Deloitte.

Vnitřní kontrolní systém a jeho audit

7. SETKÁNÍ AUDITORŮ PRŮMYSLU

11. 5. 2012

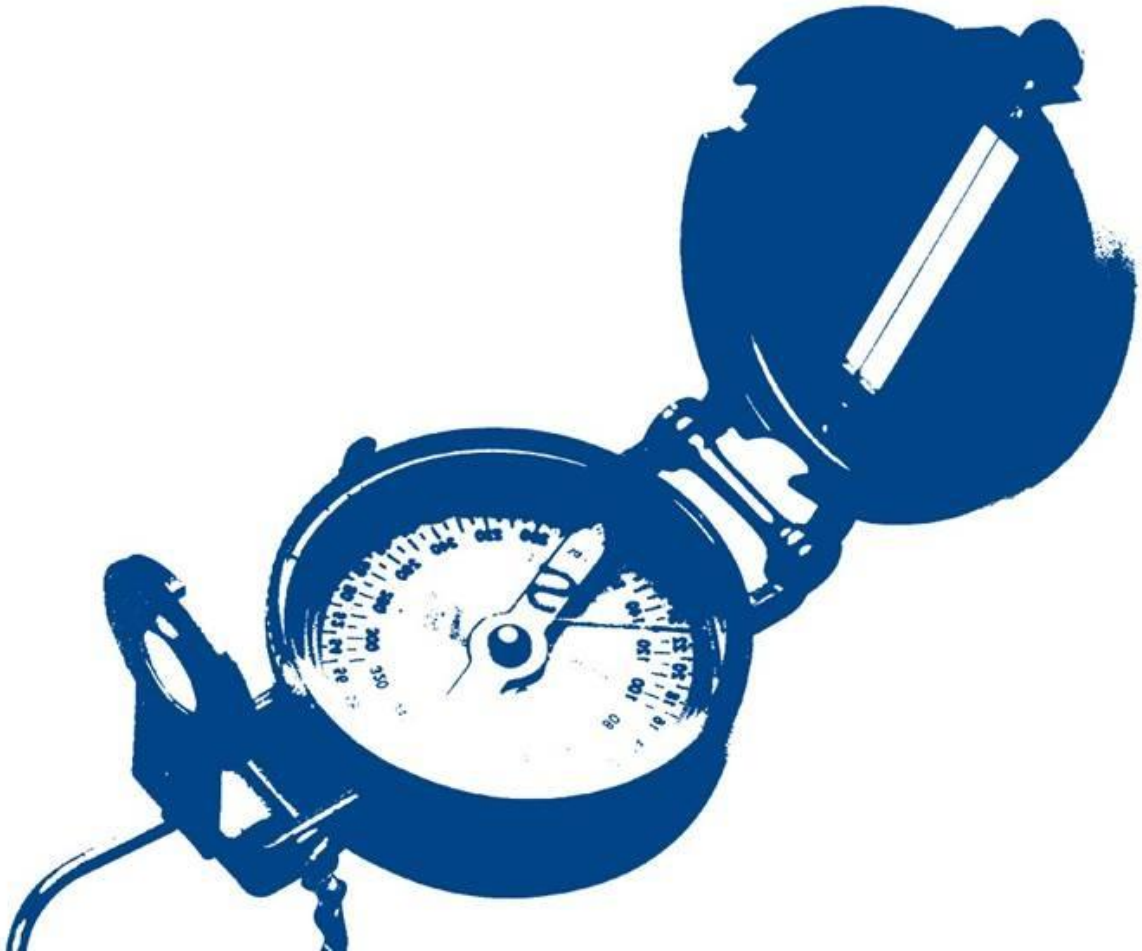
Vlastimil Červený, CIA, CISA

Audit.Daně.Poradenské služby.Finanční poradenství.

Agenda

- Požadavky na VŘKS dle metodik a standardů
- Definice VŘKS dle rámce COSO
- Role interního auditu v rámci VŘKS
- Hodnocení účinnosti a efektivnosti VŘKS
- Z praxe auditora – typické nedostatky VŘKS

Požadavky na VŘKS dle metodik a standardů



Porovnání požadavků na VŘKS různých standardů

Požadavky na VŘKS vycházejí ze stejných principů. Liší se zejména v cílech VŘKS.

