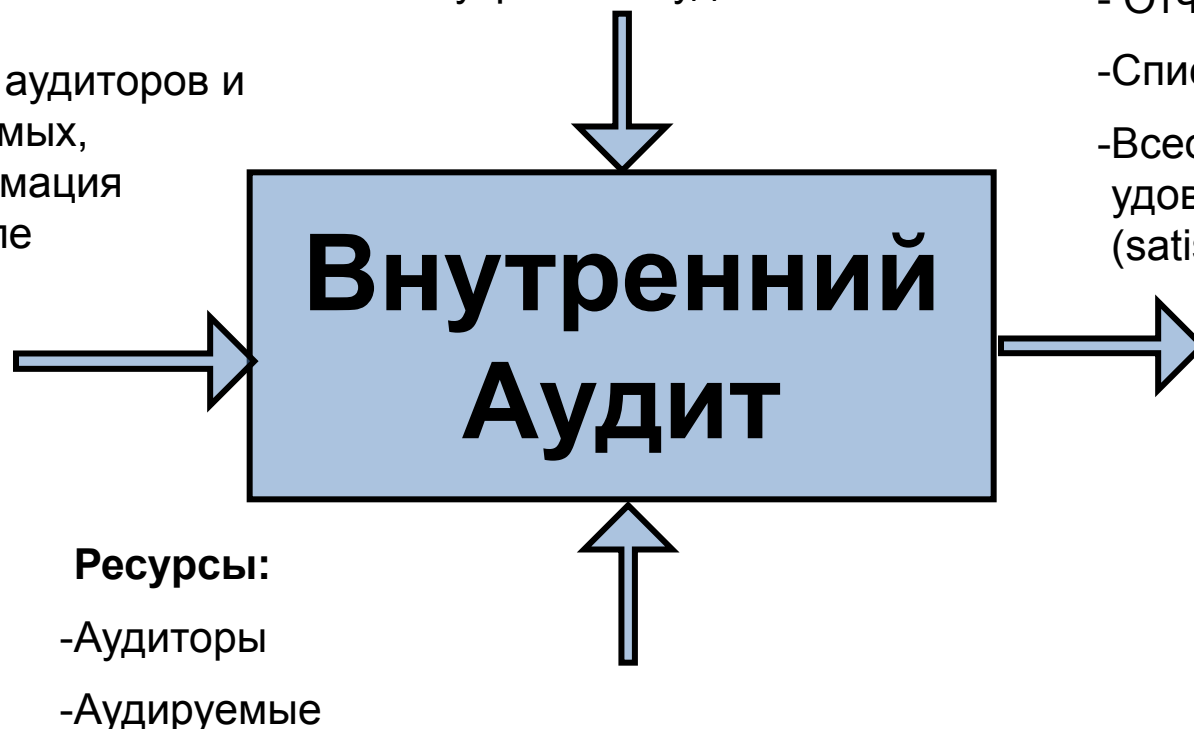
- Название отдела,
- План,
- Имена аудиторов и аудируемых,
- Информация об отделе

Управление: процедура

«Внутренний аудит»

Выход:

- Отчет по аудиту
- Список несоответствий
- Всеобщее удовлетворение (satisfaction) ☺



Ресурсы:

- Аудиторы
- Аудируемые

Цикл PDCA (пример)

Планирование Аудитов

Plan

Устранение несоответствий,
планирование превентивных
действий

Action

Осуществление
аудитов

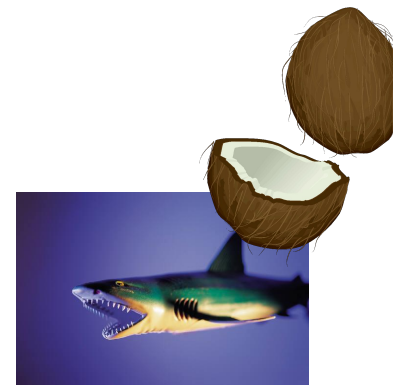
Do

Check

Проверка на соответствие
требованиям ИБ

Риски – центральная тема СУИБ

- Мало кто знает, что ...
- За год от падения кокосов погибает в десятки раз больше людей, чем от акул
 - Часто мы боимся не то, что нужно
- Мужчины поражаемы молнией в 4 раза более часто чем женщины
 - В жизни бывают странные закономерности
- Шанс выиграть в лотерею обычно ~1 из 14млн.
Шанс заболеть птичьим гриппом 1 из 100млн.
 - Наши ожидания и страхи зачастую иррациональны, пока не проанализируешь их



Риски – центральная тема СУИБ

- Риски необходимо **учитывать**
- **Разные** риски должны обрабатываться «по-разному»

- СУИБ предоставляет набор инструментов по управлению рисками

Управление рисками в СУИБ

- **Угроза** - причина нежелательного инцидента, который может привести к негативным последствиям для организации .
- **Уязвимость** – недостаток информационного ресурса или группы ресурсов, который способствует реализации угрозы.
- **Риск** - комбинация вероятности срабатывания угрозы через уязвимость, с последующим уроном для активов организации
- **Защитная мера** – действия по минимизации риска

