**152 – SEZNÁMENÍ S IT PROSTŘEDÍM**

Zde je zdokumentováno auditorovo seznámení s IT prostředím[[1]](#endnote-2), pochopení a vyhodnocení IT rizik (rizik vyplývajících z používání IT) a vyhodnocení návrhu a implementace příslušných obecných IT kontrol relevantních pro audit.

**ORGANIZACE IT[[2]](#endnote-3)**

**POCHOPENÍ A VYHODNOCENÍ RIZIK VYPLÝVAJÍCÍCH Z POUŽITÍ IT[[3]](#endnote-4)**

|  |  |  |
| --- | --- | --- |
|  | **Aplikace A** | **Aplikace B** |
| **Název IT aplikace** |  |  |
| **Popis a účel IT aplikace[[4]](#endnote-5)** |  |  |
| **Související účetní položky[[5]](#endnote-6)** |  |  |
| **Důležitost aplikace pro účetní závěrku** |  |  |
| **Rizika vyplývající z používání IT[[6]](#endnote-7)** |  |  |
| **Popis relevantních obecných IT kontrol[[7]](#endnote-8)** |  |  |
| **Způsob posouzení obecných IT kontrol[[8]](#endnote-9)** |  |  |
| **Závěr[[9]](#endnote-10)** |  |  |

**ZJIŠTĚNÉ NEDOSTATKY[[10]](#endnote-11)**

**IDENTIFIKOVANÁ RIZIKA[[11]](#endnote-12)**

|  |
| --- |
|  |

***Příloha:***

*Níže jsou uvedeny příklady prvků, které mohou být relevantní při auditorově seznamování se s jednotlivými složkami IT prostředí.*

***ORGANIZACE IT***

* *Je přístup účetní jednotky k informačním systémům a souvisejícím podpůrným činnostem centralizovaný nebo decentralizovaný?*
* *Je oblast IT správy řešena interně (pomocí svých zaměstnanců) nebo účetní jednotka využívá servisní organizace (externího dodavatele). Pokud interně má účetní jednotka několik málo pracovníků s omezenými znalostmi IT nebo s IT kvalifikací nebo přímo specializované IT oddělení s kvalifikovanými pracovníky.*
* *Účetní jednotka používá nejnovější technologie (např. blockchain, robotika nebo umělá inteligence), které ovlivňují její účetní výkaznictví nebo se nejnovější technologie nepoužívají.*
* *Složitost charakteru IT aplikací a základní IT infrastruktury – např. malý, jednoduchý notebook či řešení využívající klientské servery nebo složitý mainframe, velký nebo složitý klientský server, web-facing, infrastruktura jako služba využívající cloudová řešení.*
* *Typy IT aplikací – pořízené IT aplikace (jednoduché komerční softwary) nebo na zakázku tvořené.*

***IDENTIFIKACE IT APLIKACÍ***

*Auditor na základě seznámení s charakterem a složitostí IT prostředí účetní jednotky, včetně charakteru a rozsahu kontrol zpracování informací, určí, které IT aplikace účetní jednotky jsou klíčové pro náležité zpracování finančních informací a pro zajištění jejich integrity. Identifikace těchto klíčových IT aplikací následně ovlivňuje to, které automatizované kontroly (z těch, jež ošetřují identifikovaná rizika materiální nesprávnosti) se auditor u těchto aplikací rozhodne testovat. Jestliže nějaká IT aplikace není pro účetní jednotku klíčová, automatizované kontroly u takové aplikace pravděpodobně nebudou pro testy provozní účinnosti kontrol vhodné ani dostatečně přesné.*

*K automatizovaným kontrolám, které auditor identifikuje v souladu s ISA 315R.26(b), patří například automatizované výpočty nebo kontroly vstupu, zpracování a výstupu. Příkladem může být trojsměrné párování nákupní objednávky, přepravního dokladu a faktury od dodavatele. Jestliže auditor dojde po identifikaci automatizovaných kontrol a na základě seznámení s IT prostředím účetní jednotky k závěru, že pro účetní jednotku je klíčová nějaká IT aplikace, která obsahuje automatizované kontroly, pravděpodobně takovou IT aplikaci vyhodnotí jako aplikaci, která je vystavena rizikům vyplývajícím z používání IT.*

