Kybernetická bezpečnost

Tematické požadavky

Topical Requirement

Uživatelská příručka

The Institute of
Internal Auditors

Obsah

Přehled Tematických požadavků

Tematické Požadavky, spolu s Globálními standardy interního auditu™ a Globálními návody tvoří základní součást Mezinárodního rámce profesní praxe®. Institut interních auditorů požaduje, aby se Tematické požadavky používaly ve spojení s Globálními standardy interního auditu, které poskytují autoritativní základ pro požadované postupy interního auditu. Odkazy na Standardy jsou v této příručce uvedeny průběžně jako zdroj podrobnějších informací.

Tematické požadavky formalizují způsob, jakým způsobem interní auditoři přistupují k převládajícím rizikovým oblastem, a tím podporují kvalitu a konzistentnost v rámci profese. Stanovují základ a poskytují relevantní kritéria pro provádění ujišťovacích služeb vztahujících se k předmětu Tematických požadavků (Standard 13.4 Hodnotící kritéria). Soulad s Tematickými požadavky je povinný pro ujišťovací služby a doporučená pro hodnocení poradenských služeb. Tematické požadavky nemají za cíl pokrýt všechny možné aspekty, které by měly být při provádění ujišťovacích zakázek zvažovány; jejich hlavním účelem je spíše stanovit minimální soubor požadavků, které umožní konzistentní a spolehlivé posouzení daného tématu.

Tematické požadavky jasně odkazují na Model tří linií IIA a na Globální standardy interního auditu. Řízení a správa společnosti, řízení rizik a kontrolní procesy tvoří hlavní složky Tematických požadavků, které jsou v souladu se Standardem 9.1 Porozumění procesům a správy společnosti, řízení, řízení rizik a řídicím a kontrolním procesům. Model tří linií řadí řízení a správu společnosti pod orgány společnosti, řízení rizik pod druhou linii a kontroly a kontrolní procesy pod první linii. Zatímco vedení má zastoupení v první i druhé linii, útvar interního auditu je umístěn ve třetí linii jako nezávislý a objektivní poskytovatel ujištění, který je přímo podřízen orgánům společnosti (Princip 8 Dohled orgánů společnosti).

Použitelnost, riziko a odborný úsudek

Tematické požadavky je nutné dodržovat, když útvar interního auditu provádí ujišťovací zakázky týkající se oblastí, pro která Tematické požadavek existují, nebo pokud jsou prvky Tematických požadavků identifikovány v rámci jiných ujišťovacích zakázek.

Jak je uvedeno ve Standardech, hodnocení rizik je důležitou součástí plánování vedoucího auditora. Určení ujišťovacích zakázek, které mají být zahrnuty do plánu interního auditu, vyžaduje alespoň jednou ročně posoudit strategie, cíle a rizik organizace (Standard 9.4 Plán interního auditu). Při plánování jednotlivých ujišťovacích zakázek musí interní auditoři vyhodnotit rizika relevantní pro danou zakázku (Standard 13.2 Hodnocení rizik zakázky).

Pokud je oblast Tematických požadavků identifikována během procesu plánování interního auditu s ohledem na rizika a je zahrnuto do plánu auditu, je nutné při posuzování daného tématu v příslušných zakázkách uplatnit požadavky uvedené v Tematických požadavcích. Dále, pokud interní auditoři při provádění zakázky (bez ohledu na to, zda je součástí plánu) a narazí na prvky Tematických požadavků, musí tento požadavek posoudit z hlediska jeho relevance pro danou zakázku. Nakonec, pokud je vyžádána zakázka, která původně nebyla v plánu auditu a týká se daného tématu, je třeba posoudit, zda je v daném kontextu použitelný.

Při uplatňování Tematických požadavků hraje klíčovou roli odborný úsudek. Hodnocení rizik je podkladem pro rozhodování vedoucích pracovníků auditu o tom, které zakázky zahrnout do plánu interního auditu (Standard 9.4 Plán interního auditu). Vedle toho interní auditoři využívají odborný úsudek k určení, které aspekty budou v rámci každé zakázky zahrnuty (Standardy 13.3 Cíle a rozsah zakázky, 13.4 Hodnotící kritéria a 13.6 Pracovní program). Příloha A "Příklady praktického použití" popisuje, jak interní auditoři určují, zda se na ně vztahují Tematické požadavky.

Musí být zachovány důkazy o tom, že každý požadavek v Tematických požadavcích byl posouzen z hlediska použitelnosti, včetně odůvodnění, které vysvětluje vyloučení jakýchkoli požadavků. Soulad s Tematickými požadavky musí být zdokumentován s využitím odborného úsudku auditora, jak je popsáno ve Standardu 14.6 Dokumentace zakázky.

