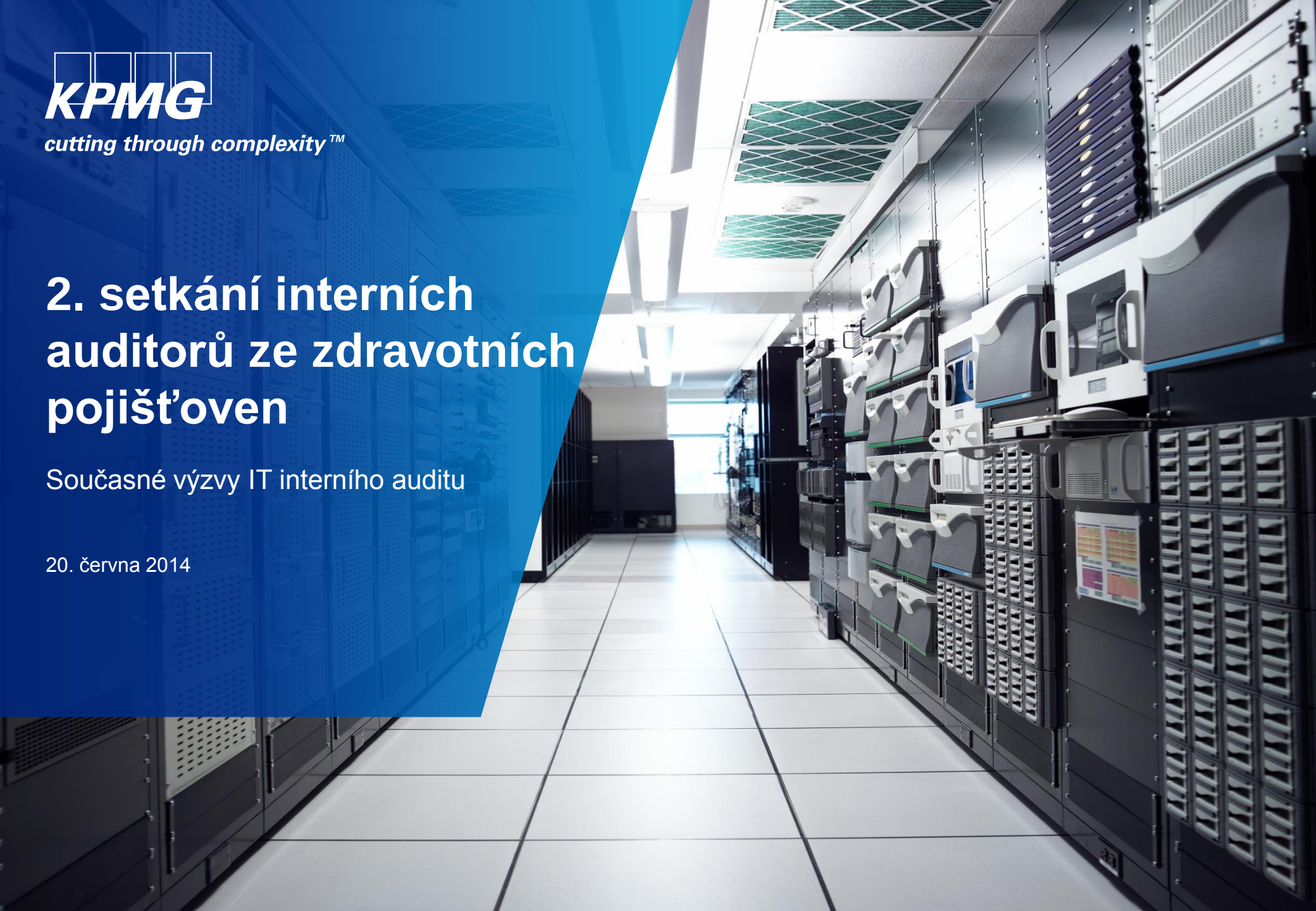


KPMG

cutting through complexity™

2. setkání interních auditorů ze zdravotních pojišťoven

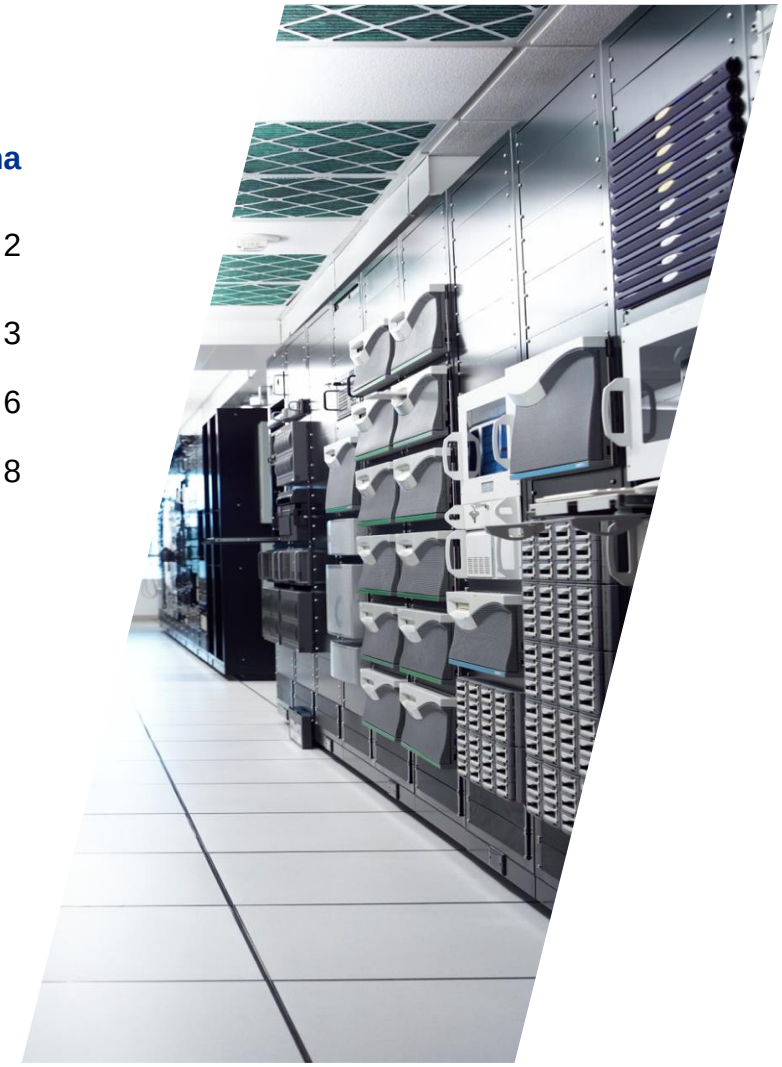
Současné výzvy IT interního auditu

20. června 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 respondenty 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), z toho 4 zdravotní pojišťovny

KPMG průzkum stavu interního auditu IT
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 poskytovatelů

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.

KPMG průzkum stavu interního auditu IT
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 průzkum stavu interního auditu IT
Zdravotní pojišťovny – vybrané oblasti

- Interní auditoři jsou funkčně podřízeni a reportují přímo Řediteli ZP
- Školení je věnováno zpravidla 40-60 hodin – v souladu s celkovými výsledky
- Na IT audity jsou zpravidla využívání externí zdroje (outsourcing/co-sourcing)
- Zaměření především na „tradiční“ oblasti – obecné IT kontroly, technické zabezpečení IT, klíčové IT projekty
- Auditní plán je zpravidla připraven na základě kombinace rizikového a cyklického přístupu
- Analýza rizik je prováděna s roční periodicitou
- Pro auditní práci nejsou zpravidla využívány systémové nástroje (datová analýza, auditní software)

Typické oblasti IT interního auditu (1/2)

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 (2/2)

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	

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 „myname“. • 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</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**	**<u>Chybějící analýza informačních rizik</u>** • 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**	**<u>Zabezpečení mobilních zařízení</u>** • Služební notebooky nejsou šifrovány • Firemní telefony nejsou dostatečně chráněny	
9	**Datový přenos**	**<u>Datový přenos mezi produkčním a účetním systémem</u>** • Manuální zásahy v procesu datového přenosu	
10	**Schvalovací workflow v systému**	**<u>Workflow pro schvalování faktur není v systému implementováno</u>** • Faktury se schvalují mimo systém a poté manuálně zadávají do systému • Absence kompenzačních kontrol