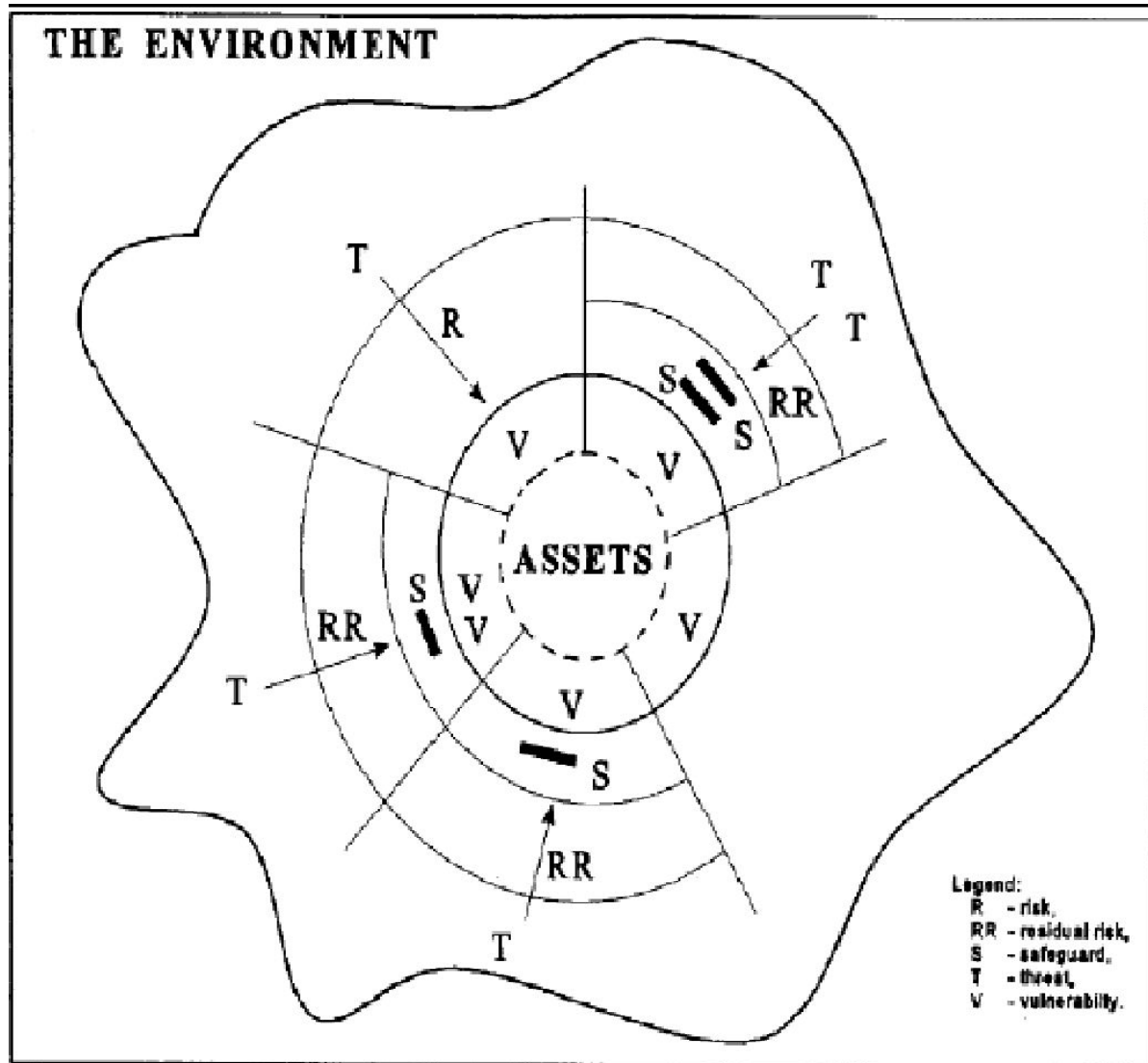
Некто может пробраться в офис и украсть лаптоп