Zatímco Tematické požadavky kybernetické bezpečnosti poskytují základní rámec kontrolních procesů, které je třeba zvážit, organizace, které hodnotí kybernetické riziko jako velmi vysoké, mohou potřebovat posoudit další aspekty.

Pokud vedoucí interního auditu rozhodne, že útvar interního auditu nemá potřebné znalosti k provádění auditních zakázek na téma Tematických požadavků, může být práce na zakázce zadána externě (Standardy 3.1 Kompetentnost, 7.2 Kvalifikace vedoucího interního auditu, 10.2 Řízení lidských zdrojů). Ani v takovém případě outsourcing nezbavuje útvar interního auditu odpovědnosti za dodržování Tematických požadavků. Konečnou odpovědnost za zajištění souladu si ponechává vedoucí interního auditu. Navíc pokud vedoucí auditor rozhodne, že zdroje interního auditu jsou nedostatečné, musí informovat orgány společnosti o dopadu nedostatečných zdrojů a způsobu řešení jejich případného nedostatku (Standard 8.2 Zdroje).

Výkon, dokumentace a podávání zpráv

Při uplatňování Tematických požadavků musí interní auditoři rovněž dodržovat standardy a vykonávat svou práci v souladu s Doménou V: Provádění služeb interního auditu. Standardy v Doméně V popisují plánování zakázek (Princip 13 Plánujte zakázky účinně), provádění zakázek (Princip 14 Realizujte zakázku řádně) a komunikaci výsledků zakázek (Princip 15 Komunikujte závěry zakázky a monitorujte akční plány).

Zahrnutí Tematických požadavků lze zdokumentovat buď v plánu interního auditu, nebo v pracovních dokumentech zakázky, a to na základě odborného úsudku auditora. Jedna nebo více zakázek interního auditu může pokrýt dané požadavky. Navíc nemusí být všechny požadavky vždy použitelné. Musí být zachovány důkazy o tom, že Tematické požadavky

byly posouzeny z hlediska použitelnosti, včetně odůvodnění vysvětlujícího případné vyloučení.

Volitelný nástroj v příloze C lze použít jako referenci a k dokumentaci práce interních auditorů.

Zajištění kvality

Standardy vyžadují, aby vedoucí auditu vypracoval, implementoval a udržoval program pro zajišťování a zvyšování kvality, který pokrývá všechny aspekty funkce interního auditu (Standard 8.3 Kvalita). Výsledky musí být sděleny orgánům společnosti a vrcholovému vedení, které musí být informováno o souladu útvaru interního auditu se Standardy a o dosažení výkonnostních cílů.

Soulad s Tematickými požadavky bude hodnocen v rámci posuzování kvality. Pro přípravu na hodnocení kvality mohou interní auditoři využít nástroj uvedený v příloze C.

Kybernetická bezpečnost

Kybernetická bezpečnost je rozsáhlé téma, které se týká většiny technologických aspektů jakékoli organizace. Kromě informačních technologií je kybernetická bezpečnost běžně součástí podnikových procesů, což vyžaduje, aby interní auditoři posuzovali rizika související s kybernetickou hrozbami při plánování, stanovování rozsahu a provádění ujišťovacích zakázek.

Národní institut pro standardy a technologie (NIST), který spadá pod americké ministerstvo obchodu, definuje kybernetickou bezpečnost jednoduše jako "schopnost chránit nebo bránit využívání kybernetického prostoru před kybernetickými útoky". Tematické požadavky kybernetické bezpečnosti se zaměřují na vnější ochranu, kterou organizace zabezpečují, aby zmírnily rizika spojená s neoprávněnými uživateli a škodlivými kybernetickými hrozbami. Kybernetická bezpečnost je podmnožinou širšího konceptu informační bezpečnosti, kterou NIST definuje jako "ochranu informací a informačních systémů před neoprávněným přístupem, použitím, zveřejněním, narušením, změnou nebo zničením za účelem zajištění důvěrnosti, integrity a dostupnosti".

Požadavky Tematických požadavků kybernetické bezpečnosti zahrnují:

- Řízení a správa – jasně definované základní cíle a strategie kybernetické bezpečnosti, které podporují cíle, zásady a postupy organizace.
- Řízení rizik – procesy pro identifikaci, analýzu, řízení a monitorování kybernetických hrozeb, včetně procesu pro rychlou eskalaci kybernetických rizik.
- Kontroly – vedením stanovené kontrolní procesy, které jsou pravidelně hodnoceny za účelem zmírnění kybernetických rizik.

Přístupy

Interní auditoři mohou využít následující přístupy k podpoře při posuzování požadavků uvedených v rámci Tematických požadavků kybernetické bezpečnosti. Tyto přístupy, které odkazují na příslušné požadavky, jsou ilustrativní, ale nejsou závazné. Interní auditoři by se měli při rozhodování o tom, co zahrnout do svého hodnocení, opírat o odborný úsudek.

