HRVATSKA
REVIZORSKA
KOMORA

Stručno savjetovanje ovlaštenih revizora u organizaciji Hrvatske revizorske komore

za 2023. godinu

Opći i specifični IT rizici i primjena u reviziji financijskih izvještaja

HRVATSKA
REVIZORSKA
KOMORA

Ratko Drča

Napomena

Sadržaj ovog prezentacijskog materijala je informativnog karaktera. Upotreba prezentacijskog materijala ne oslobađa korisnika od poduzimanja potrebnih mjera predostrožnosti prije njegove uporabe, odnosno ne oslobađa korisnika od obveze primjene izvornih zakonskih odredbi i pravila struke, s toga se Hrvatska revizorska komora i autor prezentacijskog materijala ne mogu smatrati odgovornima prilikom uporabe ili u vezi s uporabom sadržaja koji se nalazi u prezentacijskom materijalu.

Uporaba sadržaja i podataka iz ovog prezentacijskog materijala dopuštena je pod uvjetom navođenja izvora podataka, osim u slučajevima kada je naznačeno drugačije.

Sadržaj

Revizija i kibernetički rizici

Dodatak 5

Ranjivost IT aplikacija, baza podataka i drugih aspekata IT okruženja od kibernetičkih rizika – ***Jedan od faktora za razumijevanje i procjenu IT okruženja***

MRevS315

Opseg i vrsta primjenjivih rizika koji proizlaze iz korištenja IT-a variraju ovisno o vrsti i karakteristikama identificiranih IT aplikacija i drugim aspektima IT okruženja.

Dodatak 6

Svaki od IT rizika sadržava kibernetičku komponentu, a pogotovo:

- Neovlašteni pristup podacima
- Ovlasti šire od zahtijevanih
- Neovlaštene promjene podataka
- Gubitak i/ili nemogućnost pristupa podacima kad je potrebno

Opći IT rizici – Upravljanje pristupom

Privilegije korisničkog pristupa

- Korisnici imaju pristupne privilegije izvan onih koje su potrebne za obavljanje dodijeljenih dužnosti što može stvoriti nepravilnu segregaciju dužnosti.

Izravan pristup podacima

- Neprimjerene promjene se provode izravno u financijskim podacima kroz sredstva koja su različita od transakcija aplikacije.

Sistemske postavke

- Sistemi nisu adekvatno konfigurirani ili ažurirani radi ograničavanja pristupa pravilno autoriziranim i primjerenim korisnicima.

Opći IT rizici – Upravljanje promjenom

Promjene aplikacije

- Neprimjerne promjene su učinjene u sustavu aplikacija ili programima koji sadrže relevantne automatizirane kontrole (tj. postavke koje se mogu konfigurirati, automatizirani algoritmi, automatizirane kalkulacije i automatizirana povlačenja podataka) ili u logici izvještaja.

Promjene u bazama podataka

- Neprimjerene promjene su učinjene u strukturi baze podataka i odnosima između podataka.

Promjene u sustavnom softveru

- Neprimjerene promjene su učinjene u sistemskom softveru (npr. operativni sustav, mreža, softvare za upravljanje promjenama, softvare za kontrolu pristupa).

Opći IT rizici – IT operacije

Mreža

- Mreža ne sprječava adekvatno da neautorizirani korisnici dobiju neprimjeren pristup informacijskim sustavima.