SOX - PCAOB standard AS2

- uvádí jako jeden z vhodných VŘKS rámec dle COSO.
- požadavky zákona SOX se týkají spolehlivosti finančního výkaznictví.

IIA - Standard 2120

Auditor by měl hodnotit VŘKS z pohledu:

- spolehlivosti a integrity finančních a provozních informací,
- účinnosti a efektivnosti procesů,
- ochrany aktiv,
- dodržování zákonů, předpisů a smluv.

COBIT – Kontrolní rámec pro řízení IT

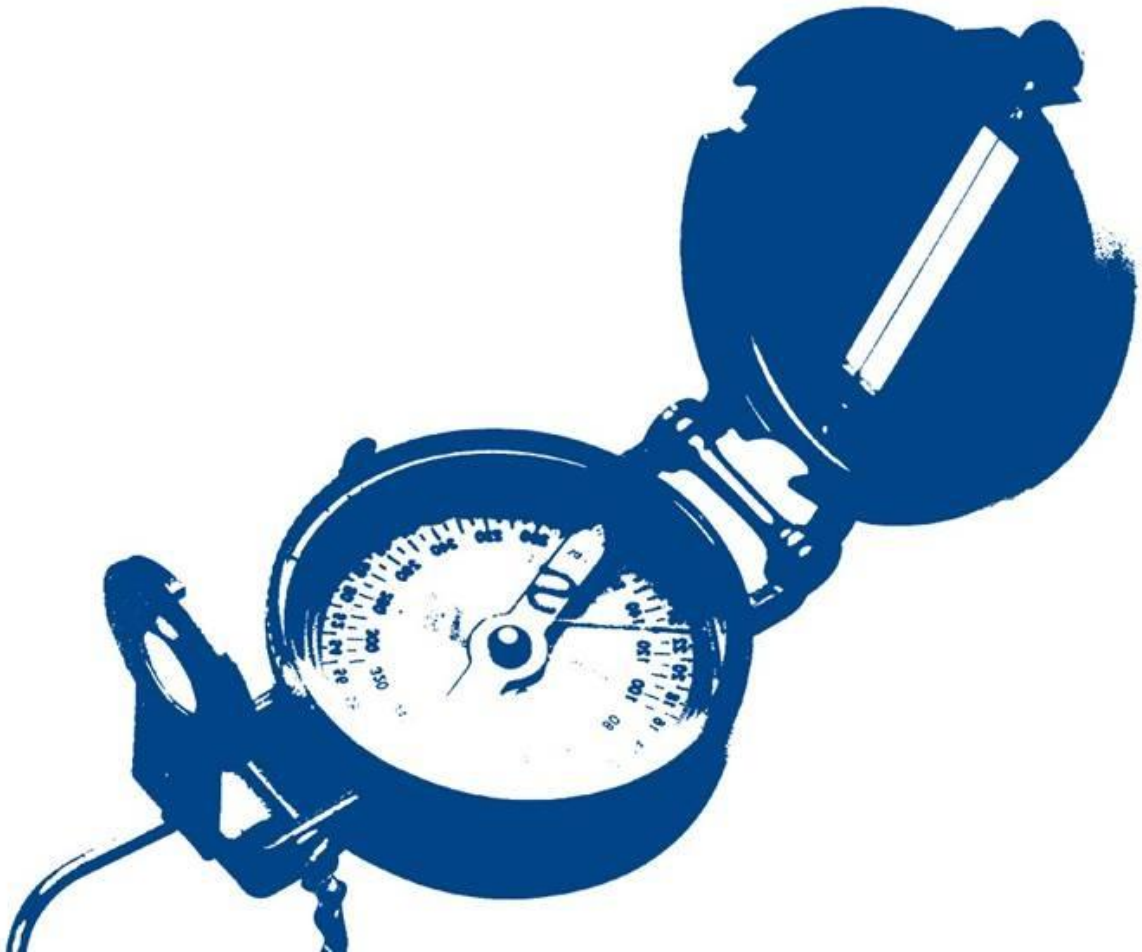
- plánování a organizace IT
- akvizice a implementace IT
- Provoz a podpora IT
- Monitoring a hodnoceni

Direktiva EU 8 - článek 41, odst. 2, b) povinnost zřídit výbor pro audit.