|  |  |
| --- | --- |
| *Příklady charakteristických znaků IT aplikací, které pravděpodobně* ***nejsou*** *vystaveny rizikům vyplývajícím z používání IT* | *Příklady charakteristických znaků IT aplikací, které pravděpodobně* ***jsou*** *vystaveny rizikům vyplývajícím z používání IT* |
| * *Samostatné aplikace;* * *Objem dat (transakcí) není významný;* * *Funkcionalita aplikace není složitá;* * *Každá transakce je doložena originální dokumentací v tištěné podobě.* | * *Aplikace jsou propojeny přes rozhraní;* * *Objem dat (transakcí) je významný;* * *Funkcionalita aplikace je složitá, protože:*   *– aplikace automaticky generuje transakce;*  *– automatické zápisy jsou založeny na řadě složitých výpočtů* |
| *IT aplikace pravděpodobně není vystavena*  *rizikům vyplývajícím z používání IT, protože:*   * *objem dat není významný, a proto se vedení při jejich zpracování či správě nespoléhá na obecné IT kontroly;* * *vedení se nespoléhá na automatizované kontroly ani jiné automatizované funkce, auditor neidentifikoval automatizované kontroly v souladu s ISA 315R.26(a);* * *i když vedení používá ve svých kontrolách zprávy generované systémem, nespoléhá se na ně, ale odsouhlasuje je s dokumentací v tištěné podobě a ověřuje výpočty ve zprávách;* * *auditor přímo testuje informace vytvořené účetní jednotkou, které používá jako důkazní informace.* | *IT aplikace pravděpodobně je vystavena*  *rizikům vyplývajícím z používání IT, protože:*   * *vedení používá pro zpracování a správu dat systém aplikací, neboť objem dat je významný;* * *vedení provádí některé automatizované kontroly prostřednictvím systému aplikací a auditor tyto kontroly také identifikoval* |

***RIZIKA VYPLÝVAJÍCÍ Z POUŽÍVÁNÍ IT***

*Rizika vyplývajících z používání IT spočívají v tom, že účetní jednotka může spoléhat na IT aplikace nesprávně zpracovávající data nebo na IT aplikace zpracovávající nesprávná data, případně obojí. Příkladem takových rizik jsou:*

* *Riziko neoprávněného přístupu k datům, který může vést k jejich zničení nebo nesprávným změnám, včetně zaznamenávání neschválených nebo neexistujících transakcí nebo nesprávného záznamu transakcí. Riziko hrozí především v případech, kdy více uživatelů přistupuje ke společné databázi;*
* *Riziko, že pracovníci IT získají přístupová oprávnění nad rámec oprávnění nezbytných k plnění jejich povinností, čímž je porušeno oddělení pravomocí;*
* *Riziko neoprávněných změny dat v hlavních souborech;*
* *Riziko neoprávněných změny IT aplikací nebo jiných aspektů IT prostředí;*
* *Riziko neprovedení nezbytných změn v IT aplikacích nebo jiných aspektech IT prostředí;*
* *Riziko nevhodného manuálního zásahu;*
* *Riziko ztráty dat nebo přístupu k datům.*

***OBECNÉ IT KONTROLY***

*Obecné kontroly IT jsou zásady a postupy, které slouží k podpoře efektivního fungování aplikací, včetně efektivního provozu automatizovaných kontrol zabudovaných v aplikacích, integrity zpráv generovaných z aplikací a zabezpečení dat uložených v aplikacích. Tyto kontroly mají zajišťovat, že rizika vyplývající z používání IT jsou snížena na přijatelně nízkou úroveň.*

*V rámci auditu by se měl auditor seznámit s kontrolními činnostmi relevantními pro audit, což jsou kontrolní činnosti, které považuje za nezbytné k pochopení, aby vyhodnotil rizika materiální nesprávnosti a navrhnul další auditorské postupy. Níže uvedené kontroly jsou obecné IT kontroly, které jsou relevantní při auditu, aby auditor mohl posoudit rizika a naplánovat testy kontrol a testy věcné správnosti. V závislosti na skutečnostech a okolnostech mohou existovat i jiné obecné IT kontroly, které jsou relevantní.*

