Analýza rizík pre nové technológie
Performing Risk Assessments of Emerging Technologies
VOLUME 6 | 2022 ISACA JOURNAL

Rozvíjajúce sa technológie predstavujú hlavné zdroje rizika a vzhľadom na ich zložitosť, sa ťažko posudzujú. Pri analýze rizík je potrebné zvážiť celkový pohľad na systémy, ktoré nové technológie sprevádzajú, aké je ich využitie a aká je súhra s inými technológiami. Využitie vznikajúcich technológií často závisí od priemyselného odvetvia, či podnik bude novú technológiu využívať sám, alebo bude na jej využití spolupracovať s inými podnikmi alebo predajcami. Tieto aspekty, ktoré nové technológie prinášajú, bývajú často zle pochopené, čo sťažuje porozumieť ich zraniteľnostiam a rizikám, vrátane rozsahu rizík a definovaniu opatrení na ich zmiernenie. Na stanovenie rizika je možné použiť niekoľko existujúcich spôsobov, je však dôležité úspešne implementovať nové technológie, pochopiť zložitosti spojené s posudzovaním rizika a uvedomiť si, že spoliehanie sa na jedinú metodiku predstavuje riziko.

Riziká nových technológií

Technológia je rozhodujúca pre mnohé priemyselné odvetvia, s ktorými sú priamo prepojené (napr. telekomunikácie), alebo tie na ktorých sú silne závislé (napr. bankovníctvo, medicína) a tiež tie, ktoré ich vo väčšej miere práve začínajú používať (napr. poľnohospodárstvo, pohostinské služby). S novými technológiami sa stretáme každý deň. Aby organizácie dosiahli svoje plné uplatnenie musia vedieť nové technológie posúdiť, nakoľko budú pre ich prevádzku výhodné. Kľúčom k rozlíšeniu výhod a nevýhod implementovania nových technológií je pochopenie rizík, ktoré prinášajú a nájdenie riešení ako ich zmierniť.

Problémy hodnotenia rizík nových technológií.

Nové technológie sú podľa definície pomerne nové. O ich vlastnostiach sa dá veľa dozvedieť - jednak z hľadiska požiadaviek na ich prevádzku a ich možných vplyvov v prípade, že nebudú funkčné tak, ako sa to od nich očakáva.

Predpovedanie možnosti takýchto zlyhaní je zložité, pretože nie sú historicky podložené. Potenciálne hrozby na nové technológie možno často predvídať, ale opatrenia potrebné na zabezpečenie prevádzky pred poruchami a úmyselnými útokmi môžu byť neznáme.

Riziko viacerých strán

Mnohé nové technológie sú nielen technologicky zložité, ale prinášajú so sebou aj problémy ako napr. potreba vzájomnej spolupráce s viacerými stranami, nejednoznačnosť regulačných opatrení, nedostatok vlastných prevádzkových skúseností a ich uplatnenie. Tieto činitele ovplyvňujú úspešnosť nasadenia a prevádzky nových technológií, a tým i schopnosť efektívne posúdiť ich riziko. Napríklad, technológia môže zahŕňať platformu s mnohými vzájomne prepojenými aplikáciami, kombináciu viacerých zúčastnených strán, z ktorých každá z nich ponúka určitú časť celkového systému (napr. Softvér ako služba [SaaS] poskytovaná spoločnosťou, ponúkanie obchodných služieb), alebo súkromný blockchain - distribuovanú účtovnú knihu organizácie ako uzavretú kryptograficky zabezpečenú databázu používanú konzorciom s viacerými uzlami a zdieľanými zodpovednosťami.

Organizácii môžu chýbať potrebné politiky a procesy pre vznikajúcu technológiu a nemusia byť pochopené úlohy a kontroly potrebné na riadenie rizík. Väčšina vznikajúcich technológií vyžaduje značné úsilie na ich pochopenie, získavanie poznatkov o tom, ako sú pre podnik dôležité.

Nové technológie si často vyžadujú nové znalosti, zručnosti a schopnosti, preto mnohé organizácie sa spoliehajú na externé strany na posúdenie ich vlastností, použitia, čo vedie k zvýšenému riziku vplyvom tretích strán. Napríklad, v automobilovom sektore výrobcovia hľadajú pre autá technologické podniky na dodávanie potrebného hardvéru a softvéru. To však predstavuje nové riziko, pretože ak budú s novou technológiou problémy, nie je jasné, kto je v konečnom dôsledku za stratu dôvery zodpovedný. Vyžaduje si to čas a námahu pochopiť úlohy zúčastnených strán a zahrnúť do zmlúv potrebné opatrenia.

