Как управлять аудитом информационной безопасности?

Дмитрий Никипелов
CISO
BAS Innovation

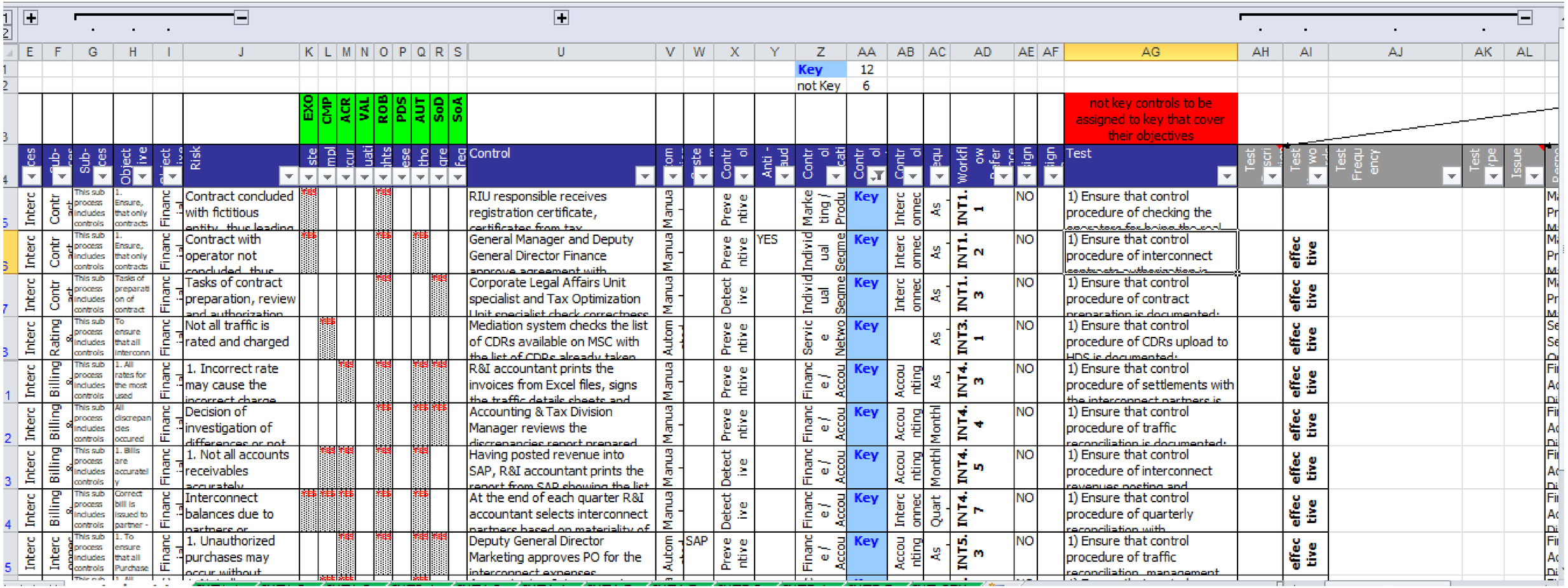
Цели и задачи аудита ИБ?

- Анализ рисков
- Оценка текущего уровня защищенности
- Локализация узких мест в системе защищенности
- Оценка соответствия системы защищенности существующим стандартам индустрии

Реестр рисков

2					
3	Risk drivers	Control block	Description	Control block owner	Controls
4	• Business requirements not understood or addressed by IT management • No regular and formal consultation between IT management and business and senior management • IT plans not aligned with business needs • Unnecessary IT initiatives and investments • IT plans inconsistent with the organisation's expectations or requirements • IT not focused on the right priorities	not implemented			
5	• Inadequate information for business functions • Inconsistency between information requirements and application developments • Data inconsistency between the organisation and systems • Inefficient planning of IT-enabled investment programmes due to lack of information • Accumulation of data that are not relevant, consistent or usable in an economical manner	not implemented			
6	• Inappropriate security requirements • Inadequate or excessive investments in security controls • Occurrence of privacy, data confidentiality, integrity and availability incidents • Non-compliance with regulatory or third-party requirements • Inefficient or inconsistent information for decision making	not implemented			
	• Improperly secured business data	not implemented			