Povinnosti výboru pro audit:

- (a) monitorování procesu finančního výkaznictví,
- (b) monitorování efektivnosti VŘKS, interního auditu a řízení rizik.

Definice VŘKS dle rámce COSO



Definice VŘKS dle rámce COSO

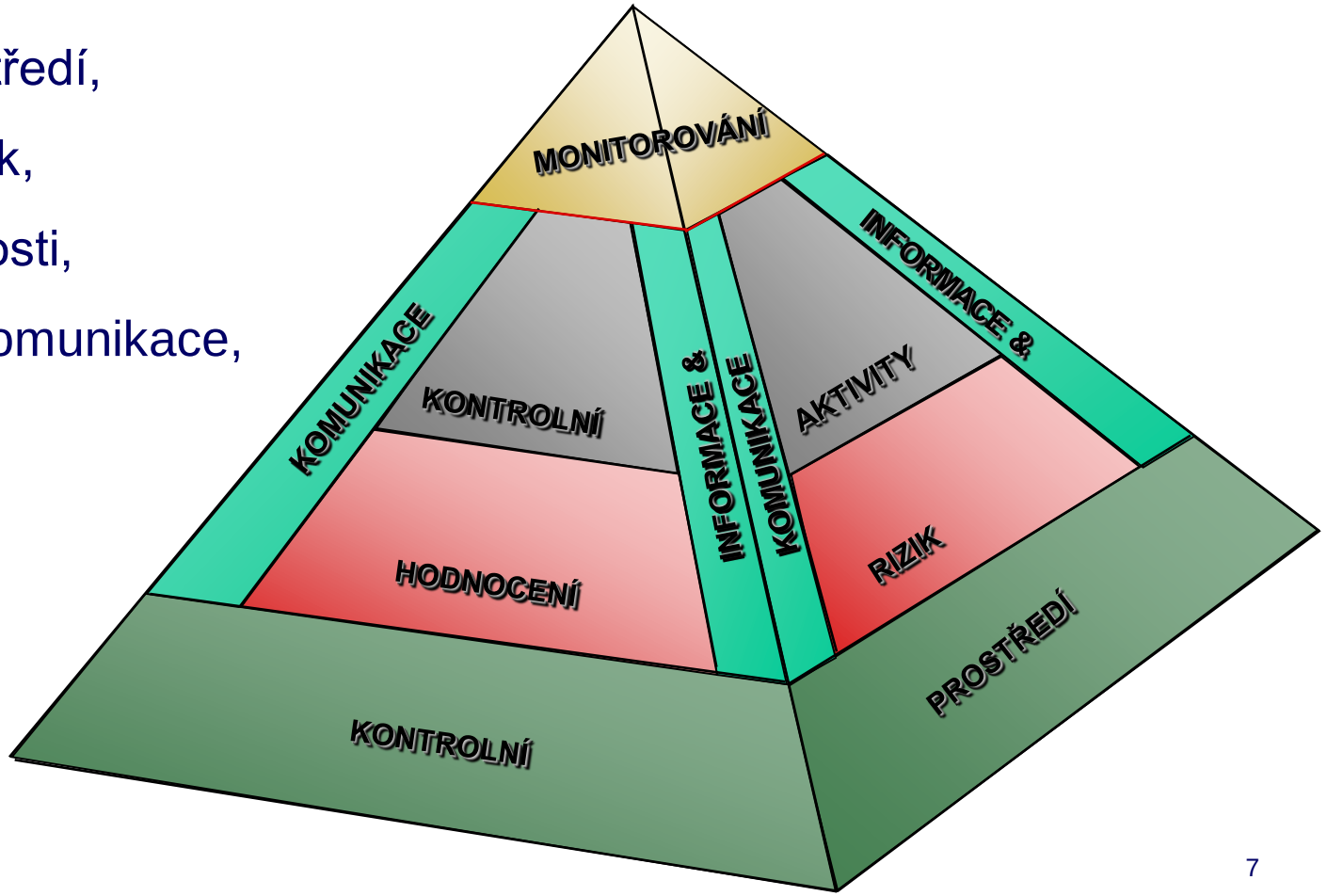
Interní kontrolní systém je proces uskutečňovaný vedením společnosti a jinými pracovníky organizace, jehož cílem je poskytnout přiměřené ujištění o plnění cílů v následujících kategoriích:

- efektivnost a účinnost operací,
- spolehlivost finančního výkaznictví,
- soulad s legislativou a ostatními platnými předpisy.