Riziká a etapy prijatia novej technológie

Posúdenie vznikajúceho technologického rizika sa dá zistiť pomocou rôznych rozhodovacích kritérií zodpovedajúcich fázam prijatia novej technológie (Obrázok 1).

OBRÁZOK 1

Etapy rozhodovania o použití novej technológie

Etapy prijatia novej technológie	Znalosť organizácie o novej technológii	Potreba porozumenia	Požadovaný výsledok
Všeobecné obchodné úvahy	Doteraz nie	Výhody možného použitia, špecifické hrozby, kontroly a náklady	Potenciálna obchodná hodnota - prevažujú možné výhody nad nákladmi?
Prvý prípad použitia	Doteraz nie	Možnosti použitia, špecifické hrozby a potrebné kontroly, určenie odhadu nákladov	Určenie najlepšej možnosti pre dosiahnutie prospechu
Realizácia ďalších prípadov použitia	Obmedzené použitie	Stavať na počiatočných skúsenostiach a zvážiť, poznatky o novej technológii	Uspech pre každý prípad použitia
Integrácia so stratégiou postupného investovania, postupnej implementácie	Nejednotný, často nesúdržný pohľad	Najlepšia možnosť na dosiahnutie súladu stratégie s hrozbami, kontrolami, nákladmi a prínosmi	Dosiahnuť najväčšie výhody, úspory a zisk

Výber metodiky na hodnotenie rizík

Systémy na riadenie rizík boli vyvinuté na pomoc organizáciám pre riadenie prevádzky v súlade so stanovenými predpismi. Niektoré organizácie sa spoliehajú viac na kvantitatívne ohodnotenie účinkov používania nových technológií a kontrol. Pre vznikajúce technológie zatiaľ neexistuje žiadny spôsob ohodnotenia rizík, ale je tu možné použiť niektoré existujúce modely s rôznym stupňom úspechu v závislosti od štádia prijatej technológie a či ide o všeobecné alebo špecifické hodnotenie rizika (napr. kybernetická bezpečnosť). Niekoľko príkladov hodnotenia rizík zahŕňajú nasledovné metódy hodnotenia rizík a kontroly:

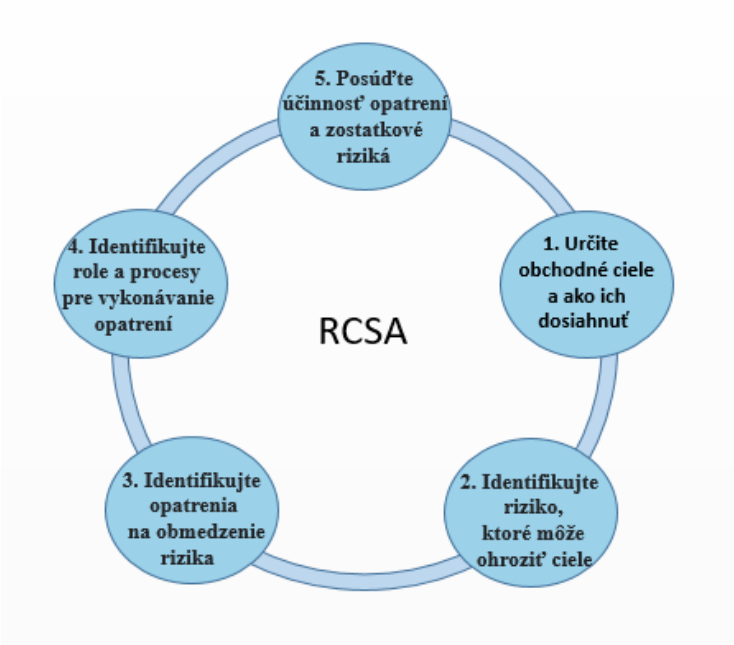
- Risk and Control Self-Assessment (RCSA),[2]
- Faktorová analýza informačného rizika (FAIR) - základná metodika hodnotenia rizík[3]
- KPMG Dynamické hodnotenie rizika.[4]

Tieto tri príklady je možné použiť ako východisko pre organizácie a podobne možno aplikovať aj iné metodiky.

