Prováděcí směrnice

Etický kodex – Důvěrnost

International Professional Practices Framework

3. Zásada Etického kodexu IIA: Důvěrnost

Interní auditoři respektují vlastnictví a hodnotu informací, které získávají při své činnosti, a tyto informace neposkytují bez příslušného souhlasu, pokud neexistuje právní nebo profesní povinnost tak učinit.

Pravidla jednání

Interní auditoři:

3.1. Budou obezřetní při použití a ochraně informací, které získají v průběhu plnění svých povinností.

3.2. Nepoužijí získané informace pro jakýkoli osobní prospěch a ani žádným jiným způsobem, který by byl v rozporu se zákonem nebo na újmu oprávněných zájmů organizace a jejích etických cílů.

Začínáme

Mezinárodní standardy pro profesní praxi interního auditu vyžadují dosažení souladu s Etickým kodexem, který se skládá ze 4 zásad. Každá zásada je doplněna pravidly jednání, která musí interní auditoři naplňovat, aby správným způsobem prokázali splnění dané zásady. Tato prováděcí směrnice je určena pro prokázání způsobu, jakým dosáhnout souladu se zásadou důvěrnosti.

Pro interní auditory je vhodným začátkem seznámení se s profesními povinnostmi, které jsou vyjádřeny v IPPF, a s ostatními profesními standardy a směrnicemi týkajícími se dané organizace a odvětví, ve kterém vykonávají svoji práci. Členství v profesních organizacích může interním auditorům napomoci při zajištění informací o aktuálním stavu profesních povinností.

Informace zahrnují data ve fyzické podobě, jako jsou tištěné dokumenty, a v elektronické podobě, jako jsou audio, video a kódovaná data. Důvěrnost zahrnuje ochranu informací před jejich neoprávněným zpřístupněním jednotlivcům a entitám, jak uvnitř, tak vně organizace. Interní auditoři by se měli seznámit se zákony a regulatorními požadavky, které se týkají důvěrnosti a informační bezpečnosti v právních rámcích,

v kterých jejich organizace působí, a také by měli znát všechny zásady dané organizace a útvaru interního auditu. Tyto zásady mohou například stanovovat, jaký druh informací může být zveřejněn, definovat subjekty, které musí schválit zveřejnění a postupy, kterými je nutno se řídit.

I když na důvěrnost není explicitně ve *Standardech* odkazováno, požadavky související s omezením distribuce výsledků zakázek jsou diskutovány v prováděcích standardech 2201.A1, 2330.A1, 2330.C1, 2410.A3 a 2440.A2. Interní auditoři by se měli seznámit s těmito standardy, jejich prováděcími směrnicemi a souvisejícími doplňkovými směrnicemi IIA.

Přístupy využívané pro realizaci

Vedoucí interního auditu

Zásady a postupy

Organizace většinou vydávají zásady informační bezpečnosti, aby chránily data, která získávají, využívají a produkují, a aby zajistily soulad se zákony a regulatorními požadavky, které se týkají odvětví a právního rámce, v nichž působí (např. Obecné nařízení o ochraně osobních údajů Evropské unie (GDPR) nebo EU – U.S. rámec ochrany důvěrnosti). Tyto zásady jsou naplňovány prostřednictvím jednoznačných postupů a ostatních kontrolních a řídicích mechanismů a typicky zahrnují oblast důvěrnosti dat, uchovávání záznamů a fyzické a digitální bezpečnosti informací uvnitř a vně dané organizace.

Aby lépe pochopil dopad právních a regulatorních požadavků a ochranných opatření (například právní výsady nebo ochrana komunikace klient – advokát), vedoucí interního auditu (CAE) by se měl poradit s právním zástupcem. Zásady a postupy dané organizace mohou vyžadovat, aby konkrétní subjekty posoudily a schválily obchodní informace před jejich externím zveřejněním.

CAE může zavést další zásady, procesy a postupy, podle kterých útvar interního auditu a externí konzultanti musí postupovat; typicky jsou sladěny se Závaznými směrnicemi IPPF. Interní auditoři by se měli řídit zásadami a postupy stanovenými danou organizací a CAE, a také být v souladu se všemi souvisejícími zákony a regulatorními požadavky.