- Нет системы доступа в офис
- Отсутствуют кабели-замки для компьютеров

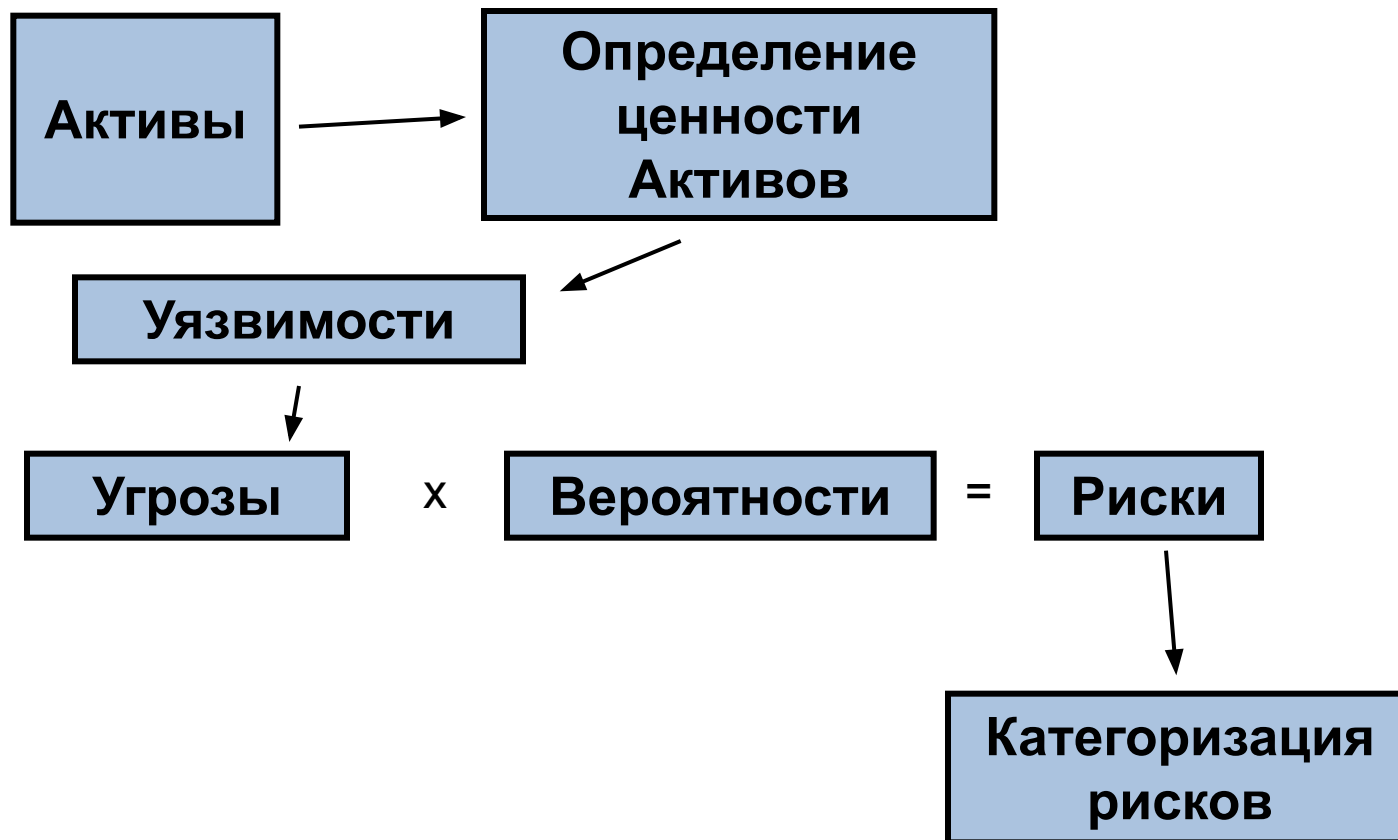
Некто проникнет в офис и украдет компьютер по причине отсутствия кабеля-замка

Внедрить в практику использование специальных кабелей-замков для всех портативных компьютеров

Управление рисками в СУИБ



Процесс оценки рисков



Список защитных мер (ИСО 27002)