Metodika RCSA

Mnohé organizácie prijímajú RCSA na analýzu operačného rizika. Táto metodika je tiež často používaná finančnými inštitúciami pri plnení regulačných požiadaviek na každoročné vlastné preskúmanie celopodnikového operačného rizika. Dá sa použiť aj ako metodika hodnotenia rizík dodávateľov tretích strán. Metodika RCSA zvyčajne pozostáva z piatich kľúčových prvkov zobrazených na Obrázku 2[5].

Obrázok č. 2



RCSA sa vo všeobecnosti vykonáva v organizácii pre každú obchodnú jednotku. Výsledky hodnotenia sa potom zhromažďujú a slúžia na komplexné vyjadrenie rizika v rámci celej organizácie. RCSA je užitočná na stanovenie vznikajúceho technologického rizika. Hlavnou slabinou RCSA pri riešení vznikajúceho technologického rizika je to, že zainteresované strany organizácie často nemajú dostatok

odbornosti alebo znalosti o novej technológii, a tým schopnosti identifikovať procesy a kontroly potrebné na zistenie ich slabých stránok.[6]

Zatiaľ nebola stanovená špeciálna metodika na hodnotenie rizík nových technológií, ale niektoré existujúce metódy môžu byť v závislosti od štádia osvojenia si technológie s rôznym stupňom úspechu použité na všeobecné resp. špecifické hodnotenie rizika.

Metodika FAIR

FAIR poskytuje model na pochopenie, analýzu a kvantifikáciu kybernetického a operačného rizika v podmienkach finančného sektora. Základná metodika tejto analýzy pre hodnotenie rizika pokrýva štyri fázy zobrazené na obrázku 3.[7]

Obrázok 3

Fázy metodiky FAIR

Význam metodiky FAIR spočíva v kvantifikácii kybernetického a technického rizika pomocou vyčíslenia obchodných dopadov, ktoré slúžia manažmentu pri rozhodovaní o organizácii.
FAIR sa spolieha na získavanie údajov zo systémov a kontrol a v kombinácii s údajmi z vyhodnotených dopadov transformuje ich do odhadu nízkej, vysokej a najpravdepodobnejšej hodnoty dopadu. Niekedy sa používa spolu s modelovaním Monte Carlo, ktoré predpovedá pravdepodobnosť rôznych výsledkov pri prítomnosti zásahu náhodných premenných).[8] FAIR nie je určený pre hodnotenie potenciálneho rizika v rannom štádiu nových technológií, preto jeho prípadné využitie pre tento účel nevhodné.

Metóda FAIR ponúka možnosti tam, kde sa akákoľvek vznikajúca technológia používa namiesto existujúcej technológie, alebo môže byť použitá pri podobných procesoch a kontrolách.
Ako možný prípad použitia by mohlo byť modelovanie vychádzajúce z predpokladov, ako bežné riadenie a situácie môžu prinášať riziko, a tým poskytnúť predstavu o tom, ako by nová technológia

v organizácii mohla fungovať. Ale spoliehanie sa skôr na domnienky než zvažovanie nových prístupov by mohlo ovplyvniť výsledné hodnotenie rizika. Okrem toho vyhodnotené riziko by mohlo zmeniť výpočty tak, aby boli užitočné. FAIR môže byť ťažko použiteľné pri počiatočnom hodnotení, vzhľadom na vzájomné vzťahy technológií, bezpečnosti, kontroly procesov a účinnosti týchto kontrol pre konkrétne použitie vznikajúcej technológie.

Dynamické hodnotenie rizík

Tradične dynamické hodnotenie rizík znamená ich priebežné hodnotenie na pomoc pri rozhodovaniu v prostrediach, ktoré sa menia, ale môžu tiež pomôcť v situáciách so zložitým, vysoko interaktívnym prostredím, v ktorom často dochádza k zmene údajov. Metód na dynamické hodnotenia rizík je veľa.