Přístupy k řízení a správě

Pro posouzení, jak jsou procesy řízení a správy aplikovány na cíle kybernetické bezpečnosti, mohou interní auditoři přezkoumat:

A. Formalizovaný a zdokumentovaný strategický plán a cíle kybernetické bezpečnosti, včetně důkazů o tom, že orgány společnosti pravidelně (zpravidla čtvrtletně) přezkoumávají aktualizace kybernetické bezpečnosti poskytované vedoucím funkce informační bezpečnosti, například ředitelem pro informační bezpečnost (CISO). Důkazy mohou zahrnovat zprávy o:
   - Monitorování dosažení strategických cílů.
   - Rozpočtové potřeby pro podporu cílů a úkolů kybernetické bezpečnosti.
   - Zaměření na rizika a vnitřní kontroly, včetně pokroku v nápravných opatřeních.
   - Klíčové ukazatele výkonnosti (KPI) k měření úspěšnosti.
   - Lidské zdroje potřebné k náboru, školení a rozvoji odborníků na kybernetickou bezpečnost.

B. Zásady, postupy a další příslušnou dokumentaci používaná k řízení procesů kybernetické bezpečnosti, včetně:
   - Zásad, které jsou přezkoumávány a aktualizovány alespoň jednou ročně. Nově vznikající kybernetická rizika mohou vyžadovat častější revize a aktualizace.
   - Procesu posuzování, zda jsou zásady a postupy dostatečné pro podporu operací v oblasti kybernetické bezpečnosti.
   - Široce přijímaných rámců (NIST, COBIT a dalších) k posílení procesů kybernetické bezpečnosti a vnitřních kontrol.

C. Role a odpovědnosti podporující dosažení cílů kybernetické bezpečnosti, včetně struktury zajišťující, že funkce kybernetické bezpečnosti podává hlášení na takové úrovni organizace, která má dostatečný přehled k dosažení organizační podpory.
   - Proces pravidelného hodnocení znalostí, dovedností a schopností pracovníků zastávající role v oblasti kybernetické bezpečnosti.

D. Důkazy o zapojení relevantních zainteresovaných subjektů (například vrcholového vedení, provozu, řízení rizik, lidských zdrojů, právního oddělení, compliance, strategických dodavatelů a dalších), včetně komunikace o stávajících a vznikajících kybernetických rizicích a známých potenciálních zranitelnostech. Důkazy o komunikaci mohou zahrnovat zápisy z jednání, zprávy anebo e-maily.

Přístupy k řízení rizik

Pro posouzení, jak jsou procesy řízení rizik aplikovány na cíle kybernetické bezpečnosti, mohou interní auditoři přezkoumat:

A. Jak organizace hodnotí a řídí kybernetická rizika, včetně způsobu, jakým jsou hrozby a zranitelnosti:
   - Nejprve identifikovány a hlášeny.
   - Analyzovány za účelem vyhodnocení rizik pro dosažení cílů organizace.
   - Zmírněny, včetně akčních plánů ke snížení rizika na přijatelnou úroveň.
   - Sledovány, včetně plánu pro průběžné reportování až do úplného odstranění hrozeb.

B. Jak organizace získává pravidelnou informaci o řízení rizik kybernetické bezpečnosti od funkčních oblastí, jako jsou informační technologie, řízení podnikových rizik, lidské zdroje, právní oddělení, oddělení compliance, provoz, účetnictví a finance. K získávání informací může být využit mezioborový tým pro kybernetickou bezpečnost nebo řídicí výbor pro IT.

C. Jak organizace přidělila odpovědnost za řízení kybernetických rizik jednotlivci nebo týmu.
   - Odpovědné osoby by měly pravidelně (čtvrtletně, měsíčně nebo podle potřeby) komunikovat aktuální informace o kybernetických rizicích napříč organizací a mohou také zahrnout požadavky na zdroje pro strategie zmírňování rizik.

D. Eskalační procesy pro kybernetická rizika, včetně způsobu, jakým jsou úrovně hrozeb nebo rizik vyhodnocovány, přiřazovány a prioritně řazeny. Přezkum může zahrnovat identifikaci:
   - Úrovně rizik definované organizací – například vysoké, střední a nízké – s podrobným vysvětlením každé úrovně rizika a postupů eskalace pro jednotlivé kategorie rizik.
   - Seznamu aktuálně identifikovaných kybernetických rizik a stavu jejich zmírnění.
   - Příslušných právních, regulačních a compliance požadavků.
   - Jak finančních, tak nefinančních dopadů rizik (například reputační).