*Cílem obecných IT kontrol je ošetření rizik vyplývajících z používání IT. Auditor tedy při rozhodování o tom, které obecné IT kontroly identifikuje, používá poznatky, jež získal o identifikovaných IT aplikacích a dalších aspektech IT prostředí účetní jednotky a příslušných rizicích vyplývajících z používání IT. Jestliže účetní jednotka používá nějaký IT proces v rámci celého IT prostředí nebo v několika IT aplikacích, auditor obvykle identifikuje společná rizika vyplývající z používání IT a společné obecné IT kontroly.*

***Oblast správy přístupu***

* *Kontroly autentizace za účelem omezení přístupu k aplikaci a databázi - kontroly zajišťující, že uživatel vstupující do IT aplikace nebo do jiného aspektu IT prostředí používá vlastní přihlašovací údaje (tj. nepoužívá přihlašovací údaje jiného uživatele) – např. kontroly hesel, včetně minimální délky, složitosti a vypršení platnosti*
* *Kontroly autorizace - kontroly, které uživatelům umožňují přístup k informacím nezbytným pro plnění jejich pracovních povinností, ale k jiným informacím nikoli. Tyto kontroly podporují náležité oddělení pravomocí (např. kontrola přístupu uživatelů prováděná vedením, aby se zajistilo, že přístup udělený v příslušných systémech je úměrný pracovním povinnostem uživatelů a vynucuje oddělení povinností)*
* *Kontroly zřizování uživatelských oprávnění - kontroly, jejichž předmětem je autorizace nových uživatelů a úpravy přístupových oprávnění stávajících uživatelů*
* *Kontroly rušení uživatelských oprávnění - kontroly, jejichž předmětem je odebrání přístupu uživatele po ukončení pracovního poměru nebo převedení jinam*
* *Privilegovaný přístup - kontroly, jejichž předmětem je administrátorský přístup nebo přístup privilegovaných uživatelů*
* *Prověrky přístupu uživatelů - kontroly, jejichž předmětem je recertifikace nebo vyhodnocení trvajícího přístupu uživatele*
* *Kontroly zabezpečení konfigurace - každá technologie má nějaké základní nastavení konfigurace, které omezuje přístup do jejího prostředí*
* *Fyzický přístup - kontroly, jejichž předmětem je fyzický přístup k datovému centru a k hardwaru, protože tento fyzický přístup lze zneužít k obcházení kontrol*

***Oblast správy změn*** *(tj. proces pro správu programových nebo jiných změn IT prostředí, kontroly řízení změn, které zajistí, že do systému budou implementovány pouze autorizované změny pro systémy považované za relevantní pro audit):*

* *Proces řízení změn – kontroly, jejichž předmětem je proces navrhování, programování, testování a migrace změn do produkčního prostředí (tj. prostředí koncového uživatele)*
* *Oddělení povinností týkajících se migrace změn - kontroly, které oddělují přístup k provádění změn a jejich migraci do produkčního prostředí*
* *Vývoj, akvizice nebo implementace systémů - kontroly, jejichž předmětem je prvotní vývoj nebo implementace IT aplikací (případně ve vztahu k jiným aspektům IT prostředí)*
* *Konverze dat - kontroly, jejichž předmětem je konverze dat během vývoje, implementace nebo aktualizace IT prostředí.*

***Oblast správy fungováni IT*** *(tj. kontroly plánování a monitorování úloh, kontroly za účelem zálohování v souladu s plánem a zda je zajištěn přístup pro včasné obnovení, kontroly monitorující zranitelnost IT prostředí a případy jeho narušení):*

* *Kontroly plánování úloh - kontroly, jejichž předmětem je přístup umožňující plánování a spouštění úloh nebo programů, které mohou ovlivnit účetní výkaznictví*
* *Kontroly monitorování úloh - kontroly, jejichž předmětem je sledování úspěšného provádění úloh nebo programů týkajících se účetního výkaznictví*
* *Kontroly zálohování a obnovení - kontroly, jejichž předmětem je to, zda jsou data účetního výkaznictví zálohována v souladu s plánem a zda je k nim zajištěn přístup pro včasné obnovení v případě výpadku nebo útoku*
* *Kontroly detekce narušení - kontroly monitorující zranitelnost IT prostředí nebo případy jeho narušení*