Definice VŘKS dle rámce COSO

Dle COSO se VŘKS skládá z pěti vzájemně provázaných komponent, které dohromady tvoří integrovaný rámec. Tyto komponenty jsou následující:

- kontrolní prostředí,
- hodnocení rizik,
- kontrolní činnosti,
- informace a komunikace,
- monitorování.



Komponenty COSO - kontrolní prostředí

- **Kontrolní prostředí** - zahrnuje celkový přístup vedení k řízení organizace - firemní kulturu.
- Do kontrolního prostředí patří prvky nehmotné i hmotné povahy:
  - integrita a etické hodnoty,
  - správa a organizační struktura,
  - filozofie vedení,
  - řízení pravomocí a odpovědností,
  - pravidla a praxe lidských zdrojů.
- Vedení ovlivňuje kontrolní prostředí organizace zaváděním etických standardů, svým chováním, účinným informováním o pravidlech a procedurách.

Komponenty COSO - hodnocení rizik

- **Hodnocení rizik** - zahrnuje identifikaci a analýzu rizik, které ohrožují plnění cílů společnosti.
- Hodnocení rizik začíná identifikací rizik souvisejících s obchodními cíli provázanými se všemi úrovněmi organizace:
  - **Na úrovni celé organizace**
    - cíle organizace, čeho chce organizace dosáhnout, jsou základním kamenem účinného VŘKS,
    - vycházejí ze strategického a obchodního plánu.
  - **Na úrovni jednotlivých aktivit**
    - stanovováním cílů konkrétních projektů, procesů a aktivit.
- Posuzování rizik vyžaduje zhodnocení externích i interních faktorů a jejich vlivu na provoz, finanční výkaznictví a soulad s předpisy.
- Používá různé techniky:
  - sebehodnocení kontrol (CSA), řízení podnikových rizik (ERM) a mnoho dalších.

Komponenty COSO - kontrolní činnosti

- **Kontrolní činnosti** - jsou politiky, postupy, pravidla a činnosti, jejichž účelem je pomoc při dosahování cílů a snižování rizik.
- Kontrolní činnosti musí být implementovány do procesů společnosti a využívány k řízení rizik. Soustředí se na prevenci, odhalování a nápravu.
- Typy kontrolních činností:
  - schválení, autorizace a ověřování,
  - prověřování ukazatelů výkonnosti (např. klíčové ukazatele výkonnosti, metriky),
  - ochrana aktiv,
  - oddělení odpovědností (např. iniciace transakce - schvalování - zaznamenání),
  - kontroly informačních systémů (např. řízení přístupu).

Komponenty COSO - kontrolní činnosti - pokračování

- Kontrolní činnosti na úrovni celé organizace (CLC)
  - ovlivňují organizaci jako celek nebo více procesů

- Kontrolní činnosti na úrovni procesů (PLC)
  - ovlivňují jednotlivé procesy nebo činnosti

