KPMG

cutting through complexity™

10. setkání interních auditorů v oblasti průmyslu

Současné výzvy IT interního auditu

7. Března 2014

Obsah

Kontakt:

Michal Čup
Manager
KPMG Česká republika, s.r.o.
tel. +420 222 123 331
mob. +420 724 981 320
e-mail: mcup@kpmg.cz

KPMG průzkum stavu interního auditu IT

- Průzkum se konal v roce 2013 v zemích regionu EMA (Evropa, Blízký východ, Afrika)
- Zúčastnilo se celkem 400 společností z 21 zemí
- Hlavními respondendz byli vedoucí oddělení auditu IT nebo vedoucí oddělení řízení rizik
- V ČR se zúčastnilo celkem 21 společností napříč několika sektory (především finanční instituce a nadnárodní společnosti)

Klíčové výzvy IT IA (1/2)

Rozsah interního auditu není přizpůsoben rizikům a potřebám společnosti, ale je ovlivněn současným znalostmi a zkušenostmi IT interních auditorů

- Tři čtvrtiny společností uvádí nedostatek znalostí a dovedností jako hlavní důvod nespokojenosti s interním auditem, přesto pouze třetina společností využívá služeb externích poskytovatel

Nutnost reagovat na nově vznikající rizika (SaaS, kybernetická bezpečnost, Big Data, cloud, mobilní technologie, sociální média) a zajistit jejich pokrytí z interních nebo externích zdrojů

Plány IT interního auditu by měly podléhat důslednější kontrole ze strany vedení společnosti.

Činnost interního auditu IT je potřeba lépe sladit s ostatními aktivitami v oblasti správy a řízení společnosti.

Klíčové výzvy IT IA (2/2)

Potřeba dosáhnout vyšší kvality prováděním kontroly kvality činností a používáním rámce pro provádění auditů (v ČR cca polovina respondentů neprovádí kontrolu kvality IA)

Ve společnostech, kde nepůsobí specializovaní IT auditoři je pokrytí oblastí nižší – zaměření především na „tradiční“ oblasti – obecné IT kontroly, technické zabezpečení IT, klíčové IT projekty

Chybí formální cyklus plánování (nebo plánování dle nákladovosti či dostupných dovedností a nikoliv podle hrozícího rizika)

Čtvrtina respondentů v ČR nevyžaduje od IT interních auditorů žádnou profesní certifikaci (na rozdíl od EMA regionu). Pouze 30 procent společností poskytuje svým IT interním auditorům technická školení.

KPMG metodika interního auditu

Zná naše společnost svůj aktuální rizikový profil?

Jsou identifikovaná hlavní rizika? Jsou auditní postupy zacíleny na tyto rizika?

Máme stanoveny auditní procedury, alokovány nutné kapacity?

Hlavní fáze našeho přístupu

Plánování:

→ příprava detailního auditního plánu pro oblasti identifikované interní rizikovou analýzou

Realizace auditu

→ realizace jednotlivých IT auditů (oblastí)

→ prezentace výsledků auditu

Hlavní benefity našeho přístupu:

→Flexibilní přístup

→Porovnání s „best practice“ v průmyslovém sektoru (benchmarking)

→Jasná a strukturovaná prezentace auditních zjištění

→Transparentní komunikace

→Žádná překvapení – všechna zjištění jsou včas komunikována a vysvětlena s odpovědnými zaměstnanci

→Průběžné sledování nápravy zjištění

Máme nástroj monitorující stav zjištění a nápravných opatření? Jsou pravidelně sledována a vyhodnocována?

Máme připravený detailní audit program? Mají naši IT auditoři odpovídající znalosti?

Jaká by měla být forma našich výstupů, kdo jsou jejich příjemci?

Typické oblasti IT interního auditu (1/3)

Area	Proces	Popis
IT bezpečnost	Řízení informačních rizik	
	Řízení a administrace přístupových práv	
	Autentizace (nastavení hesel)	
	Metodický rámec pro řízení bezpečnosti	
	Bezpečnost koncových zařízení	
	Síťová topologie a bezpečnost	
	Antivirus	
	Business continuity and disaster recovery	

Typické oblasti IT interního auditu (2/3)

Area	Proces	Popis
IT bezpečnost	Organizace IT bezpečnosti	
	Fyzická bezpečnost	
	Řízení bezpečnostních incidentů	
Řízení IT	IT strategie	
	IT Organizace	
IT provoz	Zálohování	
	Datové přenosy a interface mezi systémy	
	Kontrola migrace dat (z původního systému na nový)	
	Řízení incidentů	
Řízení změn	Proces řízení změn	
	Oddělené testovací prostředí	

Typické oblasti IT interního auditu (3/3)

Area	Proces	Popis
Specifické testy systému SAP	Obecné IT kontroly	
	Segregation of Duties	
	3-way match	
	Kontrola dvojí fakturace	

Typická zjištění (1/3)