1. Prostředí IT lze definovat jako zásady a postupy, které účetní jednotka implementuje a aplikační systémy, datové sklady, zapisovače zpráv a základní IT infrastrukturu (databáze, operační systémy, sítě, rozhraní), které účetní jednotka používá k podpoře obchodních operací a dosáhnutí obchodních strategií. Příklady konkrétních prvků, jež mohou být v rámci tohoto formuláře uvedeny, jsou obsaženy v Příloze tohoto formuláře. [↑](#endnote-ref-2)
2. Popište stručně organizaci v rámci IT prostředí. [↑](#endnote-ref-3)
3. Zdokumentujte pro každou IT aplikaci důležitou pro audit. V případě většího počtu IT aplikací přidejte další sloupce (podle počtu aplikací) anebo zkopírujte danou tabulku a vyplňte ji pro každou aplikaci zvlášť. Komplexnější IT prostředí mohou vyžadovat rozsáhlejší popisy, které může být obtížné vtěsnat do tabulky v tomto formuláři. V takovém případě může být nutno potřebné informace zdokumentovat separátně, nicméně doporučuje se strukturovat informace v krocích naznačených výše uvedenou tabulkou. [↑](#endnote-ref-4)
4. Popište, jestli se jedná o aplikaci, software, datový sklad či generator sestav, a dále k jakému účelu se IT aplikace využívá, např. vedení účetnictví, hlavní ERP system (komplexní informační systém k efektivnímu řízení firemních zdrojů, informační systém, který ve firmě zastřešuje veškeré důležité procesy), CRM system (informačním systémem spravující údaje týkající se interakce se zákazníkem a bývá propojen poté s dalšími IS), objednávkový systém apod. [↑](#endnote-ref-5)
5. Uveďte položky účetní závěrky, resp. účty, které jsou ovlivněny příslušnou IT aplikací. [↑](#endnote-ref-6)
6. Příklady jsou uvedeny v Příloze tohoto formuláře. [↑](#endnote-ref-7)
7. Příklady jsou uvedeny v Příloze tohoto formuláře. [↑](#endnote-ref-8)
8. Zaznamenejte stručně, jakým způsobem byla kontrola auditorem posouzena. Pro každou kontrolu je třeba (i) posoudit, zda je kontrola navržena tak, že účinně ošetřuje riziko materiální nesprávnosti na úrovni tvrzení nebo že účinně podporuje fungování jiných kontrol; (ii) zjistit, zda kontrola byla zavedena, a to nejen dotazováním pracovníků účetní jednotky, ale i provedením dalších postupů (např. pozorování nebo opakované provedení kontroly, inspekce dokumentů nebo výkazů prokazujících provedení kontroly, nebo sledování průběhu transakce informačním systémem). [↑](#endnote-ref-9)
9. Závěr auditora, zdali jsou posuzované obecné IT kontroly vhodně navrženy a zavedeny. [↑](#endnote-ref-10)
10. Zde se zdokumentují zjištěné nedostatky v návrhu či zavedení kontrol, které budou komunikovány vedení (všechny nedostatky), popřípadě osobám pověřeným správou a řízením (významné nedostatky). Pokud auditor zjistil jeden či více kontrolních nedostatků, je povinen posoudit dopady, které tyto nedostatky mají pro jeho návrh dalších auditorských postupů. Toto posouzení je vhodné zdokumentovat v tomto formuláři a jeho výsledky promítnout ve formuláři 180 – VYHODNOCENÍ RIZIK A PLÁN AUDITU. [↑](#endnote-ref-11)
11. Riziko obvykle vyplývá ze zjištěné absence či nedostatečnosti kontrol, pokud daná absence či nedostatek dle názoru auditora přispívá ke vzniku rizika materiální nesprávnosti. Riziko ale též může být identifikováno v oblastech, kde existují silné kontroly, protože se jedná o oblasti, kde samo vedení cítí existenci rizika vzniku materiálních nesprávností (a proto v dané oblasti kontroly zavedlo). Existence takových kontrol tudíž může ukazovat na rizikové oblasti. Identifikovaná rizika přenést do formuláře 180 – VYHODNOCENÍ RIZIK A PLÁN AUDITU. [↑](#endnote-ref-12)