ISACA JOURNAL Volume 3

Operational Resilience: Preparing for the Next Global Crisis

SUMEDHA ADAVADE | CISA

Odolnosť prevádzky: Príprava na ďalšiu globálnu krízu

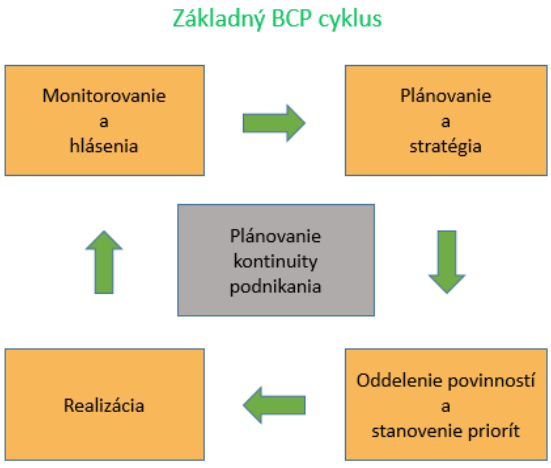
Hoci odolnosť obchodných operácií na nepredvídané udalosti bola pre organizácie prioritou už pred vypuknutím pandémie COVID- 19, v dôsledku naďalej prebiehajúcej globálnej pandémie je táto téma stále kritická a naliehavá. Dokonca aj tie najmenšie organizácie vzali do úvahy kontinuitu podnikania, zálohovanie a plánovanie obnovy do rámca bežných operácií. Tento nový význam odolnosti prevádzky *bude mať trvalý vplyv na organizácie.*

Prevádzková odolnosť je pojem, ktorý možno použiť v širokej škále priemyselných odvetví, nemožno ju zúžiť len na jeden konkrétny sektor. Pandémia COVID-19 z hľadiska prevádzkovej odolnosti priniesla rovnaké hrozby pre podniky vo všetkých ich sektoroch a odvetviach. Hoci za posledné dva roky sa v tejto oblasti urobilo veľa práce, je táto téma stále aktuálna. Všetci zainteresovaní majú pri jej plnení pred sebou ešte dlhú cestu, pretože svet sa s dôsledkami poslednej pandémie ešte stále vyrovnáva.

Veľa organizácií verí, že prevádzková odolnosť je výsledkom efektívneho riadenia operačných rizík (ORM - Operational Risk Management). Hoci niektoré organizácie môžu prevádzkovú odolnosť spájať s ORM, iné na tom pracujú spolu s ORM, alebo na jej dosiahnutie využívajú vstupy z ORM. Je tu viac možností a stojí to zato preskúmať ich a zaujať na operačnú odolnosť nový pohľad - na výzvy, ktoré prináša a spôsoby, ako ju riešiť. Tradičné postupy BCP implementované organizáciami potrebujú poznatky a vstupy o vplyvoch vonkajšieho prostredia, aby tak v prípade potreby boli pripravené reagovať na akékoľvek krízové situácie. Organizácie musia zvážiť existujúce požiadavky na riadenie rizík, ich zmierňovanie, hlavne v oblasti kybernetickej bezpečnosti, ochrany údajov, kontinuity podnikania a poskytovania služieb tretími stranami.

Realizácia

Pre organizácie je už určitý čas plánovanie kontinuity podnikania (BCP) súčasťou riadenia procesov týkajúcich sa bežných obchodných činností prevádzkových—postupov. Hlavnou úlohou BCP je na základe rôznych scenárov pripraviť organizáciu na krízové udalosti a ich prekonanie. Každý úsek organizácie zodpovedá za procesy, plní rôzne kritické činnosti, ktoré počas krízovej situácie vyžadujú rôzne úrovne plánovania. BCP pozostáva zo štyroch základných fáz (obrázok 1).



Obrázok 1

Poučenie z globálnej pandémie si však vyžaduje viac pozornosti. Prevádzková odolnosť ide o krok pred BCP v tom, že odolná organizácia sa učí a aktualizuje postupy kontinuity podnikania na základe nových vonkajších vplyvov, ktoré s tým súvisia. Medzi fázou plánovania a fázou monitorovania je potrebné vykonať situačnú analýzu, ktorá zahŕňa sledovanie vonkajších vplyvov súvisiacich s obchodnou činnosťou a následné úpravy plánov. Jedným z príkladov tejto zmeny boli organizácie, ktoré v dôsledku pandémie COVID-19 prijali režim práce z domu, alebo zmiešaný pracovný model.