	Oblast	Zjištění	Detail zjištění
1	**Řízení přístupů**	**<u>Sdílený uživatelský účet v systému XY</u>** • Systém, který je používán pro administraci klientů má sdílený účet . • Přihlašovací údaje k tomuto účtu jsou sdíleny třemi zaměstnanci útvaru podpory uživatelů.	
		<u>Přidělování přístupových práv</u> • Přístupová práva nejsou žadatelem řádně specifikována • Konfliktní matice rolí na pracovní pozice není zavedena	
		<u>Nedostatečná kontrola přístupových práv</u> • Není prováděna kontrola aktivních účtů na odchozí zaměstnance • Není prováděna kontrola rozsahu uživatelských práv na žádosti nebo na konfliktní matici • Kontrola není prováděna pravidelně a pro všechny systémy • Kontrola není formálně dokumentována	
2	**Segregation of Duties**	**<u>Nedostatečně nastavené kontroly konfliktních rolí v systému SAP</u>** • Systém pro kontrolu konfliktních rolí/transakcí není správně nastaven/nakonfigurován	

Typická zjištění (2/3)

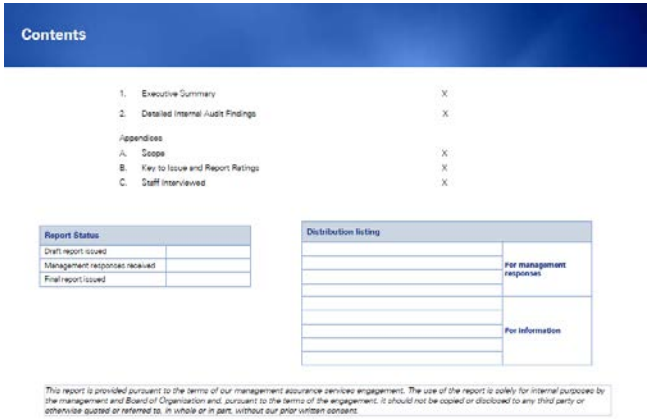
	Oblast	Zjištění	Detail zjištění
3	**Účty třetích stran**	**<u>Přístupy třetích stran do produkčního prostředí</u>** • Nepřetržitý přístup třetích stran do produkčního prostředí společnosti • Přístup třetích stran do produkčního prostředí není monitorován	
4	**Řízení změn**	**<u>Neformální proces řízení změn</u>** • Proces řízení změn není formálně definovaný • Není používán žádný nástroj na řízení změn, který by v sobě měl implementované odpovídající workflow • Klíčové „know-how“ týkající se systému je soustředěno u jednoho člověka • Změny nejsou odpovídajícím způsobem dokumentovány	
5	**Oddělené testovací prostředí**	**<u>Absence odděleného testovacího prostředí</u>** • Absence samostatného testovacího prostředí • Nedostatečný rozsah testování (pouze UAT) • Nejsou vytvořena testovací data • Nejsou zpracované testovací scénáře	
6	**Klasifikace informačních aktiv**	**<u>Vlastnictví a klasifikace informačních aktiv</u>** • Není zaveden registr informačních aktiv (společnost nemá jasně definované, co jsou její nejdůležitější aktiva) • Nejsou určeni vlastníci dat • Není definováno jak s jednotlivými informacemi bezpečně nakládat	

Typická zjištění (3/3)

	Oblast	Zjištění	Detail zjištění
7	**Analýza informačních rizik**	**Chybějící analýza informačních rizik** • Analýza rizik nebyla zatím provedena • Pro analýzu rizik nebyla použita žádná metodika • Analýza rizik není periodicky opakována • Rizika identifikovaná analýzou rizik nejsou odpovídajícím způsobem řízena	
8	**Mobilní zařízení**	**Zabezpečení mobilních zařízení** • Služební notebooky nejsou šifrovány • Firemní telefony nejsou dostatečně chráněny	
9	**Datový přenos**	**Datový přenos mezi produkčním a účetním systémem** • Manuální zásahy v procesu datového přenosu	
10	**Schvalovací workflow v systému**	**Workflow pro schvalování faktur není v systému implementováno** • Faktury se schvalují mimo systém a poté manuálně zadávají do systému • Absence kompenzačních kontrol	

BACKUP

Příklady auditních reportů



Contents

1. Executive Summary X
2. Detailed Internal Audit Findings X

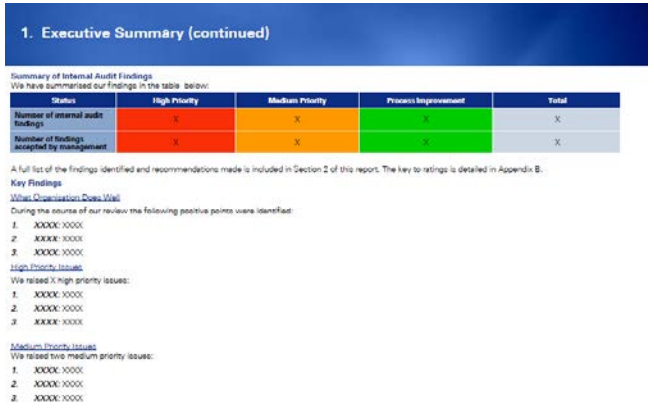
Appendices

A. Scope X
B. Key to Issue and Report Ratings X
C. Staff Interviewed X

Report Status	
Draft report issued	
Management responses received	
Final report issued	

Distribution listing	
	For management responses
	For information

This report is provided pursuant to the terms of our management assurance services engagement. The use of the report is solely for internal purposes by the management and Board of Organization and, pursuant to the terms of the engagement. It should not be copied or disclosed to any third party or otherwise quoted or referred to, in whole or in part, without our prior written consent.