Матрица ICM



	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL
1																					Key	12											
2																					not Key	6										
3							EXO	CMP	ACR	VAL	ROB	PDS	AUT	SoD	SoA													not key controls to be assigned to key that cover their objectives					
4	ces	Sub-ces	Sub-ces	Object ive	Object ive	Risk	ste	mpl	ccur	uati	hts	ese	tho	gre	req	Control	om	ste m	Contr ol	Anti - raud	Contr ol cati	Contr ol	Contr ol	equ	Workfl ow Refer re	lign	lign	Test	Test scri	Test wo	Test Frequ ency	Test ype	Issue	Respo
5	Interc	Contr act	This sub process includes controls	1. Ensure, that only contracts	Financ ial	Contract concluded with fictitious entity, thus leading										RIU responsible receives registration certificate,	Manua		Preve ntive		Marke ting / Produ	Key	Interc onnec	As	INT1. 1	NO		1) Ensure that control procedure of checking the						Ma Pr Ma
6	Interc	Contr act	This sub process includes controls	1. Ensure, that only contracts	Financ ial	Contract with operator not concluded, thus										General Manager and Deputy General Director Finance	Manua		Preve ntive	YES	Individ ual Segme	Key	Interc onnec	As	INT1. 2	NO		1) Ensure that control procedure of interconnect		effec tive				Ma Pr Ma
7	Interc	Contr act	This sub process includes controls	Tasks of preparati on of contract	Financ ial	Tasks of contract preparation, review and authorization										Corporate Legal Affairs Unit specialist and Tax Optimization	Manua		Detect ive		Individ ual Segme	Key	Interc onnec	As	INT1. 3	NO		1) Ensure that control procedure of contract		effec tive				Ma Pr Ma
8	Interc	Rating &	This sub process includes controls	To ensure that all Interconn	Financ ial	Not all traffic is rated and charged										Mediation system checks the list of CDRs available on MSC with	Autom		Preve ntive		Servic e Netwo	Key		As	INT3. 1	NO		1) Ensure that control procedure of CDRs upload to		effec tive				Se Se Di
1	Interc	Billing &	This sub process includes controls	1. All rates for the most used	Financ ial	1. Incorrect rate may cause the										R&I accountant prints the invoices from Excel files, signs	Manua		Preve ntive		Financ e / Accou	Key	Accou nting	As	INT4. 3	NO		1) Ensure that control procedure of settlements with		effec tive				Fi Ac Di
2	Interc	Billing &	This sub process includes controls	All discrepan cies occured	Financ ial	Decision of investigation of										Accounting & Tax Division Manager reviews the	Manua		Preve ntive		Financ e / Accou	Key	Accou nting	Monthl	INT4. 4	NO		1) Ensure that control procedure of traffic		effec tive				Fi Ac Di
3	Interc	Billing &	This sub process includes controls	1. Bills are accuratel y	Financ ial	1. Not all accounts receivables										Having posted revenue into SAP, R&I accountant prints the	Manua		Detect ive		Financ e / Accou	Key	Accou nting	Monthl	INT4. 5	NO		1) Ensure that control procedure of interconnect		effec tive				Fi Ac Di
4	Interc	Billing &	This sub process includes controls	Correct bill is issued to partner -	Financ ial	Interconnect balances due to										At the end of each quarter R&I accountant selects interconnect	Manua		Detect ive		Financ e / Accou	Key	Interc onnec	Quart	INT4. 7	NO		1) Ensure that control procedure of quarterly		effec tive				Fi Ac Di
5	Interc	Interc onnec	This sub process includes controls	1. To ensure that all Purchase	Financ ial	1. Unauthorized purchases may										Deputy General Director Marketing approves PO for the	Autom	SAP	Preve ntive		Financ e / Accou	Key	Accou nting	As	INT5. 3	NO		1) Ensure that control procedure of traffic		effec tive				Fi Ac Di

Пример описания контрольной метрики

Process Owner:	Roaming & Interconnection Unit/Roaming Expert, Roaming Specialist	**Tested by:**	fffffff
Test Date:	**09.07.2009**	**Signature:**	
Process Name:	**Roaming**		
Sub Process:	Partnership Management	**Reviewed by:**	fffffff
Workflow Reference	ROA1.1		
Objective:	To ensure, that relationships are established with proper operator, having good credentials and in favor of Astelit		
Assertion(s):	*Authorization, Rights and Obligations*		
Control:	**IBU specialist finds Roaming partner via GSM Infocentre (GSM Association) to ensure that relationships established only with legal entities, existing in GSM Association Directory, prepares draft of agreement and addendums using GSM association standard templates and paraphes it after negotiations.**		
Test Steps:	1) Ensure that control procedure of tracing the existence of operator via GSM Infocentre is documented; 2) Inquire control owner about the procedure of verification that new roaming partner is registered member of GSM association; 3) Select a sample of acting roaming agreements and obtain copies; 4) Inspect roaming agreements whether they are paraphed by responsible from Interoperator Business Unit; 5) Document test results		
Control frequency:	As needed		
Sample size:			
Testing period:	2009		
TEST PERFORMED:			
Testing period:	Q1 & Q2 of 2009		
	1) Tested that control procedure of tracing the existence of operator via GSM Infocentre is documented in International Roaming Workflow procedure;		
	SEE TEST OF CONTROL ROA1.2		
	CONCLUSION:		
09.07.2009	Based on test performed and **no exceptions** noted I find control to be **effective.**		

Реестр IT-систем

A	B	C	D	E	F	G	H	I
System group	System name	Description	Type OS/DB/App	Host name (IP)/ DB name/ app name	admin interface	soft version	unit	System owner
SCP	SCP	SCP	OS		ssh	HP-UX 11.23 U	Enterprise IT	Dmitry Nikipelov
			DB	internal		TimesTen 6.4		
AD	DC, DNS server; DHCP server	(Ctrl) ntroller; DNS server; DHCP server	OS	srv-adc-01 (10.10.10.200);	MMC Console	Windows 2003	Enterprise IT	Dmitry Nikipelov
ERP	Netsys	ERP System	OS	srv-erp-1 (10.10.0.32)	Netsys Admin Console	Windows 2003	Enterprise IT	Dmitry Nikipelov
			DB	srv-erp-2 (10.10.0.33)		Ms SQL 2005		
Accounting	Galaktika	Accounting software	OS	srv-gal (10.10.0.10)	Galaktika Management Console	Windows 2003	Enterprise IT	Dmitry Nikipelov
			DB	srv-gal (10.10.0.10)		MS SQL 2005		

Спасибо за внимание!

Дмитрий Никипелов
CISO
BAS Innovation