Táto fáza je rozhodujúca na pripravenosť organizácie reagovať na akýkoľvek náhly výskyt nežiadúcich udalostí ovplyvňujúcich zdroje, procesy, ich monitorovanie a vyhodnocovanie. Vzhľadom na túto novú situačnú analýzu existuje päť krokov na dosiahnutie prevádzkovej odolnosti organizácie:

1. Definovanie dôležitých obchodných aktivít.
2. Nastavenie tolerancií dopadov.
3. Určenie vlastníctva a zodpovednosti za systémy a procesy.
4. Zabezpečenie odolnosti tretích strán.
5. Dodržiavanie regulačných predpisov a platných noriem.

„Pri nastavovaní tolerancií dopadov vo všeobecnosti neexistujú žiadne predchádzajúce skúsenosti alebo ponaučenia, z ktorých by sa dalo vychádzať, pretože tento postup je pre každú organizáciu iný (jedinečný.)“

Krok 1: Definovanie dôležitých obchodných aktivít

Prvým krokom k vypracovaniu plánu kontinuity podnikania je identifikácia dôležitých obchodných aktivít. Prieskum ORX Progressing Operational Resilience, Švajčiarsko, Switzerland, uskutočnený v roku 2021, zameraný na dôležité obchodné aktivity v známych bankách v Spojenom kráľovstve ukázal, že zúčastnené organizácie mali množstvo dôležitých aktivít v rozsahu od 10 do 100. V dôsledku pandémie staršie aktivity a procesy, s ktorými predtým problémy neboli, začali sa teraz prejavovať. Ako príklad, uvažujme o prevádzkových procesoch pobočkového bankovníctva. Aby sa počas počiatočných obmedzení pohybu znížila miera infekcie pracovali pobočky bánk v rôznych pracovných hodinách. Technologicky menej zdatní zákazníci, ktorí žijú vo vzdialených lokalitách bez veľkej digitalizácie a sú zvyknutí chodiť do pobočiek, mali v týchto časoch pri vykonávaní bankových transakcií problémy.

Tento príklad dokazuje, že pri plánovaní prevádzkovej odolnosti nemožno nič zanedbať a je dôležité zvážiť všetky okolnosti.

Čo robí obchodné aktivity dôležitými? Pre úspešnú implementáciu prevádzkovej odolnosti je možné považovať za dôležité akúkoľvek činnosť alebo proces, ktorý ak je prerušený, môže ovplyvniť jej obchodné operácie nad rámec stanovenej tolerancie organizácie. Na základe vonkajších okolností môžu byť činnosti organizácie zo zoznamu jej aktivít pridané, alebo odstránené. Môžu sa tiež v zozname dôležitosti pohybovať nahor a nadol, podľa toho, ako sa daná aktivita stáva viac alebo menej naliehavou. Pri definovaní dôležitých podnikateľských činností však existujú určité problémy:

• Na definovanie tej istej dôležitej činnosti možno použiť viacero definícií a porovnávacích hodnôt.

• Regulačné smernice pre odvetvia sa môžu celkom líšiť.

• Štandardné postupy používané v rámci toho istého odvetvia sa môžu v jednotlivých podnikoch líšiť.

• Zvažovanie nových vonkajších okolností môže spôsobiť, že organizácia nie je pripravená vykonávať činnosti, ktoré boli predtým považované za samozrejmosť.

Tieto problémy sa dajú riešiť:

• Dôkladným pochopením všetkých procesov, činností a ich zosúladením s obchodnou stratégiou.

• Definovaním jediného slabého miesta procesu a stanovením všetkých činností, ktoré ním môžu byť ovplyvnené, narušené. Je to odlišné od určovania štandardného apetítu rizika – rizika, ktoré je organizácia k dosiahnutiu svojich cieľov ochotná riskovať, pretože definované slabé miesto môže vyžadovať časté revízie a dolaďovanie na základe vonkajších okolností, kým sa nedosiahne požadovaná úroveň.

• Uprednostňovanie činností na základe definícií BCP (napr. požadovaná doba obnovy [RTO – Recovery Time Objective], maximálna prípustná doba straty údajov [RPO – Recovery Point Objective]).

• Dôsledné testovanie plánov kontinuity podnikania na základe požadovaných intervalov.