KPMG Dynamické hodnotenie rizika je príkladom toho, ako sofistikované algoritmy a analýzy údajov môžu byť využité na identifikáciu, prepojenie a zobrazenie rizika v štyroch rozmeroch. Dynamické hodnotenie rizík KPMG rámec zohľadňuje nielen pravdepodobnosť a dopady, ale aj rýchlosť a konektivita. Rýchlosť vyjadruje vývoj, šírenie sa incidentu. Dá sa použiť aj na popis pre narastajúce a kaskádové riziko (hrozba zneužíva zraniteľnosť aktíva a spustí reťazovú reakciu - „domino efekt“ na iné aktíva . Konektivita zahŕňa spôsob, akým riziko môže viesť k väčšiemu riziku a mieru, do akej sú zdroje rizika vzájomne prepojené.

Vzhľadom na prepojenosť niektorých vznikajúcich technológií a sietí s inými partnermi, v mnohých prípadoch môže špecialista na riziká modelovať rôzne spôsoby vzniku scenárov , ktoré sa môžu navzájom ovplyvňovať.

Scenáre môžu tiež uvažovať rýchlosti s akou sa môžu incidenty vyvíjať a tiež dopady rizika na iné riziká. Pri vzájomnom pôsobení viacerých rizík môžu špecialisti zvoliť scenáre, v ktorých zdanlivý zdroj nižšieho rizika môže byť dôležitejší a vyžaduje prednostné stanovenie priorít, pretože by to mohlo prerásť do rizika s väčším dopadom.

Hodnotenie rizík pre vznikajúce technológie by malo začínať metodikou, ktorá rieši zodpovedajúce podnikateľské riziko.

Využitie takejto metodiky na hodnotenie interakcií medzi používateľmi a zdrojmi rizika môže byť obzvlášť užitočné pre nové technológie, ktoré si vyžadujú sieťové prepojenie, ako napríklad, ak viaceré spoločnosti používajú technológiu privátneho blockchain , ktorý umožňuje interakciu medzi viacerými užívateľmi. Keď bude táto technológia viac známa a bude lepšie pochopená, bude mať táto metodika a prístup k nej väčšiu hodnotu. Pochopenie a umožnenie prístupu použitia rôznych scenárov pre zainteresované strany znamená využitie možnosti metodík definovať špecifické rizikové prepojenia.[9]

Porovnanie prístupov na hodnotenie rizík

Každá z uvedených troch metód má svoje výhody a výzvy na hodnotenie rizík nových technológií v závislosti od schopnosti organizácie zvážiť a prijať rozhodnutie na použitie novej technológie.

Hodnotenie rizík pre vznikajúce technológie by sa malo začať spôsobom, ktorý rieši súvisiace podnikateľské riziko. Mali by sa posúdiť hrozby a vypracovanie systému riadenia rizík tak, aby organizácia mala nad nimi zabezpečený dohľad. Ak sú dostupné informácie, môže byť vykonaná

analýza hrozieb pomocou FAIR a rozhodnutia o kontrolách je možné primerane vykonať pomocou RCSA. Pre situácie s viac ako jedným rizikom je možné použiť dynamické hodnotenie rizík, hlavne v prostredí, v ktorom sa hrozby menia. Obrázok 4 poskytuje porovnanie možnej užitočnosti každej metodiky podľa štádia implementácie novej technológie.

OBRÁZOK 4

Možnosti použitia metodík podľa etapy prijatia novej technológie

Etapa prijatia	RCSA	FAIR	Dynamické
Všeobecný prípad podnikania	Metodika by mohla poskytnúť pohľad na riziká a pomôcť s kompromisnou analýzou	Použitie je obmedzené, pretože chýbajú údaje na podrobné posúdenie	Pridaná hodnota pri zvažovaní prepojenosti viacerých rizík
Prvá realizácia	Metodika je vhodná na posudzovanie prevádzky, jej vplyv na iné podnikanie a na technologické riziká	Pre počiatočný stav obmedzené, ale neskôr, keď pribudnú údaje vhodné na analýzu rizík	Obmedzené použitie, pohľad na závislosti rizík je nejasný, musí sa stanoviť prepojiteľnosť rizík
Implementácia ďalších prípadov použitia	Získanie prehľadov z predchádzajúcich analýz, podpora prevádzky pre širšiu analýzu rizík	Údaje z každého prípadu použitia môžu pomôcť k širšiemu posúdeniu rizík	Začína sa budovať – model by mohol poskytnúť prehľad pre nasledujúce prípady a pre ďalšie etapy realizácie
Integrácia so stratégiou rozširovania	Kombináciou s hodnotením celkového rizika podniku táto metodika poskytuje dôkladný pohľad na strategické riziká	Údaje z existujúceho podnikania umožňujú širšiu analýzu rizík a jej zdokonaľovanie podľa vývoja stratégie	Údaje z existujúceho podnikania umožňujú širšiu analýzu rizík a poskytnú pohľad na vrstvené riziká*, ktoré možno pominúť, alebo pomôžu nájsť lepší spôsob pre postupné investovanie