1. Executive Summary (continued)

Summary of Internal Audit Findings
We have summarised our findings in the table below:

Status	High Priority	Medium Priority	Process Improvement	Total
Number of internal audit findings	X	X	X	X
Number of findings accepted by management	X	X	X	X

A full list of the findings identified and recommendations made is included in Section 2 of this report. The key to ratings is detailed in Appendix B.

Key Findings

What Organization Does Well

During the course of our review the following positive points were identified:

1. *XXXX:* XXXX
2. *XXXX:* XXXX
3. *XXXX:* XXXX

High Priority Issues

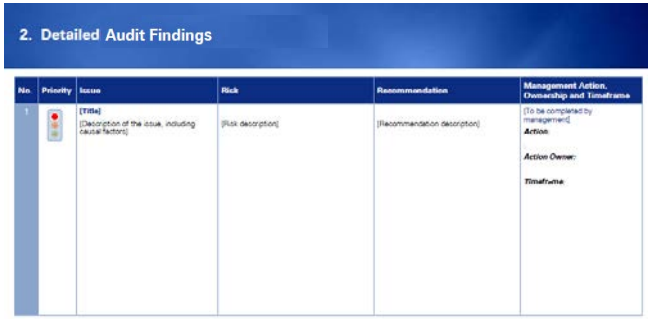
We raised X high priority issues:

1. *XXXX:* XXXX
2. *XXXX:* XXXX
3. *XXXX:* XXXX

Medium Priority Issues

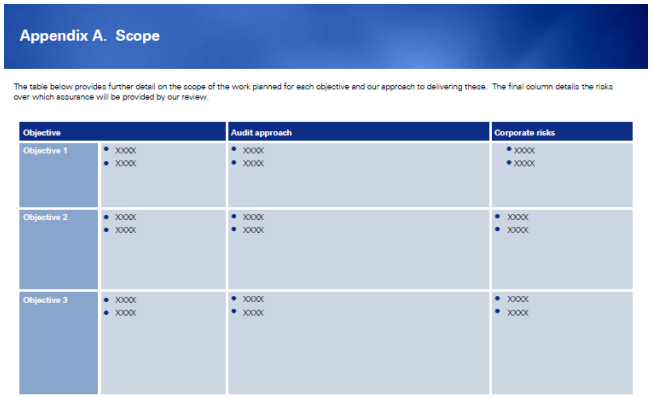
We raised two medium priority issues:

1. *XXXX:* XXXX
2. *XXXX:* XXXX
3. *XXXX:* XXXX



2. Detailed Audit Findings

No.	Priority	Issue	Risk	Recommendation	Management Action, Ownership and Timeframe
1		[Title] [Description of the issue, including causal factors]	[Risk description]	[Recommendation description]	[To be completed by management] *Action* *Action Owner:* *Timeframe*



Appendix A. Scope

The table below provides further detail on the scope of the work planned for each objective and our approach to delivering these. The final column details the risks over which assurance will be provided by our review.

Objective		Audit approach	Corporate risks
Objective 1	• XXXX • XXXX	• XXXX • XXXX	• XXXX • XXXX
Objective 2	• XXXX • XXXX	• XXXX • XXXX	• XXXX • XXXX
Objective 3	• XXXX • XXXX	• XXXX • XXXX	• XXXX • XXXX

Appendix B. Key to Issue and Report Ratings

The tables below set out the definitions used by Internal Audit for the priority ratings for (a) issues, and (b) reports. These have been developed and agreed with Organization management for prioritising Internal Audit findings according to their relative significance depending on their impact to the process. The individual Internal Audit findings contained in this report have been discussed and rated with management.

Guidance for rating Internal Audit issues

Priority rating for issues raised		
High: Issues arising referring to important matters that are fundamental to the system of internal control. We believe that the matters observed might cause a business objective not to be met or leave a risk unmitigated and need to be addressed as a matter of urgency.	**Medium:** Issues arising referring mainly to matters that have an important effect on controls but do not require immediate action. A business objective may still be met in full or in part or a risk adequately mitigated but the weakness represents a significant deficiency in the system.	**Process Improvement:** Issues arising that would, if corrected, improve internal control in general but are not vital to the overall system of internal control. Process improvement issues will also focus on opportunities to improve efficiency of processes or the management and control of risk.

Guidance for rating report

Priority rating for overall report		
Inadequate: Multiple issues arising referring to important matters that are fundamental to the system of internal control.	**Requires Improvement:** Most issues arising refer to matters that have an important effect on controls but do not require immediate action.	**Adequate:** Most issues arising would, if corrected, improve internal control in general but are not vital to the overall system of internal control.