• Využitie skúseností získaných počas testovania na spresnenie slabého miesta a stanovenie priorít požadovaných opatrení na jeho posilnenie.

Krok 2: Stanovenie tolerancie dopadov (impact tolerances - maximálna tolerovateľná úroveň narušenia dôležitej obchodnej služby / predstavuje bod, za ktorým sa škoda spôsobená prerušením služby stáva neprípustnou.

Vo všeobecnosti na určenie tolerancie dopadov neexistujú žiadne predchádzajúce skúsenosti alebo ponaučenia, z ktorých by sa dalo potrebné usmernenie vyvodiť. Uvedené cvičenie je pre každú organizáciu iné ,a preto je dôležité, aby organizácie zvážili všetky potenciálne možnosti, ktoré by mohli tento proces ovplyvniť. To, čo platilo v predchádzajúcich rutinných plánoch BCP, už nemusí byť platné. Slabé miesto je potrebné určiť uvážlivo na základe vonkajších vplyvov a pomocou vlastného poznania, prispôsobovania sa okolnostiam, čo nie je vždy ľahké dosiahnuť okamžite.

Ďalšie výzvy pri nastavovaní tolerancií dopadov môžu zahŕňať:

• Stanovenie všeobecne platných tolerančných limitov pre procesy ovplyvňujúce rôzne obchodné jednotky, ich činnosti, funkcie alebo geografické oblasti.

• Stanovenie tolerančných limitov pre vzájomne súvisiace procesy a činnosti.

• Stanovenie limitov tolerancie pre činnosti s vypracovanými plánmi obnovy, pre časť ich aktivít.

• Nepretržité učenie sa z nepriaznivých situácií a monitorovanie slabých miest s cieľom dosiahnuť ich posilnenie. Na riešenie týchto výziev je možné podniknúť tieto kroky:

• Určenie hlavného slabého miesta, pričom do úvahy sa berú procesy, ich celkové súvislosti a organizačné politiky, ktoré môžu byť prispôsobené podľa geografických oblastí a trhových podmienok. Napríklad, ak je pre kritický IT systém prijateľný prestoj x hodín, možno ho doladiť na x+1/-1 hodiny a to na základe meniacich sa trendov, situácie poskytovateľa služieb a trhových praktík. Túto hodnotu x hodín môžu prijať všetky úseky organizácie v rôznych geografických oblastiach, alebo ak sa tu na základe miestnych predpisov vyžadujú odlišné hodnoty, možno ju upraviť tak, aby vyhovovala konkrétnej geografickej oblasti. Ak sa tento proces vykonáva opatrne, tieto hodnoty (t.j. x hodín) by sa od seba nemali veľmi líšiť.

• Pre aktivity ovplyvňujúce viaceré obchodné úseky, mali by byť limity tolerancie stanovené na základe súhlasu všetkých ovplyvnených jednotiek. Napríklad oddelenie kreditných kariet a oddelenie vykonávania transakcií môžu mať spoločne nastavené limity tolerancie pre činnosti súvisiace so spracovaním transakcií, berúc do úvahy miestne okolnosti, regulačné smernice a organizačné predpisy.

• Na stanovenie tolerancií dopadov možno použiť nástroje na riadenie prevádzkových rizík, ako je hodnotenie kritických scenárov a vnútorná kontrola riadenia rizík.

• Pri hodnotení uvedených scenárov je možné každoročne pridávať nové scenáre. Predpoklady a výpočty strát možno upraviť podľa vonkajších okolností (napr. nový malvérový útok možno použiť na prijatie procesov v scenári, akým je kybernetický útok na IT systém organizácie), spolu s prislúchajúcimi vnútornými zmenami a dopadmi. To je užitočné pri posilnení slabého miesta.

• Pri hodnotení kontrol na riadenie rizika by sa mali zvážiť vplyvy vonkajších okolností na proces, kedykoľvek je to opodstatnené a použiteľné. Môže sa zvážiť aj pridanie nového rizika a podľa toho aj prislúchajúce kontroly.