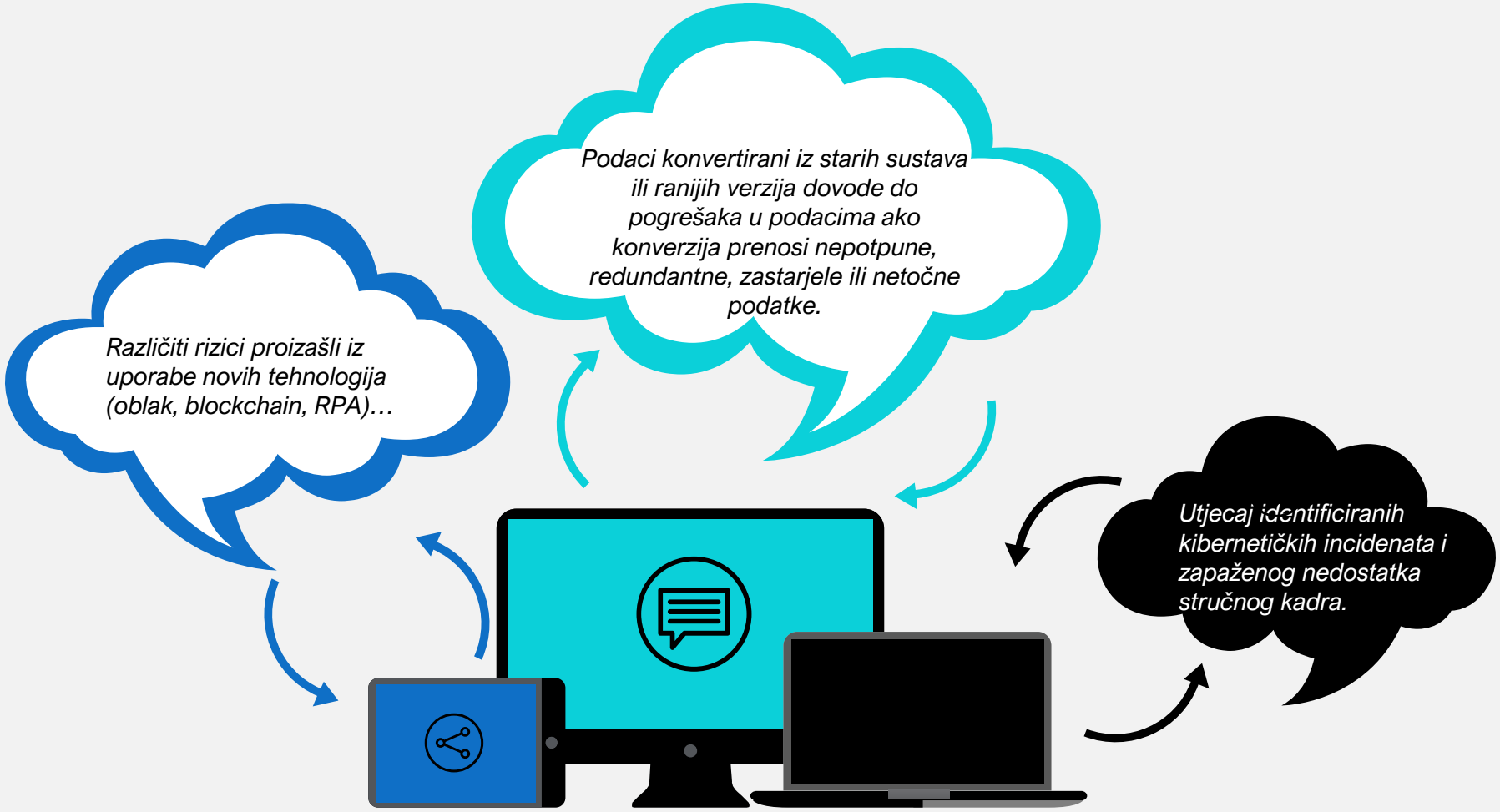
Kopije podataka i oporavak

- Financijski podaci ne mogu biti oporavljeni i ne može im se pristupiti pravovremeno kad postoji gubitak podataka.

Skupne obrade

- Produkcijski sustavi, program ili poslovni rezultiraju u netočnoj, nepotpunoj ili neautoriziranoj obradi podataka.

Specifični IT rizici



Indikatori klasifikacije IT rizika 1

Indikator klasifikacije rizika	Pokazatelj nižeg rizika	Pokazatelj višeg rizika
Kompleksnost poslovanja i financijskog izvještavanja	Samostalni sustav koji utječe na mali broj poslovnih procesa	Sustav koji utječe na više poslovnih procesa ili više ovisnih sustava
Korišteni podaci	Male količine podataka ili jednostavni podaci	Velika količina podataka ili složeni podaci
Automatske kontrole	Mali broj ili jednostavne automatske kontrole	Velik broj ili složene automatske kontrole
Automatska izvještajna logika	Jednostavna izvještajna logika	Složena izvještajna logika
Visoko automatizirana obrada bez papira	Nije prisutna	Prisutna
Ulazi podataka i sučelja (interfaces)	Mali broj ulaza podataka /ili jednostavna sučelja	Veliki broj ulaza podataka i složena sučelja za prijenos
Povijest neispravnosti u automatizaciji	Nema povijesti neispravnosti	Prisutna povijest neispravnosti

Indikatori klasifikacije IT rizika 2

Indikator klasifikacije rizika	Pokazatelj nižeg rizika	Pokazatelj višeg rizika
IT okruženje i korporativna kultura	Zrelo, stabilno kontrolno okruženje, iskusno vodstvo i osoblje	Novo ili start-up, novo vodstvo ili neiskusno osoblje
Tehnološka platforma i arhitektura	Zrela i stabilna tehnologija, mali ili jednostavni Klijent-poslužitelj princip, SAAS cloud	Složena i zahtjevna tehnologija, složeni klijent-poslužitelj princip, izloženo web-u, IAAS cloud
Pristup krajnjih korisnika	Mali broj korisnika s pristupom sustavu	Veliki broj korisnika s pristupom sustavu
Vrsta aplikacije	Kupljena aplikacija bez ili s malo prilagodbi	Interno razvijena aplikacija ili kupljena sa značajnim prilagodbama
Broj i vrsta promjena	Mali broj ili jednostavne promjene	Veći broj ili složene promjene, agilni razvoj
Konverzija podataka (ukoliko je primjenjivo)	Manja nadogradnja verzije, ograničeni set podataka u migraciji	Veća nadogradnja verzije, promjena sustava
Uporaba skupnih obrada	Ograničen broj jednostavnih skupnih obrada	Veći broj složenih skupnih obrada

Utjecaj kibernetičkih incidenata na reviziju

Utvrđivanje kibernetičkog incidenta

- Primjeri procedura za stjecanje razumijevanja da li se kibernetički incident dogodio:
- Razgovor s Voditeljem sigurnosti ili drugom osobom odgovornom za upravljanje kibernetičkom sigurnošću
- Razgovor s voditeljima IT-a i Financija
- Pregled izvještaja interne revizije i zapisnike nadzornog odbora te neovisnih izvora (mediji i sl.)

Revizorski postupci uslijed utvrđenog kibernetičkog incidenta

- Ako je identificirana informacija o povredi sigurnosti, revizor redovno razmatra opseg do kojeg takva povreda ima potencijal utjecati na financijsko izvještavanje. Ukoliko može imati utjecaja na financijsko izvještavanje, revizor može odlučiti razumjeti i testirati povezane kontrole radi utvrđivanja mogućeg utjecaja ili opsega potencijalnih pogrešnih prikazivanja u financijskim izvještajima ili može utvrditi da je subjekt pružio adekvatne informacije u vezi s takvom povredom sigurnosti.

Hvala na pozornosti!

Ratko Drča

rdrca@deloittece.com