E. Proces komunikace kybernetických rizik vedení a zaměstnancům, který zahrnuje:
   - Pravidelná (alespoň jednou ročně) školení zaměstnanců v oblasti kybernetické bezpečnosti, například neohlášené simulované phishingové kampaně k testování a sledování povědomí organizace.
   - Aktualizace k nápravě stávajících problémů v oblasti kybernetické bezpečnosti s předpokládanými daty dokončení.
   - Sledování nedodržování předpisů, které zahrnuje informování orgánů společnosti a vrcholového vedení.

- Přehodnocení hrozeb v případě změny přístupu organizace k riziku a tolerance vůči rizikům.

F. Procesy zavedené organizací pro reakci na incidenty a obnovu, které zahrnují:

- Zdokumentovaný plán, který je přezkoumáván a aktualizován v závislosti na změnách v provozu organizace. Plán by měl zahrnovat:
  - Způsob detekce a oznamování incidentů.
  - Způsob izolace incidentů za účelem zamezení dalším škodám.
  - Způsob, jakým bude organizace reagovat a obnovovat provoz.
  - Způsob analýzy incidentu s cílem poučit se a zabránit opakování podobných událostí v budoucnu.
- Pravidelné testování (alespoň jednou ročně), například formou simulace krizového řízení (tabletop cvičení), a předávání výsledků vrcholovému vedení a relevantním zainteresovaným subjektům. Testování může vést k vytvoření akčních plánů.

Přístupy k řídicím a kontrolním procesům

Pro posouzení toho, jak jsou kontrolní procesy aplikovány na cíle kybernetické bezpečnosti, mohou interní auditoři přezkoumat:

A. Přístup vedení k budování účinného prostředí vnitřní kontroly kybernetické bezpečnosti, včetně:

- Posouzení a zavedení vnitřních kontrol potřebných k mitigaci zvýšených rizik a k ochraně citlivých, kritických, osobních nebo důvěrných dat, vycházející z procesu hodnocení rizik organizace.
- Stanovení požadavků na zdroje k udržení klíčových kontrol kybernetické bezpečnosti.
- Zohlednění kontrol dodavatelů jako součást kontrolního prostředí, včetně přezkoumání zpráv o kontrolách poskytovatelů služeb (SOC) před navázáním obchodního vztahu a v jeho průběhu.
- Pravidelné testování funkčnosti kontrol kybernetické bezpečnosti s cílem snižování rizik dosažení stanovených cílů kybernetické bezpečnosti.
- Proces nápravy nedostatků interních kontrol nebo řešení zjištění z hodnocení provedených interním auditem nebo jinými poskytovateli ujištění (například penetračním testováním).

B. Proces řízení talentů v organizaci při náboru a vzdělávání odborníků na kybernetickou bezpečnost, včetně způsobu, jakým organizace identifikuje příležitosti ke zvýšení kompetencí těchto specialistů s cílem podpořit technické znalosti a zvýšit povědomí o nových hrozbách.

- Příkladem může být účast na školeních, zapojení do skupin sdílejících znalosti a kontinuální profesní vzdělávání, včetně získávání certifikací v oblasti kybernetické bezpečnosti.

C. Proces řízení identifikace, prioritizace, monitorování a reportování nově vznikajících kybernetických hrozeb a zranitelností, který probíhá kontinuálně a zaměřuje se na každodenní provoz. Přezkum může zahrnovat ověření, zda byly zavedeny procesy pro posouzení hrozeb a zranitelností souvisejících s novými či nastupujícími technologiemi, například využitím umělé inteligence.

D. Procesy a kontrolní mechanismy zavedené vedením za účelem správy a ochrany majetku IT v průběhu celého životního cyklu, včetně výběru, používání, údržby a vyřazování hardwaru, softwaru a služeb dodavatelů. Hardware zahrnuje servery, síťová zařízení (např. směrovače nebo firewally), stolní počítače, notebooky, mobilní telefony, tablety a periferní zařízení. Software zahrnuje operační systémy (např. Windows), software pro plánování podnikových zdrojů, aplikace, antivirové programy a další. Hardware a software může zahrnovat:
   - Používání šifrování, antivirového softwaru, správy mobilních zařízení, požadavků na složitá hesla, virtuální privátní sítě (VPN)/sítě s nulovou důvěrou (ZTN) pro ověřování a pravidelnou aktualizaci firmwaru.
   - Proces správy majetku, který zajišťuje, že hardware vydaný společností má při vydání vhodnou konfiguraci zabezpečení a při vyřazení majetku je řádně zlikvidován.
   - Kontroly související s databázemi, které zahrnují omezení přístupu uživatelů a správců, zajištění používání šifrování, zálohování a testování databází a přítomnost silných kontrol zabezpečení sítě.
   - Jak se v životním cyklu vývoje systému (SDLC) zohledňují kybernetické bezpečnostní hrozby nebo zranitelnosti.
   - Přístup používaný vývojovými, bezpečnostními a provozními odděleními (DevSecOps) k zajištění toho, aby proces vývoje softwaru zahrnoval kybernetickou bezpečnost a proaktivně identifikoval zranitelnosti.