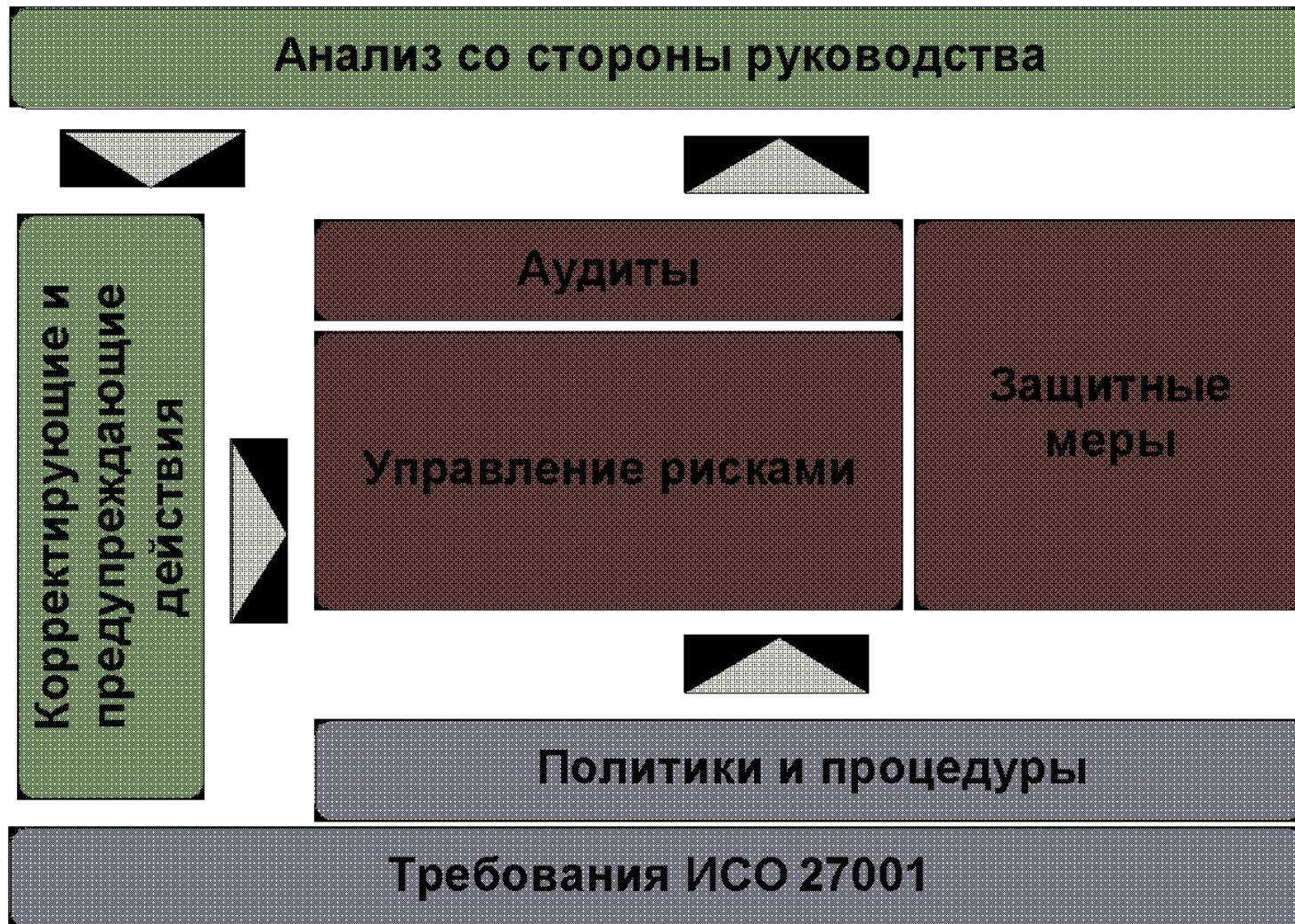


Практика

Вызовы при создании СУИБ

- Необходимость в установлении специфических процессов
 - Например, измерение эффективности защитных мер, аудиты по безопасности
- Создание комплекта документации
 - Шаблоны, практики, собственно сам документооборот
- Необходимость в автоматизация процессов
 - Например, управление рисков очень трудоемко без автоматизации
- Организационные аспекты
 - Ответственные за политики, тренинг персонала, как получить «вовлеченность менеджмента» (management commitment)
- Сложный процесс сертификации

Схема функционирования СУИБ



Пример определения угроз и уязвимостей

- Фильтрация по доступным активам
- Определение списка угроз для выделенного актива
- Определение уязвимостей, посредством которых данная угроза может реализоваться

Threats and Vulnerabilities : Form

Filter Settings

Asset Name:	Asset Category:	Asset Type:	Asset Owner:
ADSL modem	ICT	Access control system	Customer
All office equipment	Operations	Administrative systems	Employee
All office infrastructure	Processes and procedures	Backup media	ICT Manager
All office laptops	Projects	Business continuity plan and	Management
All office printers	Servers	Customer equipment	P&N
All office scanners (and all-in-one devices)		E-mail & instant messaging	Project manager
All office workstations		Employees	Site manager
Backup HDD		Employees' personal data	
BCP and recovery procedures		Image and reputation	

Reset Filter

Asset Attributes (for selected asset)

Name: All office printers	Asset Owner: ICT Manager
Category: ICT	Asset Value: 1,67
Type: Scanners/ printers	

Threats

Power supply or air conditioning failure	
Threat of printout	

Threat for selected Asset

Vulnerabilities

Not following by right procedures	
Access rights leak	

List of Vulnerabilities for selected Threat

Пример оценки рисков

Risk Treatment : Form

Filter Settings

Asset Name:	Asset Category:	Asset Type:	Asset Owner:
ADSL modem All office equipment All office infrastructure All office laptops All office printers All office scanners (and all-in-one devices) All office workstations	ICT Operations Processes and procedures Projects Servers	Access control system Administrative systems Backup media Business continuity plan and Customer equipment E-mail & instant messaging Employees	Customer Employee ICT Manager Management P&N Project manager Site manager

Reset Filter Risk Rank: 1 (0-12) / Low
2 (13-32) / Medium
3 (33-64) / High

Risk Assessment

↓

Risk Treatment

↓

Control Implementation

Asset Attributes (for selected asset)

Name: All office printers	Asset Owner: ICT Manager
Category: ICT	Asset Value: 1,67
Type: Scanners/ printers	

Risk Attributes (for selected risk)

ID	ThreatName	VulnerabilityName
93	Power supply or air conditioning failure	No maintenance in place
92	Power supply or air conditioning failure	Not enough knowledge or handling trainings
90	Power supply or air conditioning failure	Not following by right procedures
95	Theft of printout	Access rights leak

Risk Assessment attributes and Treatment strategy

Impact Category: Financial losses	Risk exposure range (E=AV*L*T): 10,02	<input checked="" type="checkbox"/> Risk Confidentiality
Impact: Medium (Significant)	Risk Rank: 1 / Low	<input checked="" type="checkbox"/> Risk Integrity
Likelihood: High (once a month is possible)		<input type="checkbox"/> Risk Availability

Risk Treatment

Treatment Option: Apply Control	Residual Impact: Low (Negligible)	Risk Exposure Range: 1,67
Reason for decision: Management Decision	Residual Likelihood: Low (Occurrence of event is almost improbable)	Residual Risk Rank: 1 / Low
	Reason for risk reduction: Set of controls' actions are applied.	

All Controls	Applied controls
5.1.1 Information security policy document 5.1.2 Review of the information security policy 6.1.1 Management commitment to information security	11.1.1 Access control policy 11.2.2 Privilege management

Отчеты

- Стандарт требует некоторые обязательные отчеты
 - Например план по обработке рисков (Risk Treatment Plan)
 - Положение о применимости (Statement of Applicability)
- Важно динамическая генерация отчетов
- Доступ к любой информации в базе

Risk Treatment Plan

tiebo.com

Software centres
Belarus Software Centre

2009-02-11

Risk Treatment Approach: Apply Control

Risk Name: 306. Employee errors and wrong actions / Not enough knowledge or trainings

Asset Details

Name Top management	Owner Site manager
Category Operations	Asset Value 2
Type Employees	

Risk Details

Likelihood High (once a month is possible)	<input checked="" type="checkbox"/> Risk Confidentiality
Impact Medium (Significant)	<input type="checkbox"/> Risk Integrity
Impact	<input type="checkbox"/> Risk Availability
Risk Exposure Range 12	
Risk Rank 1 / Low	