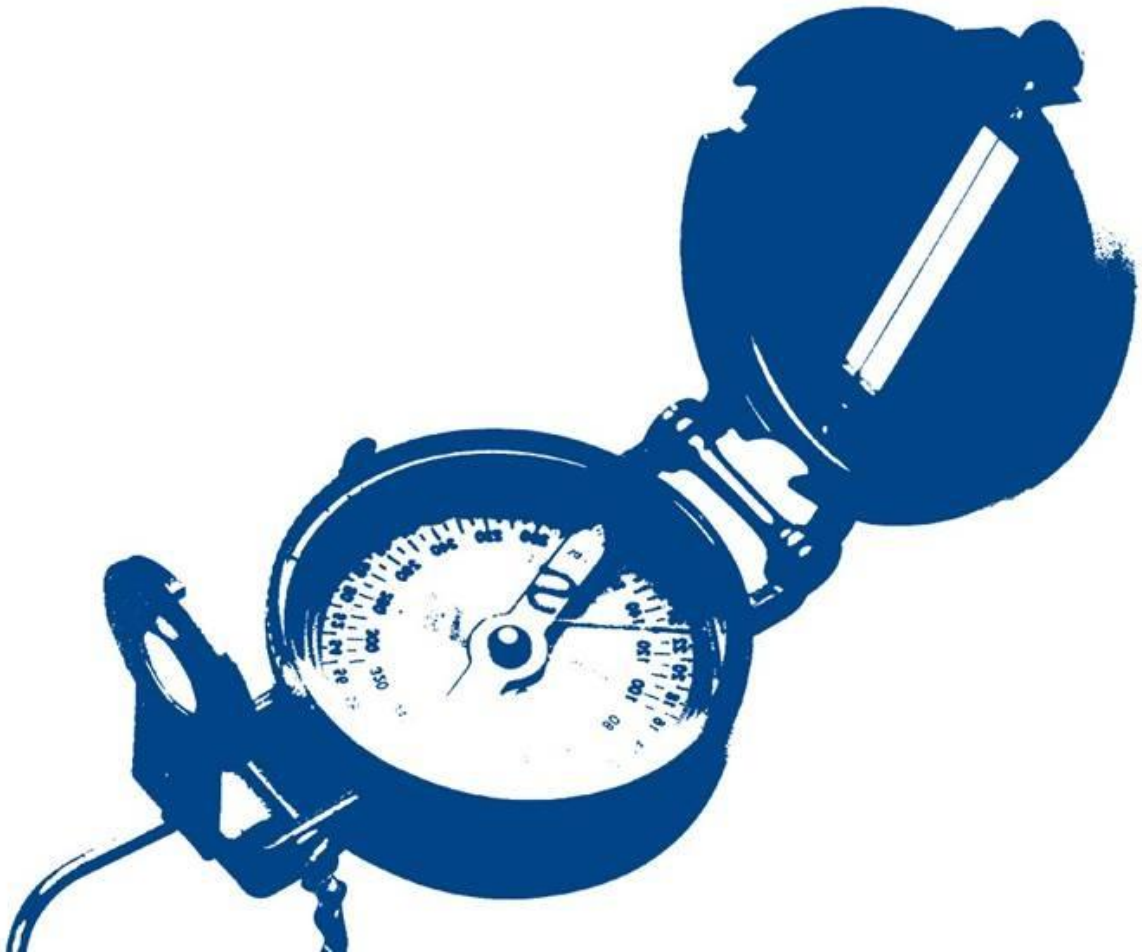
Komponenty COSO - informace a komunikace

- **Informace a komunikace** - zajišťuje, že relevantní informace jsou získány a zpracovány tak, aby byly správné, aktuální a dostupné včas a na správném místě.
- Poskytovány různými formálními i neformálními způsoby:
  - ústně (např. jednání, zpětná vazba)
  - písemně (např. pravidla, procesy, popisy práce)
  - chováním (např. vedení jde příkladem)
- Úplnost informací je pro obchodní rozhodnutí naprostou nutností:
  - interní kontrolní mechanismy musí zajistit, že informace jsou odpovídající, aktuální, včasné, přesné a dostupné.
  - vazba na kontrolní mechanismy IS/IT (COBIT)
- Odpovědnost vedení:
  - komunikace v organizaci musí probíhat horizontálně i vertikálně oběma směry
  - komunikační kanály se zákazníky, dodavateli a ostatními stranami musí být otevřené

Komponenty COSO – monitorování

- **Monitorování** - zjišťuje dohled nad VŘKS; ověřuje, že kontrolní činnosti jsou správně navrženy a efektivně prováděny.
- Účinnost VŘKS by měla být hodnocena průběžným monitorováním operací a samostatnými periodickými hodnoceními.
- Rozsah a frekvence monitorovacích činností závisí na významnosti kontrolovaných rizik a důležitosti kontrol při snižování rizik.
- Monitorovací činnosti by měly být zabudovány do běžných opakujících se provozních činností organizace.
- U identifikovaných nedostatků by měla být stanovena jasná nápravná opatření a zodpovědnost za jejich realizaci.

Role interního auditu v rámci VŘKS



Role a odpovědnosti

Top management

- určuje standard kontrolního prostředí,
- udržuje si nejvyšší zodpovědnost za VŘKS a řízení rizik v celé společnosti.

Provozní management

- přímo zodpovědný za efektivnost provozu a VŘKS ve vztahu k cílům společnosti,
- pravidelně hodnotí a prosazuje řízení rizik a kontrolní prostředí,
- definuje a implementuje kroky pro zlepšení VŘKS.