E. Procesy používané k posílení kybernetické bezpečnosti, včetně:
   - Konfigurace nastavení zabezpečení pro minimalizaci rizika kybernetické bezpečnosti.
   - Správa mobilních zařízení (včetně používání e-mailu a aplikací) je nakonfigurována tak, aby se snížila rizika kybernetické bezpečnosti a aby ji bylo možné spravovat na dálku, pokud je zařízení uživatele ohroženo.
   - Použití šifrování pro data "v klidu", jako jsou informace uložené na pevném disku, nebo pro data "při přenosu", jako je šifrování e-mailů.
   - Záplatování serverů nebo softwaru (například operačního systému) nejnovějšími verzemi zabezpečení.

- Správa přístupu uživatelů, například používání vícefaktorového ověřování (MFA) a jedinečných uživatelských ID se složitými hesly, jejichž platnost pravidelně vyprší.
- Zavedené kontrolní mechanismy pro sledování, zda dostupnost a využití zdrojů fungují odpovídajícím způsobem, což umožňuje přezkoumání a analýzu potenciálních problémů kybernetické bezpečnosti, které ohrožují výkonnost.
- Integrace kybernetické bezpečnosti do procesu SDLC s cílem identifikovat a řešit zranitelná místa kybernetické bezpečnosti ještě před uvedením softwaru do výroby.

F. Kontroly související se sítí, které zabezpečují perimetr organizace, včetně způsobu, jakým organizace využívá:
   - Segmentace sítě.
   - Firewally.
   - Kontrola přístupu uživatele.
   - Omezení externích i interních připojení.
   - Řízení internetu věcí (IoT) pro propojené sítě.
   - Systémy detekce a prevence narušení, které zabraňují kybernetickým bezpečnostním útokům, odhalují je a zotavují se z nich.

G. Kontroly týkající se kontroly zabezpečení koncových komunikačních bodů, které se vztahují na služby, jako je e-mail, internetové prohlížeče, videokonference, zasílání zpráv (Zoom, MS Teams a další), sociální média, cloud a protokoly pro sdílení souborů. Kontroly mohou zahrnovat omezení používání určitých přípon souborů (například souborů .exe) a vícefaktorovou autentizaci pro sdílení souborů.

Příloha A. Příklady praktického použití

Následující příklady popisují scénáře, ve kterých by se Tematické požadavky kybernetické bezpečnosti uplatnily:

Příklad 1: Kybernetická bezpečnost je součástí zakázky interního auditu zahrnuté do plánu interního auditu.

Pokud útvar interního auditu dokončí svůj proces plánování založený na rizicích a zahrne do plánu interního auditu jednu nebo více zakázek týkajících se kybernetické bezpečnosti, je při provádění těchto zakázek povinen dodržovat Tematické požadavky. Souladu lze dosáhnout zahrnutím požadavků napříč jednou nebo více zakázkami v plánu interního auditu.

Kybernetická bezpečnost je široké téma, a ne každý požadavek v Tematických požadavcích se uplatní v každé zakázce. Pokud interní auditoři použijí odborný úsudek a rozhodnou, že jeden nebo více požadavků Tematických požadavků na kybernetickou bezpečnost nejsou použitelné, a proto by měly být ze zakázky vyloučeny, musí interní auditoři zdokumentovat a uchovat odůvodnění vyloučení těchto požadavků. Odůvodněním pro vyloučení některých požadavků může být například to, že útvar interního auditu provádí různé zakázky v oblasti kybernetické bezpečnosti na rotačním principu nebo že určil, že významnost rizika v dané zakázce je nízká.

Příklad 2: Rizika kybernetické bezpečnosti jsou identifikována během auditní zakázky, která není zaměřena na kybernetickou bezpečnost.

Interní auditoři mohou identifikovat rizika v oblasti kybernetické bezpečnosti při posuzování procesu, který s kybernetickou bezpečností přímo nesouvisí. Interní auditoři mohou například posuzovat proces placení závazků v rámci zakázky, která není zaměřena na kybernetickou bezpečnost, a při plánování zakázky neidentifikují rizika kybernetické bezpečnosti jako součást jejího rozsahu. Po úvodním zmapování procesních postupů (walk-through) však interní auditoři zjistí, že by tato rizika měla být v rozsahu zakázky; například identifikují rizika kybernetické bezpečnosti související s webovým podáním prvotní žádosti o objednávku (Standard 13.2 Hodnocení rizik zakázky).