Risk Treatment

Treatment Approach Apply Control
Decision Reason

Residual Exposure 2
Residual Risk Rank 1 / Low
Decision Reason

Control Name 10.7.3 Information handling procedures	
Status Implemented	
Deadline 2008-09-30	Reason for Implementation
Responsible Evmenkov Alexey	Reduce Risk

Comments

Done. Named SEC80170 By:SC Information exchange policy

Action Plan

ISMS Portal

- Необходимо создать «единую точку входа» для всех сотрудников организации
- Автоматизированный документооборот (версионность, workflows)

ISMS Portal - реализация

ByDC Welcome Evmenkov Alexey

ISMS This Site

ByDC Home **ISMS** PQ ICT HR Visits Site Action

View All Site Content

Documents

- Processes and Procedures
- ISMS Templates
- Presentations
- Management Materials
- External Security Audits

Records

- Risk Treatment
- ISMS Audits
- Trainings

Incident Management

- By Status
- By Importance

ISMS Audits

- All Audits
- Planned Audits

Improvement Actions

- All Improvement Actions
- My Improvement Actions

Surveys and Examinations (In Progress)

- Exam:Key Control Policy in BySC
- Exam:Clear desk and clear screen policy in BySC
- Exam:Information Security Management System in BySC

ByDC > ISMS

ByGDC Information Security Management System

ByGDC Policy

Protection of company assets as well as protection of customer data is vital to the success of our business. To this end, we have established an **information security management system** that operates all the processes required to identify the information we need to protect and how we must protect it.

Because the needs of our business change, we recognize that our ISMS must be **continually changed and improved to meet our needs**. To this effect, we are continually setting new objectives and regularly reviewing our processes.

Company assets and customer data protection is **general responsibility of ByGDC management**.

Every ByGDC's employee has a personal responsibility for following all the policies and procedures in scope of ISMS.

ISMS Audits

Audit ID	Audit Name	Audit Status	Audit Date (planned)	Audit Date (actual)	Lead Auditor	Lead of Auditees	# of issues	# of BP
							Sum = 38	Sum = 3
Audited Department : Administration (1)								
							Sum = 9	Sum = 1
Administration_2008-10-30	ISMS Internal Audit	Done	30/10/2008	30/10/2008 14:00	Khvalov Valery	Prudnikov Alexander	9	1
Audited Department : HR (1)								
Audited Department : PN&BI (2)								
Audited Department : Reception (1)								
Audited Department : TM (1)								
							Sum = 5	Sum = 1
TM_2008-10-29	ISMS Internal Audit	Done	29/10/2008	29/10/2008 15:00	Khvalov Valery	Naskevich Oleg	5	1
Add new item								

Links

- BySC ISMS Policy
- STANDARDS: ISO/IEC 27001:2005 and ISO/IEC 27002:2005
- TE Classification Policy
- Add new link

Announcements

New version of RTS is coming soon! NEW 11/02/2009 17:40
by Evmenkov Alexey

Complete refactoring of RTS software was conducted.
Next plans:
- new wizard-looking interface
- new functionality (according to Security Team requests)

Please contact Valery Khvalov or Alexey Evmenkov for more details.

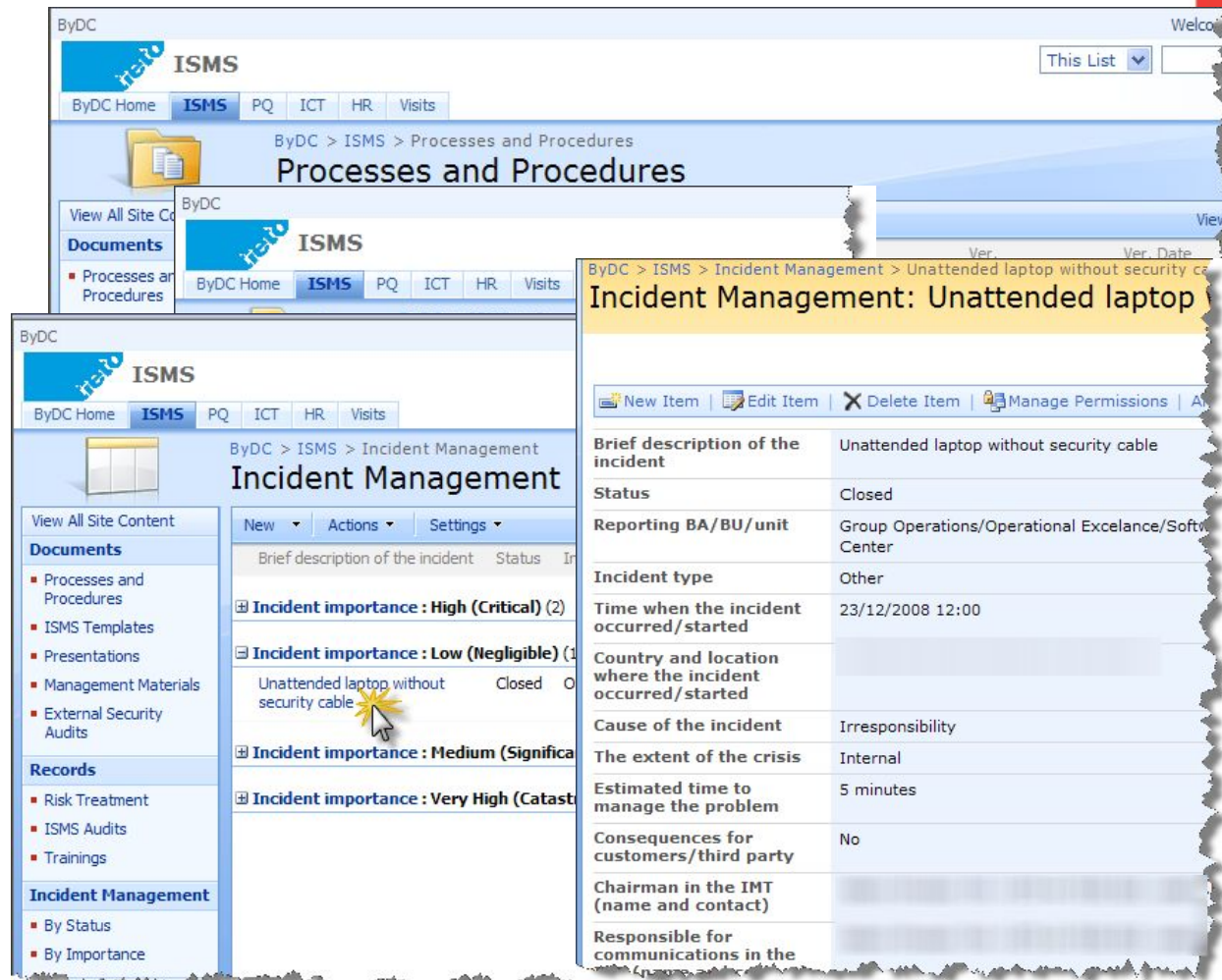
Security audit by IF has been successfully passed! NEW 04/12/2008 15:40
by Evmenkov Alexey