Z hlediska ochrany obchodních informací vlastněných organizací, mohou zásady a postupy od interních auditorů vyžadovat, aby se řídili následujícími preventivními opatřeními, a to dokonce i v případě, kdy s těmito informacemi nakládají interně:

- Shromažďovat pouze data vyžadovaná pro provedení přidělené zakázky a využívat tyto informace pouze pro účely zakázky.
- Chránit informace před úmyslným nebo neúmyslným zveřejněním prostřednictvím kontrolních a řídicích mechanismů jako je kódování dat, omezení emailové distribuce a omezení fyzického přístupu k informacím.
- Odstranění kopií dat nebo přístupu k nim v případě, že již nejsou potřebné.

Jedním z příkladů informací, které jsou většinou chráněny před interním zveřejněním, jsou osobní data týkající se lidských zdrojů; například výše mzdy a záznamy o kárném řízení nebo personálních problémech, které byly diskutovány s vedoucími a pracovníky oddělení lidských zdrojů. Přístup k těmto informacím může být omezen nebo monitorován prostřednictvím fyzických kontrolních a řídicích mechanismů, jako jsou uzamčené archivní skříně a prostřednictvím kontrolních a řídicích mechanismů informačního systému, včetně ochrany prostřednictvím hesla a kódování dat. CAE by měl pravidelně hodnotit a potvrzovat potřebu přístupu interních auditorů k oblastem a databankám, které obsahují důvěrné informace, a měl by potvrdit, že kontrolní a řídicí mechanismy týkající se přístupu fungují účinně.

Prováděcí standardy, které doprovázejí Standard 2330 – Dokumentace informací, vyžadují, aby CAE řídil přístupy k záznamům o zakázce, částečně stanovením požadavků na archivaci záznamů, bez ohledu na nosné médium. Tato pravidla musí být v souladu se směrnicemi dané organizace a ostatními souvisejícími regulatorními nebo jinými požadavky.

Dále, Standard 2440.A2 vyžaduje, aby CAE ohodnotil možné riziko zveřejnění výsledků ujišťovací zakázky a omezil užívání výsledků ujišťovací zakázky, s výjimkou případů vyžadovaných zákony, nařízeními a regulatorními požadavky. Zprávy ze zakázky většinou obsahují distribuční seznamy, které jsou společně schvalovány CAE, vedením a orgány společnosti. Zahrnutí právních, statutárních a regulatorních požadavků ve *Standardech* zajišťuje, že CAE a interní auditoři mohou postupovat v souladu s požadavky regulátorů a v souladu se zákony týkajícími se transparentnosti v organizacích veřejného sektoru.

Školení

V průběhu schůzek nebo školení útvaru interního auditu CAE může vést diskusi na téma zásad, pravidel, opatření a očekávání souvisejících s důvěrností. Interní auditoři mohou využít této příležitosti k brainstormingu a diskuzi možného dopadu sdílení různých typů důvěrných informací dané organizace. CAE může vyžadovat, aby interní auditoři podepsali formulář, kterým potvrzují, že se zúčastnili těchto školení a že se seznámili se souvisejícími zásadami, postupy a očekáváními. Pro CAE, jako představitele útvaru interního auditu, je zvláště nezbytné, aby nastavil hodnotová měřítka etiky v rámci týmu tím, že bude sám prosazovat zásady a pravidla jednání obsažená v Etickém kodexu.

Jednotliví interní auditoři

V konečném důsledku jsou to jednotliví interní auditoři, kteří jsou odpovědní za svůj osobní soulad s Etickým kodexem. To je snad nejvíce patrné v souvislosti s prováděním zakázek interního auditu, v průběhu kterých interní auditoři mohou získávat důvěrné, obchodní a/nebo osobně ztotožnitelné informace. Interní auditoři mohou zacházet s těmito informacemi v průběhu zakázky (např. při sběru informací o činnosti, která je předmětem auditu, a v průběhu testování).