„Prevádzkovú odolnosť nemožno dosiahnuť jednoducho pomocou rozsiahlych plánov kontinuity podnikania a cvičením obnovy po havárii.“

Krok 3: Vlastníctvo procesu, systému a zodpovednosť

Prevádzkovú odolnosť nemožno dosiahnuť jednoducho pomocou rozsiahlych plánov kontinuity podnikania a cvičením obnovy po havárii (DR - Disaster Recovery). Vyžaduje si to kultúrny posun v rámci organizácie a zmenu myslenia zamestnancov. Stanovenie vlastníctva a zodpovednosti za akýkoľvek systém, proces sa môže na prvý pohľad zdať jednoduché. Je to však oveľa zložitejšie. Jeden proces alebo aktivita môže zahŕňať viacero ľudí z rôznych obchodných úsekov, funkcií a zosúladenie všetkých zainteresovaných strán môže byť náročné. Organizácia môže napríklad vyžadovať skoré spustenie novej funkcie v produkte, ale tá v čase jej spustenia nemusí byť na to pripravená, alebo z hľadiska bezpečnosti IT plne otestovaná. Ohrozenie bezpečnosti digitálnych platobných produktov môže byť pre organizáciu nebezpečné.

Vlastníctvo procesov, systémov a stanovenie zodpovednosti môže predstavovať niekoľko výziev:

• Spolupráca na vzájomne prepojených procesoch a činnostiach si môže vyžadovať prácu zamestnancov z rôznych oddelení. Požiadať niekoho, aby vykonával opakujúce sa úlohy mimo jeho popisu práce, môže byť pre zamestnancov záťažou.

• Dosiahnutie rozdelenia povinností (SoD – Segregation of Duties) pri stanovení vlastníctva procesov. Napríklad môže dôjsť k nedostatku zdrojov v dôsledku zvyšujúcej sa miery infekcie počas pandémie, čo môže spôsobiť ťažkosti pri prideľovaní povinností dostupnému personálu.

• Mapovanie procesov a činností s príslušnými úsekmi a prevádzkovými jednotkami na zabezpečenie zodpovednosti. Proces alebo činnosť môže mať pre rôzne funkcie rôzny význam, preto môže byť ťažké ich zmapovať. Napríklad prevádzková jednotka môže zadať hodnoty kľúčového ukazovateľa rizika (KRI - Key Risk Indikator/ je metrika na meranie pravdepodobnosti nepriaznivej udalosti, ktorá bude mať výrazne negatívny vplyv na úspešnosť podnikania organizácie).

• Zváženie vplyvu vonkajších okolností na procesy, identifikácia nových procesných rizík, implementácia nových kontrolných mechanizmov a ich vlastníctvo. Napríklad v dôsledku náhlych zmien vládnych obmedzení v dôsledku trendov infekcie môže byť ovplyvnená preprava, čo môže ovplyvniť procesy, ako je skladovanie dokumentov vo fyzických miestach.

• Identifikácia a implementácia nových procesov alebo činností, priberanie nových zdrojov a ak je to potrebné, stanovenie úloh a zodpovedností súvisiacich s novými procesmi. Napríklad pri práci z domu, kvôli nárastu potenciálnych podvodov v dôsledku spracovania transakcií , museli banky investovať do nových špecializovaných bezpečnostných produktov, najať a vyškoliť ľudí na ich prevádzku.

Tieto výzvy možno do určitej miery zmierniť:

• Zmapovaním všetkých procesov a činností a stanovením zodpovednosti ich príslušným vlastníkom.

• Výberom metrík - spôsobu a nástrojov merania dôležitých obchodných aktivít, zohľadnením podnetov z ukazovateľov operačného kľúčového rizika.

• Objasnením úloh a zodpovedností vlastníka každého procesu na dosiahnutie primeranej SoD.

• Zabezpečením, aby všetky zainteresované strany ako súčasť organizačnej stratégie pracovali na dosiahnutí rovnakého cieľa

Krok 4: Odolnosť voči tretím stranám

Vzhľadom na neustále sa zvyšujúcu závislosť od poskytovateľov služieb tretích strán - outsourcing a z toho vyplývajúcich rizík, je nanajvýš dôležité zabezpečenie odolnosti všetkých tretích strán slúžiacich organizácii. Od vypuknutia pandémie COVID-19 sa riziko súvisiace s outsourcingovými aktivitami mnohonásobne zvýšilo. Keď zmluvní zamestnanci pristupovali ku kritickým systémom z domu, riadenie bezpečnosti bolo zložité a ešte kritickejšie. Keďže úrady boli zatvorené a služby počas národných opatrení a obmedzení kvôli COVID-19 boli obmedzené, bolo zložité zabezpečiť kontinuitu podnikania v rámci celého dodávateľského reťazca a všetkých súvisiacich zdrojov. Medzi ďalšie prekážky pri dosahovaní odolnosti tretích strán patrí:

• Stanovenie kritickosti poskytovateľov služieb môže byť náročné. Dodávateľ, ktorý poskytuje najväčšiu hodnotu, nemusí byť z hľadiska prevádzkovej odolnosti tým najdôležitejším dodávateľom.