* Vrstvené riziká predstavujú úroveň potenciálnych strát a pravdepodobnosť, s akou k nim dôjde. Spodné rizikové vrstvy zahŕňajú nízke straty s vysokou pravdepodobnosťou výskytu, zatiaľ čo horné rizikové vrstvy pokrývajú vysoké straty, ale s nízkou pravdepodobnosťou.

Pretože väčšina organizácií má svoju metodiku na hodnotenie rizík, môže si vybrať tie bežne používané bez ohľadu na to, v akom štádiu organizácia novú technológiu prijíma. Pre veľa organizácií to môže znamenať využitie tradičnej metodiky RCSA. Vzhľadom na vyššie náklady na prijatie viacero metodík súčasne, mohol by RCSA byť rozumným prístupom; avšak štruktúra príslušnej metodiky by mohla obmedziť jej uplatniteľnosť v niektorých fázach prijatia novej technológie, alebo tu môžu existovať iné obmedzenia, ako napríklad RCSA zložitosti mnohých nových technológií nevyhovuje.

Na analýzu rizík pomocou rôznych metodík je vhodný claud. Pri prvotnom osvojení cloudového riešenia by bolo najlepšie použiť prístup pomocou priemyselnej analýzy rizík (podobný ako RCSA), ktorý umožňuje všeobecnejšie úvahy o možných dopadoch a o hodnote cloudu namiesto uplatnenia špecifík, ktoré ponúkajú existujúce metodiky.

V prípade cloudového spracovania sú hrozby a kontroly čoraz viac dôležitejšie. Organizácia tu môže zvážiť použitie metodiky FAIR, ktorá má dáva efektívne použitie pri cloudovom riešení. Tak ako je to bežné chápané manažérmi rizík a auditormi, RCSA bola prijatá pre hodnotenie cloudov od dodávateľov tretích strán. Sofistikovanejšie metódy, ako je FAIR a dynamické hodnotenie rizík je možno použiť na hrozby, ktoré sú špecifické pre organizáciu. Tieto metodiky nie sú obmedzujúce pre cloudy a umožňujú riešiť aj celkové slabé miesta a prepojenia na iné zraniteľné miesta v organizácii. Zložitosti v modeloch hybridného cloudu môžu byť dobre riešiteľné využitím niektorých vlastnosti dynamického hodnotenia rizika.

Kľúčové faktory posudzovania rizík nových technológií

Pri zavádzaní nových technológií existujú tri kľúčové faktory pre hodnotenie rizika založené na výbere metodiky hodnotenia rizík. Riadenie príslušných rizík by malo zahŕňať ľudí, riadiaci proces a systémový návrh.

Ľudia

Prvým kľúčovým faktorom implementácie novej technológie a posúdenie jej rizika závisí od úrovne jej porozumenia podnikovými manažérmi a od ich spolupráce s IT:

- Aká je súčasná úroveň vyspelosti organizácie – t. j. úrovne podnikových manažérov v pochopení zložitosti a vlastností novej technológie?
- Aká je úroveň dôvery a istoty všetkých zainteresovaných strán, ktorých sa nová technológia dotýka?[10]
- Spolupracujú a komunikujú rôzne skupiny IT – napríklad riešitelia rozvoja, aplikácií, bezpečnosti a infraštruktúry s rôznymi úsekmi organizácie a pomáhajú im identifikovať riziká?[11]

Proces riadenia

Druhým kľúčovým faktorom je proces riadenia rizika s meniacimi sa predpismi.

- Je vybraná nová technológia nepretržite fungujúca v rámci prijateľných prahových hodnôt rizika?
- Sú obchodné procesy organizácie dostatočne vhodné na riadenie a vyváženie rizík súvisiacich s implementáciou vznikajúcej technológie?[12]
- Existuje nepretržité sledovanie nových predpisov a aktívnych procesov na zabezpečenie, že nové technologické modely sú v zhode so zmenami a s novými predpismi?