Finanční management

- podílí se na zodpovědnosti provozního vedení a souvisejících činnostech,
- poskytuje vodítka pro navrhování, zavádění, provádění a monitorování odpovídajících kontrolních aktivit.

Role a odpovědnosti - pokračování

Interní audit

- hodnotí adekvátnost a účinnost VŘKS,
- navrhuje plán interního auditu vycházející ze strategického řízení rizik,
- podává zprávy o zjištěních a vydává doporučení,
- poskytuje podporu pro posuzování rizik a kontrolních aktivit,
- monitoruje míru vystavení organizace riziku a vydává doporučení týkající se posuzování rizik a VŘKS.

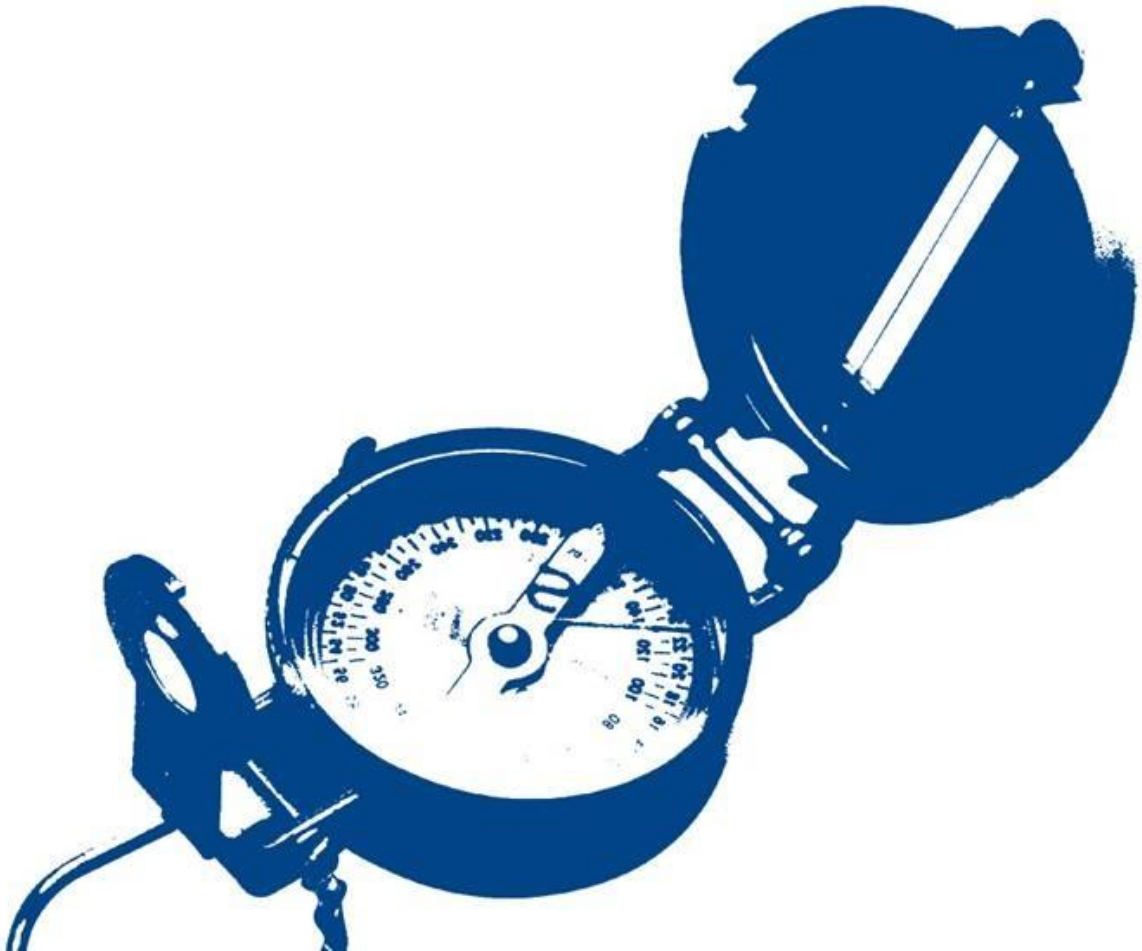
Výbor pro audit

- monitoruje efektivnosti VŘKS, interního auditu a řízení rizik,
- dohlíží na adekvátnost celkového kontrolního prostředí,
- usměrňuje pozornost představenstva k oblastem IA a VŘKS.