Po identifikaci relevantních rizik musí interní auditoři přezkoumat Tematické požadavky kybernetické bezpečnosti a určit, které požadavky z nich jsou relevantní. V tomto příkladu mohou vyloučit proces řízení kybernetické bezpečnosti nebo proces řízení rizik kybernetické bezpečnosti. V pracovní dokumentaci k zakázce musí odůvodnit vyloučení daných požadavků Tematických požadavků na kybernetickou bezpečnost a dokumentaci si uschovat.

Příklad 3: Je požadována zakázka v oblasti kybernetické bezpečnosti, která původně nebyla zahrnuta do plánu interního auditu.

Zainteresované subjekty, jako jsou orgány společnosti, vedení nebo regulační orgán mohou interní auditory požádat, aby provedli posouzení kybernetické bezpečnosti mimo původní plán auditu. Například když se organizace stane terčem kybernetického útoku, mohou orgány společnosti požádat interní audit o posouzení řídicích a kontrolních mechanismů kybernetické bezpečnosti. Tematické požadavky se na tento případ vztahují, musí být posouzeny a případné výjimky zdokumentovány.

Příloha B. Mapování na rámce

Organizace může mít své vlastní programy v oblasti kybernetické bezpečnosti a používat rámce řízení rizik a správy, jako je COBIT nebo NIST. Interní auditoři již mohou mít na základě těchto rámců vypracované programy auditu a postupy testování. Interní auditoři by měli sladit své zamýšlené testování řídicích a kontrolních mechanismů kybernetické bezpečnosti s Tematickými požadavky, aby zajistili odpovídající pokrytí. Níže uvedená tabulka porovnává Tematické požadavky kybernetické bezpečnosti se třemi běžně používanými rámci: NIST Cybersecurity Framework 2.0, COBIT 2019 a NIST 800-53. Tyto rámce byly zahrnuty do mapování, protože jsou snadno a bezplatně dostupné.

Požadavky na řízení a správu společnosti	Rámcové odkazy		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Jsou stanoveny a pravidelně aktualizovány formální strategie a cíle kybernetické bezpečnosti. Aktuální informace o plnění cílů kybernetické bezpečnosti jsou pravidelně sdělovány a přezkoumávány orgány společnosti, a to i z hlediska zdrojů potřebných k plnění strategie kybernetické bezpečnosti.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Jsou zavedeny a pravidelně aktualizovány zásady a postupy týkající se kybernetické bezpečnosti s cílem posílit kontrolní prostředí.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. Jsou stanoveny role a odpovědnosti pro plnění cílů kybernetické bezpečnosti a existuje proces pravidelného hodnocení znalostí, dovedností a schopností osob, které tyto role zastávají.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Příslušné zainteresované subjekty jsou zapojeny do diskuse o existujících zranitelných místech a nových hrozbách v oblasti kybernetické bezpečnosti a jednají podle toho. Mezi zainteresované subjekty patří vrcholové vedení, provoz, oddělení řízení rizik, oddělení lidských zdrojů, právní oddělení, oddělení compliance, dodavatelé a další.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Požadavky na řízení rizik	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Procesy hodnocení a řízení rizik v organizaci zahrnují identifikaci, analýzu, zmírňování a monitorování hrozeb kybernetické bezpečnosti a jejich vlivu na dosažení strategických cílů.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Řízení rizik kybernetické bezpečnosti probíhá napříč celou organizací a může zahrnovat následující oblasti: informační technologie, systém korporátního řízení rizik, lidské zdroje, právní záležitosti, compliance, provoz, dodavatelský řetězec, účetnictví, finance a další.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Jsou stanoveny odpovědnosti v řízení rizik v oblasti kybernetické bezpečnosti, i kdo za ně plně zodpovídá. Je určena osoba nebo tým, který pravidelně monitoruje a podává zprávy o tom, jak jsou rizika kybernetické bezpečnosti řízena, a to i z hlediska zdrojů potřebných ke zmírnění rizik a identifikaci nových hrozeb kybernetické bezpečnosti.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. Je zaveden proces pro rychlou eskalaci jakéhokoli rizika kybernetické bezpečnosti (vznikajícího nebo již dříve identifikovaného), které dosáhne nepřijatelné úrovně podle zavedených směrnic pro řízení rizik nebo platných právních a regulačních požadavků. Měly by být zohledněny finanční i nefinanční dopady kybernetického bezpečnostního rizika.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Je zaveden proces pro informování vedení a zaměstnanců o rizicích kybernetické bezpečnosti a proces, podle kterého vedení pravidelně přezkoumává problémy, mezery, nedostatky nebo selhání řídicích a kontrolních mechanismů, je včas informováno a schopno zajistit nápravu.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Pro případ kybernetického bezpečnostního incidentu má organizace zavedený proces reakce a obnovy, který zahrnuje detekci incidentu, jeho zvládnutí, obnovu a analýzu po incidentu. Proces reakce a obnovy je pravidelně testován.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Požadavky na řídicí a kontrolní procesy	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Je zaveden proces, který zajišťuje zavedení interních kontrolních mechanismů i kontrolních mechanismů u dodavatelů, aby byla chráněna důvěrnost, integrita a dostupnost systémů a dat organizace. Pravidelně se provádí hodnocení, zda kontroly fungují způsobem, který podporuje dosahování cílů kybernetické bezpečnosti organizace a pohotové řešení problémů.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