Návrh systémov

Tretím kľúčovým faktorom je návrh systémov v súlade s požiadavkami organizácie a jej politikou.

- Je dôvera vložená do návrhu novej technológie natoľko dostatočná, aby sa riziko zvažovalo v predstihu a bolo riadené už v priebehu návrhu?[13]
- Sú diskusie o rizikách a o opatreniach na implementáciu novej technológie začaté včas tak, aby bolo možné identifikovať akékoľvek neriešené problémy, zlepšenia procesov, a tak zabezpečiť, aby tieto technológie boli do podnikania úspešné integrované?

Objasnenie technológie Blockchain

Vzhľadom na relatívnu nezrelosť väčšiny organizácií v osvojení si blockchainu, je užitočné objasniť koncepcie ovplyvňujúce úvahy o rizikách a používanie metodík na ich hodnotenie.

Blockchain je novovznikajúca technológia, ktorá prináša výzvy na hodnotenie rizík. Pre používateľov vzniká neistota, pochopenie tejto technológie a jej vplyvu na organizáciu a to hlavne:

- Nevyvinuté štandardy pre blockchain vedú k rizikám bezpečnosti, súkromia a spolupráce s inými procesmi alebo údajmi.
- Ochrana údajov, najmä v súvislosti s rôznymi národnými a regionálnymi predpismi, zvyšuje zložitosť používania blockchain.
- Keďže blockchain je nová technológia, je tu potrebná dôvera vo vývojárov.
- Užívateľsky orientované riziko, ako je zachovanie súkromia kľúčov používaných na prístup k peňaženke je výzvou pre decentralizovanú sieť.
- Odolnosť a rýchlosť transakcií blockchain môžu byť ovplyvnené preťažením.
- Implementácia blockchain je ovplyvnená podľa toho, či ide o verejný/súkromný, alebo povolený/nepovolený typ blockchainu.
- Vysoká kvalita väčšiny sietí blockchain vyžaduje rozsiahlu vzájomnú spoluprácu s tretími stranami, s partnermi a poskytovateľmi služieb.

V počiatočnom štádiu rozhodovania či a ako používať blockchain, je potrebné zvážiť všetky možnosti a dôsledky rizika. V počiatočnom štádiu je pri hodnotení dopadov na podnikanie možné uplatniť všeobecné zásady metodiky RCSA. Ak sa organizácia rozhodla pre implementáciu konkrétneho použitia technológie blockchain, podrobné hodnotenie rizík možno získať použitím metodiky FAIR.
V prípade zložitých vzájomných vzťahov, kde by sa pri hodnotení rizík mala venovať najväčšia pozornosť, je vhodné použiť dynamické hodnotenie rizík.

Záver

Prijatie nových technológií má svoj vlastný životný cyklus a štádium ich osvojenia určuje spôsob požadovaného hodnotenia rizika. To zase ovplyvňuje typy metodík, ktoré môžu poskytnúť potrebný pohľad na riziko v danej fáze implementácie novej technológie**.** Stupeň, ktorým je vznikajúca technológia a jej súčasný spôsob využitia podobný existujúcej technológii, môžu byť faktormi pre použitie konkrétnej metodiky analýzy rizík.
Na začiatku procesu prijatia novej technológie sa len málo vie o jej možných účinkoch a nie sú dostupné údaje potrebné pre použitie komplexnejších modelov ako je FAIR. Prax však priniesla skúsenosti s novou technológiou, normy, prevádzkové procesy a pochopenie dopadov sa stáva základom na posúdenie širšieho využitia nových technológií. Ak organizácia už využíva viac kvantitatívne hodnotenie rizika ako je FAIR, potom údaje z predchádzajúcich prípadov použitia môžu prispieť k celkovému hodnoteniu rizík a poskytnúť podporu pre stratégiu, ktorú treba zvážiť a implementovať. Vo vyspelejšej organizácii je možné nové technológie posúdiť pomocou sofistikovanejších modelov hodnotenia rizík, pomocou vhodných dát, ako napr. dynamické hodnotenie rizík, a tak získať lepší prehľad o vzájomne prepojených rizikách. Bez ohľadu na spôsob, ktorý organizácia bežne používa, snaha používať viaceré metodiky hodnotenia rizík umožňuje zosúladiť aktívny prístup k riadeniu rizík prijatej novej technológie, a tým získanie prospechu podnikania.