Externí audit

- hodnotí efektivitu VŘKS za účelem stanovení rozsahu procedur externího auditu,
- vydává výrok k účetní závěrce.

Hodnocení účinnosti a efektivnosti VŘKS



Role interního auditu v oblasti řídicích a kontrolních mechanismů

Standard 2120 - Řízení a kontrola.

- Interní audit napomáhá společnosti udržovat účinné řídicí a kontrolní systémy tím, že hodnotí jejich účinnost a efektivnost a podporuje jejich neustálé zdokonalování.
- 2120.A1 - Na základě výsledků vyhodnocení rizik interní audit hodnotí adekvátnost a účinnost řídicích a kontrolních mechanismů, týkajících se řízení a správy společnosti, procesů ve společnosti a informačních systémů.
- Toto hodnocení se týká:
  - spolehlivosti a integrity finančních a provozních informací,
  - účinnosti a efektivnosti procesů,
  - ochrany aktiv,
  - dodržování zákonů, předpisů a smluv.

Hodnocení účinnosti a efektivnosti

- **Účinnost** znamená, že VŘKS zajišťuje plnění cílů a pokrývá příslušná rizika (dělám správnou věc - VŘKS je navržen správně).
- **Efektivnos**t znamená, že VŘKS je funguje optimálním, nejméně zdroji plýtvajícím způsobem (dělám správnou věc správným způsobem - VŘKS je navržen tak, aby co nejlépe plnil nadefinovaný cíl ekonomicky výhodným způsobem).

Hodnocení účinnosti

Interní auditor by měl při hodnocení **účinnosti** VŘKS:

- ověřit jsou-li cíle dané kontroly v souladu s cíli společnosti,
- zhodnotit, zda jsou rizika, která ohrožují plnění cílů nadefinována správně a odrážejí-li reálný stav interních procesů společnosti a externích faktorů působících z vnějšku.

COSO uvádí příklady, při kterých je třeba znovu posoudit adekvátnost cílů a rizik, jsou to například:

- změny v regulatorním prostředí,
- změny v provozních činnostech,
- nové informační systémy,
- reorganizace společnosti,
- rychlý růst společnosti.

Hodnocení efektivnosti

Při hodnocení **efektivnosti** by měl interní auditor zhodnotit:

- zda je interní kontrola prováděna nákladově efektivním způsobem,
- jestli není možno rizika snížit nějakým jiným, na spotřebované zdroje (lidské, čas) méně náročným způsobem nebo takovým, který není tolik náchylný k chybám.

Zdokonalování VŘKS

- Požadavek standardu 2120 – zdokonalování VŘKS.
- Interní audit je jedním z mála oddělení, které má příležitost vidět VŘKS jako celek. Má tedy unikátní možnost identifikovat změny VŘKS vedoucí k jeho optimalizaci.
- Optimální systém VŘKS by měl znamenat, že všechny kontrolní cíle jsou správně stanoveny, všechna rizika jsou pokryta kontrolními aktivitami a všechny kontrolní aktivity jsou prováděny nákladově efektivním způsobem.

Zdokonalování VŘKS - pokračování

- Návrhy na zdokonalování VŘKS mohou být založeny na posouzení efektivnosti kontrolních činností:
  - Preventivní kontroly vs. detektivní kontroly
  - Automatizované kontroly vs. manuální kontroly
  - Nákladová efektinost VŘKS (kontrolních činností)

Zdokonalování VŘKS - pokračování

- Návrhy na zdokonalování VŘKS mohou být založeny na posouzení efektivnosti kontrolních činností:
  - Preventivní kontroly vs. detektivní kontroly
  - Automatizované kontroly vs. manuální kontroly
  - Nákladová efektinost VŘKS (kontrolních činností)

Typické nedostatky VŘKS – praxe auditora

- Absence analýzy rizik
- VŘKS nepokrývá kontrolní cíle komplexně (např. chybějící IT kontroly)
- VŘKS není dostatečně zdokumentován
- VŘKS nereflektuje změny business procesů
- Forma kontroly je víc než její obsah
- VŘKS není efektivní

Děkuji za pozornost

Mgr. Vlastimil Červený, CIA, CISA

vcerveny@deloitteCE.com

Member of
Deloitte Touche Tohmatsu