Our customers IF were conducted an audit on Dec 3rd.

We present them our ISMS, they were impressed!

ISMS Portal - примеры

- Документация
- Записи
 - Тренинги
 - Метрики
 - Аудиты
 - И т.д.
- Управление инцидентами



The screenshot displays the ISMS Portal interface with the following components:

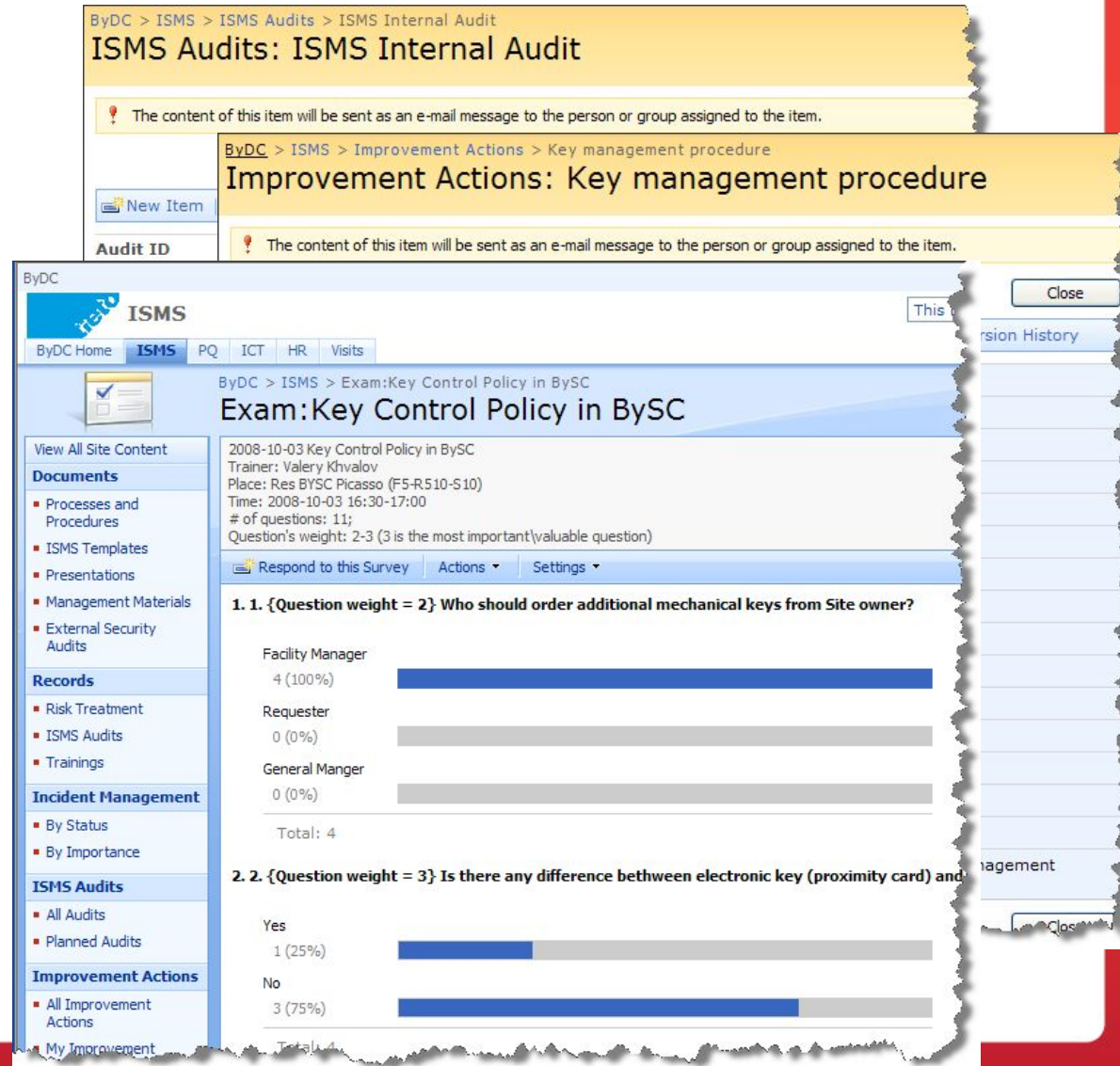
- Navigation:** ByDC Home, ISMS, PQ, ICT, HR, Visits.
- Processes and Procedures:** A breadcrumb trail shows 'ByDC > ISMS > Processes and Procedures'. A 'Documents' sidebar lists 'Processes and Procedures'.
- Incident Management:** A breadcrumb trail shows 'ByDC > ISMS > Incident Management'. A table lists incidents with columns for 'Brief description of the incident', 'Status', and 'Incident importance'. A mouse cursor points to an incident titled 'Unattended laptop without security cable'.
- Incident Details:** A detailed view for the selected incident, titled 'Incident Management: Unattended laptop', showing fields such as 'Brief description of the incident', 'Status', 'Reporting BA/BU/unit', 'Incident type', 'Time when the incident occurred/started', 'Country and location where the incident occurred/started', 'Cause of the incident', 'The extent of the crisis', 'Estimated time to manage the problem', 'Consequences for customers/third party', 'Chairman in the IMT (name and contact)', and 'Responsible for communications in the'.