Miera podobnosti novej technológie s existujúcou technológiou a jej súčasný spôsob použitia môže ovplyvniť konkrétnu metodiku hodnotenia rizík, ktorá by sa mala použiť .

Autori článku

MICHAEL KELLY | PH.D., CRISC, CISM

Je skúsený odborník v oblasti obchodu, IT telekomunikácií, rizík a bezpečnosti. Posledných päť rokov spolupracoval so Standard Chartered Bank, ktorá pomáha znižovať riziko. Ako vedúci zodpovedný za informačné bezpečnostné riziká pre technológie a inovácie v SC Ventures, je zodpovedný za bezpečnosť technologickej základne banky. Pomáhal rozvíjať systém riadenia pre používanie cloudových služieb (Infrastructure as a Service [IaaS] a Software as a Service [SaaS]) a pomáha vytvárať bezpečnostné stavebné prvky pre efektívne využívanie blockchain a technológie distribuovanej účtovnej knihy. V SC Ventures pracuje v oblasti štartupov, je proaktívny pri zvažovaní rôznych bezpečnostných štandardov a rizikových prístupov.

ADELINE CHAN | CISM

Je vedúcou systému a stratégie informačnej kybernetickej bezpečnosti pre firemné, komerčné a inštitucionálne bankovníctvo v Standard Chartered Bank, kde pracuje prvej línii riadenia bezpečnosti. Pred touto úlohou strávila osem rokov v druhej línii obrany ako rizikový pracovník zodpovedný

za implementáciu systému riadenia rizík a analýzy rizík. Pracovala na úseku riadenia operačného rizika zahŕňajúceho finančnú kriminalitu a na úseku kybernetickej bezpečnosti so zameraním na správu identity a prístupu k údajom v chránených doménach. Bola tiež zodpovedná za vývoj systémov pre riadenie na podporu startupov v SC Ventures. Aktívne pracuje ako dobrovoľníčka pre SheLeadsTech a ISACA® Singapore Chapter.

Poznámky:

1 Brachio, A.; "How to Manage the Evolving Risks of Emerging Technology," EY, 15 February 2019, https://www.ey.com/en_sg/consulting/how-to-manage-the-evolving-risks-ofemerging-technology
2 Kumar, T.; "The Methods and Tactics Behind Risk and Control Self-Assessment," The Global Treasurer, 6 February 2019, https://www.theglobaltreasurer.com/2019/ 02/06/the-methods-and-tactics-behind-risk-andcontrol-self-assessment/
3 FAIR Institute, "FAIR Risk Management," https://www.fairinstitute.org/fair-risk-management
4 KPMG, Dynamic Risk Assessment, Netherlands, June 2019, https://assets.kpmg/content/dam/ kpmg/au/pdf/2017/dynamic-risk-assessmentfour-dimensional-view.pdf
5 Op cit Kumar 6 Riggins, N.; "The Methods and Tactics Behind Risk and Control Self-Assessment," The Global Treasurer,
6 February 2019, https://www.theglobaltreasurer.com/2019/ 02/06/the-methods-and-tactics-behind-risk-andcontrol-self-assessment/
7 Op cit FAIR Institute
8 Kenton, W.; "Monte Carlo Simulation," Investopedia, 4 October 2021, https://www.investopedia.com/terms/m/ montecarlosimulation.asp
9 Op cit KPMG
10 PricewaterhouseCoopers (PwC), "Emerging and Disruptive Technology Risk," https://www.pwc.co.uk/services/risk/ technology/emerging-disruptive-technologyrisk-stay-in-control.html
11 Pariseau, B.; "IT Governance Must Catch Up With DevSecOps, Experts Say," TechTarget, 24 November 2020, https://www.techtarget.com/ searchitoperations/news/252492646/ IT-governance-must-catch-up-withDevSecOps-experts-say
12 Young, J.; "Balancing the Benefits With the Risks of Emerging Technology," TechTarget, 19 July 2021, https://www.techtarget.com/ searchsecurity/post/Balancing-the-benefitswith-the-risks-of-emerging-technology
13 Op cit Brachio

Preklad: Ing. Dušan Makoš, CISA