Podle Standardu 2330 – Dokumentace informací, interní auditoři musí dokumentovat dostatečné, spolehlivé, relevantní a účelné informace, aby podpořili výsledky zakázky a její závěry. Interní auditoři by měli zvážit

důvěrnost informací, když svou práci a pozorování dokumentují v pracovní dokumentaci zakázky a v závěrečné zprávě. Pracovní program nebo předlohy pracovní dokumentace zakázky mohou obsahovat připomenutí týkající se důvěrnosti; elektronické formáty mohou obsahovat automatizované kontrolní a řídicí mechanismy, které od interních auditorů vyžadují, aby potvrdili souhlas s těmito připomenutími předtím, než mohou přistoupit k pracovní dokumentaci a než ji mohou zkompletovat.

Několik standardů souvisejících s plánováním a prováděním zakázek konkrétně zmiňuje obezřetné používání a ochranu informací, jak je popsáno v Pravidle 3.1. Interní auditoři při plánování ujišťovací zakázky zahrnující třetí strany musí získat písemný souhlas s omezeními vztahujícími se k distribuci výsledků zakázky a k přístupům k záznamům o zakázce (Standard 2201.A1). Při předání výsledků ujišťovací zakázky subjektům mimo organizaci, interní auditoři musí smluvně stanovit omezení, jakým způsobem mohou být výsledky distribuovány využívány (Standard 2410.A3).

Aby interní auditoři byli v souladu s pravidly jednání souvisejícími se zásadou důvěrnosti, musí postupovat dle stanovených postupů pro zveřejňování, včetně kontaktování správné organizační úrovně v dané organizaci pro schválení zveřejnění jakékoliv informace. Interní auditoři mohou tento požadavek realizovat prostřednictvím získání písemného povolení, které archivují v pracovní dokumentaci.

A v poslední řadě, Pravidlo jednání 3.2 zdůrazňuje, že interní auditoři nesmí využít jakoukoli informaci pro osobní prospěch. Například interní auditoři by neměli využívat vnitřní finanční, strategické, nebo provozní znalosti organizace k získání osobního finančního prospěchu nákupem nebo prodejem akcií dané organizace. Dalším příkladem je předání vnitřních informací novinářům nebo prostřednictvím ostatních médií bez odpovídajícího schválení. Využití vnitřních informací pro vývoj konkurenčního produktu nebo prodej specifických obchodních informací konkurenci také porušuje toto pravidlo důvěrnosti. Dále by interní auditoři neměli zneužívat svá privilegovaná oprávnění k přístupu k informacím, jako je využívání přístupů k záznamům zákazníků, aby se podívali na nedávné nákupy svého souseda nebo si prohlíželi zdravotní záznamy veřejně známé osoby.

Přístupy využívané pro prokázání souladu

Vedoucí interního auditu

CAE může prokázat podporu důvěrnosti interního auditu prostřednictvím předložení zásad, procesů, postupů a školících materiálů realizovaných z důvodu zajištění důvěrnosti v podobě, jaká je vhodná pro daný útvaru interního auditu a danou organizaci. Zápisy ze schůzek a/nebo školení, kde byla důvěrnost diskutována s členy útvaru interního auditu, také prokazují činnost CAE směřující k podpoře souladu.

V oblasti zveřejňování výsledků zakázky, zpráv nebo souvisejících informací, CAE prokazuje soulad se zásadou důvěrnosti a pravidly jednání dokumentováním a archivací záznamů o zveřejněních schválených vedením a orgány společnosti a právním poradcem, pokud je právní hledisko na místě. CAE prokazuje řízení přístupu k záznamům pomocí dokumentace a komunikace zásad a postupů interního auditu a prostřednictvím

zavádění mechanismů, které omezují přístup a snižují riziko obejití nebo jiného porušení těchto řídicích a kontrolních mechanismů.