ISMS Portal - примеры

- **Аудиты**
 - Записи об аудите
 - Несоответствия

- **Экзамены и оценка тренинга**

- **Линки, объявления, календари, задачи и многое другое.**



The screenshot displays the ISMS Portal interface with the following content:

ByDC > ISMS > ISMS Audits > ISMS Internal Audit
ISMS Audits: ISMS Internal Audit

The content of this item will be sent as an e-mail message to the person or group assigned to the item.

ByDC > ISMS > Improvement Actions > Key management procedure
Improvement Actions: Key management procedure

The content of this item will be sent as an e-mail message to the person or group assigned to the item.

ByDC
ISMS

ByDC Home ISMS PQ ICT HR Visits

ByDC > ISMS > Exam:Key Control Policy in BySC
Exam:Key Control Policy in BySC

2008-10-03 Key Control Policy in BySC
 Trainer: Valery Khvalov
 Place: Res BYSC Picasso (F5-R510-S10)
 Time: 2008-10-03 16:30-17:00
 # of questions: 11;
 Question's weight: 2-3 (3 is the most important\valuable question)

Respond to this Survey Actions Settings

1. 1. {Question weight = 2} Who should order additional mechanical keys from Site owner?

Facility Manager	4 (100%)
Requester	0 (0%)
General Manger	0 (0%)
Total:	4

2. 2. {Question weight = 3} Is there any difference between electronic key (proximity card) and

Yes	1 (25%)
No	3 (75%)
Total:	4

Inventory DB

- Детальное управление активами
- Оперативное отслеживание статуса активов
- Возможность настройки под любые типы активов

Inventory DB - реализация

ByDC > ICT

Inventory

Home **Inventory**

ICT > Inventory > Workstations

Workstations

This includes computers at the employees' workplaces

New Actions Settings

Inventory ID	Inventory name	Owner	Start Date	Serial number	Network name	Monitor	Status	Additional Information
<p>Status : Damaged (1)</p> <p>Status : In support (2)</p> <p>Status : In Use (67)</p>								
57	Dell Optiplex 745		1/8/2008			Dell 1908FPc	In Use	Monitor s/n: cn-0uw-logitech;
85	Dell Optiplex 745		4/14/2008			Dell 1908FPc	In Use	Monitor s/n: cn-0pm-logitech;
53	Dell Optiplex 745		1/8/2008			Dell 1908FPc	In Use	Monitor s/n: cn-0uw-logitech;
68	Dell Optiplex 745		3/3/2008			Dell 1908FPc	In Use	Monitor s/n: cn-0pm-logitech;
95	Dell Optiplex 745		10/6/2008			Dell 1908FPc	In Use	Monitor s/n: cn-0pm-logitech;
96	Dell Optiplex 745		12/29/2007			Dell 1908FPc	In Use	Monitor s/n: cn-0uw-logitech;

Assets DB

- Workstations
- Mobile computers
- Servers
- Network components
- Internet components
- Phone components
- Scanners and printers
- Backup media
- Software
- Customer equipment
- Office equipment
- Office infrastructure

Recycle Bin

Assets' categories

Assets workflow organized by statuses usage

Inventory DB - реализация

ByDC > ICT

Inventory

Home **Inventory**

ICT > Inventory > Backup media

Backup media

This includes any kind of media used for backup purposes (hard disks, CD/DVD, memory sticks, etc)

New Actions Settings

Inventory ID	Inventory name	Backup type	Owner	Serial number	Asset location	Status
F001	JetFlash V90	Flash drive		214434-0015		In Use
F002	JetFlash V90	Flash drive		211167-1808		In Use
F003	JetFlash V90					
F004	JetFlash V90					
F005	JetFlash V90					
F006	JetFlash V90					
F007	JetFlash V90					
F008	Kingston 2Gb					

View All Site Content

Assets DB

- Workstations
- Mobile computers
- Servers
- Network components
- Internet components
- Phone components
- Scanners and printers
- Backup media
- Software
- Customer equipment