B. Je zaveden proces řízení talentů, který zahrnuje školení pro rozvoj a udržování technických kompetencí souvisejících s operacemi kybernetické bezpečnosti. Tento proces je pravidelně přezkoumáván.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Je zaveden proces průběžného monitorování a hlášení vznikajících hrozeb a zranitelností v oblasti kybernetické bezpečnosti, který pomáhá identifikovat, prioritizovat a implementovat příležitosti ke zlepšení kybernetické bezpečnosti.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Kybernetická bezpečnost je zahrnuta do řízení životního cyklu (výběr, používání, údržba a vyřazení z provozu) všech prostředků IT, včetně hardwaru, softwaru a služeb dodavatelů.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. Jsou zavedeny procesy pro posílení kybernetické bezpečnosti, včetně konfigurace, správy zařízení koncových uživatelů, šifrování, bezpečnostního záplatování (patching), správy přístupu uživatelů a monitorování dostupnosti a výkonu. Kybernetická bezpečnost je zohledněna při vývoji softwaru (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Jsou zavedeny kontroly související se sítí, jako jsou kontroly přístupu k síti a segmentace, používání a umístění firewallů, omezení připojení z externích sítí a do nich, virtuální privátní sítě (VPN)/přístup k sítím s nulovou důvěryhodností (ZTNA), kontroly sítí internetu věcí (IoT) a systémy detekce/prevence narušení (IDS a IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. Pro služby, jako jsou e-mail, internetové prohlížeče, videokonference, zasílání zpráv, sociální média, cloud a protokoly pro sdílení souborů, jsou zavedeny kontroly zabezpečení koncových bodů (endpoint-communication).	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Příloha C. Volitelný dokumentační nástroj

Od interních auditorů se očekává, že při určování použitelnosti požadavků na základě posouzení rizik budou uplatňovat odborný úsudek a přiměřeně dokumentovat vyloučení některých požadavků. Tematické požadavky mohou být zdokumentovány v plánu interního auditu nebo v pracovní dokumentaci zakázky na základě odborného úsudku auditora. Požadavky se může pokrývat jedna nebo více zakázek interního auditu. Kromě toho, ne všechny požadavky musí být relevantní. Níže uvedený formulář poskytuje jednu z možností dokumentování souladu s Tematickými požadavky kybernetické bezpečnosti, jeho použití však není povinné.

Kybernetická bezpečnost – řízení a správa

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
A. Jsou stanoveny a pravidelně aktualizovány formální strategie a cíle kybernetické bezpečnosti. Aktuální informace o plnění cílů kybernetické bezpečnosti jsou pravidelně sdělovány a přezkoumávány orgány společnosti, a to i z hlediska zdrojů potřebných k plnění strategie kybernetické bezpečnosti.		
B. Jsou zavedeny a pravidelně aktualizovány zásady a postupy týkající se kybernetické bezpečnosti s cílem posílit kontrolní prostředí.		
C. Jsou stanoveny role a odpovědnosti pro plnění cílů kybernetické bezpečnosti a existuje proces pravidelného hodnocení znalostí, dovedností a schopností osob, které tyto role zastávají.		

Požadavek	Provedené pokrytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
D. Příslušné zainteresované subjekty jsou zapojeny do diskuse o existujících zranitelných místech a nových hrozbách v oblasti kybernetické bezpečnosti a jednají podle toho. Mezi zainteresované subjekty patří vrcholové vedení, provoz, oddělení řízení rizik, oddělení lidských zdrojů, právní oddělení, oddělení compliance, dodavatelé a další.		

Kybernetická bezpečnost – řízení rizik

Požadavek	Provedené krytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
A. Procesy hodnocení a řízení rizik v organizaci zahrnují identifikaci, analýzu, zmírňování a monitorování hrozeb kybernetické bezpečnosti a jejich vlivu na dosažení strategických cílů.		
B. Řízení rizik kybernetické bezpečnosti probíhá napříč celou organizací a může zahrnovat následující oblasti: informační technologie, systém korporátního řízení rizik, lidské zdroje, právní záležitosti, compliance, provoz, dodavatelský řetězec, účetnictví, finance a další.		
C. Jsou stanoveny odpovědnosti v řízení rizik v oblasti kybernetické bezpečnosti, i kdo za ně plně zodpovídá. Je určena osoba nebo tým, který pravidelně monitoruje a podává zprávy o tom, jak jsou rizika kybernetické bezpečnosti řízena, a to i z hlediska zdrojů potřebných ke zmírnění rizik a identifikaci nových hrozeb kybernetické bezpečnosti.		