Jednotliví interní auditoři

Záznamy o účasti na školeních týkající se důvěrnosti by měly být archivovány spolu s podpisy interních auditorů potvrzujícími jejich seznámení se s důvěrností a se souvisejícími zásadami, postupy, zákony a regulatorními požadavky. Hodnocení výkonnosti interních auditorů také mohou zahrnovat zpětnou vazbu o tom, zda interní auditoři postupovali v souladu se zásadami a postupy souvisejícími s důvěrností a zveřejňováním informací.

Interní auditoři prokazují soulad s požadavkem důvěrnosti záznamů ze zakázky tím, že dokumentují omezení distribuce v pracovní dokumentaci zakázky a uchovávají schválení všech zveřejnění a schválených distribučních seznamů. Podepsaná prohlášení potvrzující, že s informacemi souvisejícími se zakázkou bylo zacházeno jako s důvěrnými, mohou být zahrnuta v pracovním programu.

Pokud neexistují žádné zprávy nebo vyšetřování jednotlivých interních auditorů kvůli porušení zásad, postupů a pravidel souvisejících s důvěrností, potom je pravděpodobné, že útvar interního auditu jako celek je v souladu s touto zásadou.

Uplatnitelnost a vymahatelnost etického kodexu

Interní auditoři si jsou vědomi, že Etický kodex se vztahuje jak na organizační útvary, tak na jednotlivce, kteří poskytují služby interního auditu. V případě členů IIA, držitelů nebo uchazečů o profesní certifikace IIA, porušení Etického kodexu budou vyhodnocena a následně bude postupováno dle Stanov a Administrativních směrnic IIA. Neuvedení určitého druhu jednání v Pravidlech jednání nevylučuje, aby takové jednání bylo považováno za nepřijatelné nebo diskreditační. Proto se člen, držitel certifikace nebo uchazeč o ni mohou stát subjektem disciplinární akce, která se vztahuje k jednání, které není explicitně definováno v Pravidlech jednání.

O Institutu

The Institute of Internal Auditors (The IIA) je nejvíce uznávanou autoritou, vzdělávací institucí a poskytovatelem standardů, doporučení a certifikací pro profesi interního auditu. Založen v roce 1941. The IIA dnes poskytuje servisní služby pro více než 190 000 členů ve více než 170 zemích a teritoriích. Globální centrála organizace sídlí v Lake Mary, Fla. Pro další informace navštivte www.globaliia.org.

O Prováděcích směrnicích

Prováděcí směrnice, které jsou součástí Mezinárodního rámce profesní praxe IIA® (IPPF®), poskytují Doporučené pokyny (nepovinné) pro profesi interního auditu. Jsou navrženy s cílem napomáhat jak interním auditorům, tak útvarům interního auditu při zdokonalování svých schopností dosahovat soulad s *Mezinárodními standardy pro profesní praxi interního auditu.*

Prováděcí směrnice popisují přístupy a činnosti, které mohou být využity pro zavedení Závazných směrnic IIA., ale neposkytují podrobný popis programů, procesů, postupů nebo nástrojů.

Závazné směrnice poskytované IIA jsou dostupné na naší webové stránce www.globaliia.org/standards-guidance

Prováděcí směrnice přeložené do českého jazyka jsou dostupné na webu Českého institutu interních auditorů www.interniaudit.cz.

O Etickém kodexu IIA

Etický kodex IIA se skládá ze dvou významných částí:

- Čtyř základních zásad pro profesi a praxi interního auditu.
- Pravidel jednání stanovených pro každou ze základních zásad, která popisují normy chování očekávaného od interních auditorů.

Cílem Etického kodexu IIA je podpora etické kultury v profesi interního auditu.

Úplné znění Etického kodexu je k dispozici na https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx.

Omezení odpovědnosti

IIA publikuje tento dokument pro informační a vzdělávací účely. Tento pomocný materiál není určen pro nalezení rozhodujících odpovědí na konkrétní individuální situaci. IIA doporučuje ve všech případech specifických situací vyhledat radu nezávislého odborníka. IIA nepřijímá žádnou odpovědnost za situace, kdy je výhradně spoléháno na tyto směrnice.

Copyright