ICT > Inventory > Backup media > JetFlash V90

Backup media: JetFlash V90

Close

New Item | Edit Item | Delete Item | Manage Permissions | Alert Me | Version History

Inventory ID	F005
Inventory name	JetFlash V90
Backup type	Flash drive
Owner	
Serial number	221408-0575
Asset location	
Status	In Use
Additional info	
Last Maintenance	

Version: 3.0
 Created at 10/8/2008 12:59 PM by
 Last modified at 12/11/2008 1:50 PM

Close

Заключение

ИБ и разработка ПО

- Целый раздел защитных мер стандарта посвящен «правильной разработке ПО»: «Разработка, внедрение и обслуживание информационных систем»
- В целом содержит здравые рекомендации по разработке
 - Например «проверка достоверности входных данных», «целостность сообщений»
- На практике все выливается в финансовые возможности Вашего заказчика
- Также важен профессионализм Ваших разработчиков
 - Правила хорошего программирования покрывают большинство требований стандарта

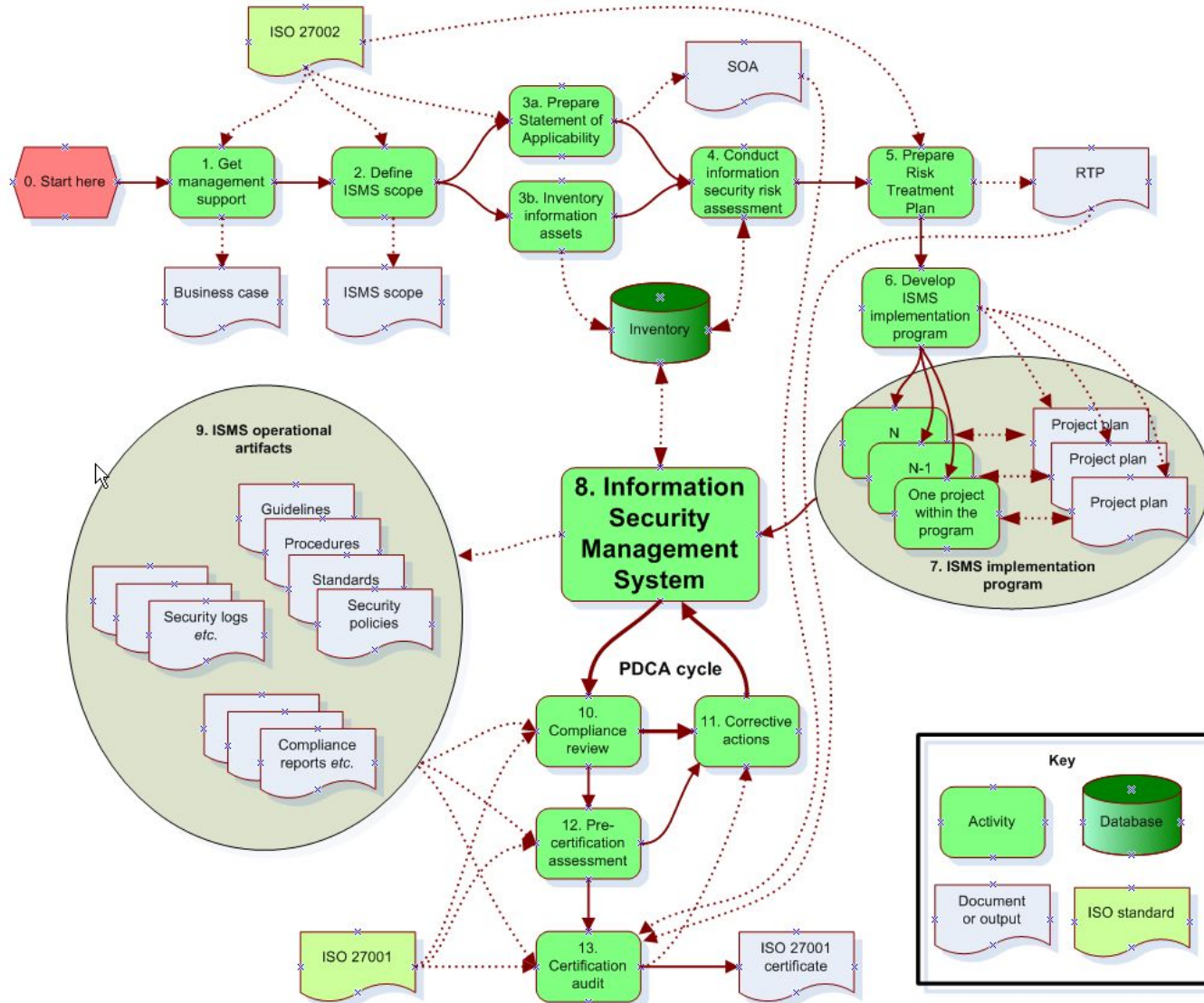
Процесс сертификации

- Тема для отдельного разговора (выбор сертифицирующего органа, общение с консалтерами, внутренняя организация)

Некоторые рекомендации:

- Требуется серьезного подхода, детального планирования, «вовлеченности руководства»
- При отсутствии собственных специалистов по безопасности, прошедших сертификацию – рекомендуется нанять организацию – консалтера
- Тренинги – основа работающей на практике СУИБ; также формально закрывает многие требования стандарта

Процесс сертификации



Вопросы и ответы

Спасибо за внимание!

Вопросы?