• Odolnosť subdodávateľov poskytovateľov služieb môže byť neznáma.

• Môže byť ťažké získať prehľad o riziku koncentrácie tretích strán - prílišné spoliehanie sa na jedného dodávateľa pre kritické služby.

• Nie je reálna úplná transparentnosť a viditeľnosť zo strany systémovo dôležitých poskytovateľov služieb, ako sú poskytovatelia služieb cloud.

• Zvýšené prijímanie nových technológií poskytovateľmi služieb má vplyv na ich prevádzkovú odolnosť. Na riešenie týchto prekážok je možné uplatniť nasledujúce riešenia:

• Priradenie patričnej významnosti každému externému poskytovateľovi služieb na základe vplyvu na prevádzku, obchod, financie, zákazníkov, likviditu, geografické oblasti alebo právne dopady, ak poskytovateľ nemôže poskytovať služby.

• Testovanie, audity a ich frekvencia sa môžu u všetkých externých poskytovateľov služieb líšiť. Napríklad testy kybernetickej bezpečnosti, ako je hodnotenie zraniteľnosti a penetračné testovanie, sú dôležité pre poskytovateľov služieb, ktorí poskytujú prevádzkové služby bankomatov, ale u poskytovateľa služieb, ktorý skladuje fyzické dokumenty, sa ich možno vzdať.

• Hodnotenia možno každoročne poskytovať všetkým poskytovateľom služieb a najslabší článok v systéme možno identifikovať prostredníctvom najnižšieho hodnotenia, čo umožňuje riešiť prislúchajúce zraniteľnosti.

• Dôkladne riadenie a kontrola plánov kontinuity činnosti externého poskytovateľa služieb, vrátane nácviku obnovy po havárii a vyhodnotenie výsledkov.

• Subdodávatelia pre poskytovateľov služieb tretích strán môžu taktiež podliehať testom a auditom zameraným na kritickosť. Tieto je možné vykonávať na základe dohody všetkých zúčastnených strán.

Krok 5: Regulačné požiadavky na prevádzkovú odolnosť

Prevádzková odolnosť je pre regulačné orgány ich celosvetovou kľúčovou oblasťou záujmu. Požiadavky stanovené regulátormi sa zameriavajú na rôzne opatrenia, ktoré majú organizácie prijať. Napríklad britský regulačný rámec PS6/21 Operational Resilience: Impact Tolerances for Important Business sa zameriava na poskytovanie dôležitých obchodných služieb.

Európska komisia sa zameriava na kybernetickú bezpečnosť a IT riziko na rozdiel odolnosti na hrozby v širšom zmysle. Švajčiarsky bazilejský výbor pre bankový dohľad (BCBS) zase kladie silný dôraz na riadenie a dohľad predstavenstva nad plánovaním a toleranciou rizika. Dodržiavanie regulačných požiadaviek na prevádzkovú odolnosť sa môže javiť ako náročné z dvoch dôvodov:

1. Regulačné orgány na celom svete naďalej citlivo určujú prístupy a požiadavky potrebné na dosiahnutie prevádzkovej odolnosti. Organizácie boli doteraz schopné dodržiavať existujúce usmernenia, ale súčasná situácia vytvorená v dôsledku pandémie si vyžaduje viac.

2. Univerzálny prístup nebude efektívne spĺňať všetky regulačné požiadavky. Niektorí regulátori poskytujú všeobecné usmernenia a ich implementáciu nechávajú otvorenú na interpretáciu zo strany organizácií, zatiaľ čo niektoré poskytujú jasné požiadavky. V prvom prípade by mohla organizácia urobiť nesprávny alebo neúplný výklad, čo by malo za následok nesúlad; v druhom prípade môže byť ťažké splniť každú požiadavku. Ak chcete lepšie pochopiť a dosiahnuť súlad s predpismi, zvážte nasledujúce pokyny:

• Ak existuje rozdiel medzi regulačnými pokynmi a internými zásadami a procesmi, je najlepšie implementovať tie, ktoré sú prísnejšie.