Požadavek	Provedené krytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
D. Je zaveden proces pro rychlou eskalaci jakéhokoli rizika kybernetické bezpečnosti (vznikajícího nebo již dříve identifikovaného), které dosáhne nepřijatelné úrovně podle zavedených směrnic pro řízení rizik nebo platných právních a regulačních požadavků. Měly by být zohledněny finanční i nefinanční dopady kybernetického bezpečnostního rizika.		
E. Je zaveden proces pro informování vedení a zaměstnanců o rizicích kybernetické bezpečnosti a proces, podle kterého vedení pravidelně přezkoumává problémy, mezery, nedostatky nebo selhání řídicích a kontrolních mechanismů, je včas informováno a schopno zajistit nápravu.		
F. Pro případ kybernetického bezpečnostního incidentu má organizace zavedený proces reakce a obnovy, který zahrnuje detekci incidentu, jeho zvládnutí, obnovu a analýzu po incidentu. Proces reakce a obnovy je pravidelně testován.		

Kybernetická bezpečnost – řídicí a kontrolní procesy

Požadavek	Provedené krytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
A. Je zaveden proces, který zajišťuje zavedení interních kontrolních mechanismů i kontrolních mechanismů u dodavatelů, aby byla chráněna důvěrnost, integrita a dostupnost systémů a dat organizace. Pravidelně se provádí hodnocení, zda kontroly fungují způsobem, který podporuje dosahování cílů kybernetické bezpečnosti organizace a pohotové řešení problémů.		
B. Je zaveden proces řízení talentů, který zahrnuje školení pro rozvoj a udržování technických kompetencí souvisejících s operacemi kybernetické bezpečnosti. Tento proces je pravidelně přezkoumáván.		
C. Je zaveden proces průběžného monitorování a hlášení vznikajících hrozeb a zranitelností v oblasti kybernetické bezpečnosti, který pomáhá identifikovat, prioritizovat a implementovat příležitosti ke zlepšení kybernetické bezpečnosti.		
D. Kybernetická bezpečnost je zahrnuta do řízení životního cyklu (výběr, používání, údržba a vyřazení z provozu) všech prostředků IT, včetně hardwaru, softwaru a služeb dodavatelů.		

Požadavek	Provedené krytí nebo zdůvodnění vyloučení	Odkaz na dokumentaci
E. Jsou zavedeny procesy pro posílení kybernetické bezpečnosti, včetně konfigurace, správy zařízení koncových uživatelů, šifrování, bezpečnostního záplatování (patching), správy přístupu uživatelů a monitorování dostupnosti a výkonu. Kybernetická bezpečnost je zohledněna při vývoji softwaru (DevSecOps).		
F. Jsou zavedeny kontroly související se sítí, jako jsou kontroly přístupu k síti a segmentace, používání a umístění firewallů, omezení připojení z externích sítí a do nich, virtuální privátní sítě (VPN)/přístup k sítím s nulovou důvěryhodností (ZTNA), kontroly sítí internetu věcí (IoT) a systémy detekce/prevence narušení (IDS a IPS).		
G. Pro služby, jako jsou e-mail, internetové prohlížeče, videokonference, zasílání zpráv, sociální média, cloud a protokoly pro sdílení souborů, jsou zavedeny kontroly zabezpečení koncových bodů (endpoint-communication).		

O Institutu interních auditorů

Institut interních auditorů (The IIA) je mezinárodní profesní sdružení, které sdružuje více než 255 000 členů po celém světě a udělilo více než 200 000 certifikátů Certified Internal Auditor® (CIA®) po celém světě. IIA byla založena v roce 1941 a je celosvětově uznávána jako lídr v oblasti standardů, certifikací, vzdělávání, výzkumu a technického poradenství v profesi interního auditu. Více informací naleznete na www.theiia.org.

Odmítnutí odpovědnosti

IIA vydává tento dokument pro informační a vzdělávací účely. Cílem tohoto materiálu není poskytnout definitivní odpovědi na konkrétní individuální okolnosti a jako takový má sloužit pouze jako vodítko. IIA doporučuje vyhledat nezávislé odborné poradenství týkající se přímo konkrétní situace. IIA nepřebírá žádnou odpovědnost za to, že se někdo bude spoléhat pouze na tento materiál.

Autorská práva

únor 2025

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101