• Usmernenia týkajúce sa prevádzkovej odolnosti nemusia obsahovať drastické zmeny oproti doteraz platným postupom. Prístupy k identifikácii kritických obchodných aktivít, ich mapovaniu a nastaveniu tolerancií dopadov možno trvale zlepšovať. Tieto musia byť zohľadnené v príslušných postupoch prevádzkovej odolnosti.

„Subdodávatelia pre dodávateľov služieb tretích strán môžu taktiež podliehať testom a auditom zameraným na kritickosť“.

• Organizácie sa musia snažiť o správny výklad regulačných smerníc. Tímy pre dodržiavanie pravidiel si musia byť vedomé všetkých nových smerníc, výkladov alebo objasnení pochybností, ktoré môžu regulátori vydať.

• Regulačné orgány, ktoré sa zameriavajú na prevádzkovú odolnosť, by tiež mali organizáciám poskytovať podporu pri implementácii a odporúčať osvedčené postupy v celom odvetví. Dá sa to dosiahnuť prostredníctvom workshopov alebo seminárov o prevádzkovej odolnosti. Organizáciám, ktoré takto postupujú, možno vysloviť uznanie. Ako ďalšie kroky môžu organizácie prijať rôzne prístupy k dosiahnutiu k pilotnej prevádzkovej odolnosti. Niektoré organizácie začínajú identifikáciou kritických obchodných aktivít, niektoré začínajú testovaním odolnosti a niektoré skúmajú existujúce obchodné aktivity, aby zistili ich kritickosť. Zvážte napríklad bezpečnosť údajov v banke, kde zamestnanci pracujú z domu. Banky zaviedli technológiu dynamického vodoznaku pre zamestnancov, ktorí pracujú z domu. Vytvára jedinečný vzor, ktorý sa zobrazuje na pozadí obrazoviek pre zamestnancov pripájajúcich sa k domácej alebo inej sieti. Táto technológia vytvára zodpovednosť v prípade úniku údajov, ale môže tiež ovplyvniť rýchlosť určitých aplikácií a spôsobiť narušenie podnikania. Možno bude najlepšie implementovať ho najprv pre obmedzený personál a potom ho pomaly rozširovať. Neexistuje správny alebo nesprávny prístup. Pilotovanie prevádzkovej odolnosti sa bude líšiť z hľadiska operácií, procesov, obchodnej stratégie, zdrojov, geografického kontextu, trhových praktík, platných predpisov a dodržiavaných noriem. Základné princípy však zostávajú rovnaké.

"Aby sme boli pripravení na budúce globálne krízy, je dôležité, aby bola prevádzková odolnosť riadená proaktívne a s vedomým úsilím.

Záver

Globálna pandémia COVID-19 jasne ukázala, že moderný svet je nestály, neistý, zložitý a nejednoznačný. Operačná odolnosť bude v budúcnosti základom každého podniku. Aby sme boli pripravení na budúce globálne krízy, je nevyhnutné, aby s vedomým úsilím bola prevádzková odolnosť riadená proaktívne, s predvídaním udalostí, plánovaním riešení, a preto by mala byť súčasťou obchodnej stratégie organizácie.

Vrcholový manažment by mal byť zapojený do všetkých etáp plánovania kontinuity podnikania, aby mal možnosť tak preniknúť do základných operácií a plánovať stratégiu podnikania, aby organizácia bola pripravená zvládnuť neočakávané scenáre so širokým dopadom.

Aby sme lepšie pochopili širší obraz prevádzkovej odolnosti, kontinuita podnikania by sa mala vyvíjať s pomocou vládnych a verejných organizácií formou iniciatív, ako sú strategické online alebo semináre na zdieľanie osvedčených postupov a uznanie najodolnejších organizácií. To pomôže podnikom zostať pripravenými na krízu a prispeje k vybudovaniu odolného hospodárstva, k bezpečnému spoločenskému životu a udržateľnému využívaniu dostupných zdrojov.

Autor článku: Sumedha Adavade, CISA Je rizikovým manažérom v DBS Bank. Má 14-ročné skúsenosti v oblasti riadenia rizík, dodržiavania predpisov, auditu informačnej bezpečnosti, poskytovania riešení na zmiernenie rizík a záruk pre banky a iné finančné inštitúcie.

Preklad: Ing. Dušan Makoš / CISA