

Revizor informacijskih sistemov: ključni akter pri trajnostnem poročanju

Nina Kravanja Novak, FCCA, pooblaščen revizorka, pooblaščen revizorka z dovoljenjem za dajanje zagotovil o trajnostnosti

Direktorica v reviziji, Deloitte Revizija d.o.o.

Članica Sveta za poročanje o trajnostnosti, SiR

Gradivo je last Slovenskega inštituta za revizijo in je predmet avtorske zaščite in drugih oblik zaščite intelektualne lastnine. Prepovedano je kakršnokoli reproduciranje, razen izključno za osebno uporabo in v nekomercialne namene, pri čemer se morajo ohraniti vsa opozorila o avtorskih ali drugih pravicah, zato se ne smejo prepisovati, razmnoževati ali kako drugače razširjati. Naveden mora biti tudi vir.

- Kratek povzetek vsebine revizije ESG
- Vključenost revizorja informacijskih sistemov pri trajnostnem poročanju
 - Revizor informacijskih sistemov kot del ekipe pripravljavcev poročil
 - Revizor informacijskih sistemov kot del ekipe zunanjega revizorja
- Zaključek

Trajnostno poročanje se je v zadnjem desetletju razvilo v enega ključnih instrumentov za transparentnost poročanja in odgovornost družb.

V ospredje stopajo okoljski, družbeni in upravljavski (ESG) vidiki, ki dopolnjujejo tradicionalno finančno računovodsko poročanje.

Z Direktivo EU o korporativnem trajnostnem poročanju (v nadaljevanju direktiva CSRD) in **Evropskimi standardi za poročanje o trajnosti** (v nadaljevanju ESRS) je obveznost priprave trajnostnih poročil postala realnost za številne družbe v Evropski uniji.

Kratika ESG pomeni v angleščini *Environmental, Social, and Governance*, oziroma v slovenščini:

- **E – Okoljski (Environmental):** kako družba vpliva na okolje – npr. poraba energije, emisije CO₂, ravnanje z odpadki, uporaba naravnih virov ipd.
- **S – Družbeni (Social):** kako družba vpliva na družbo – npr. odnosi z zaposlenimi, spoštovanje človekovih pravic, varnost pri delu, raznolikost in vključenost, vpliv na lokalno skupnost.
- **G – Upravljanje (Governance):** kako je družba vodena – npr. preglednost poslovanja, etika uprave, skladnost z zakonodajo, sestava upravnih odborov, preprečevanje korupcije.

Kratika CSRD (Corporate Sustainability Reporting Directive) se nanaša Direktivo (EU) 2022/2464 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o spremembi Uredbe (EU) št. 537/2014, Direktive 2004/109/ES, Direktive 2006/43/ES in Direktive 2013/34/EU glede poročanja družb o trajnostnosti.

- Določene družbe so bile skladno z EU direktivo in lokalno zakonodajo (določila ZGD-1) **v letu 2024 prve zavezane k** pripravi poročil o trajnostnosti.
- Iz prakse lahko vidimo, da so bila pri pripravi trajnostnostnih poročil **v prvem letu uporabljena osnovna analitična orodja**, ki temeljijo večinoma na MS Excel tabelah, z razvojem poročanja v družbah, ki bodo zavezane k pripravi trajnostnostnih poročil v prihodnjih letih in z njihovo zrelostjo, pa pričakujemo, da se bo priprava teh priporočil v prihodnje avtomatizirala na podoben način, kot imajo družbe urejene procese računovodskega poročanja.
- S tem se bo tudi **vloga IT revizorjev** tako pri pripravi kot tudi pri reviziji trajnostnostih poročil **pomembno povečala** in bodo IT revizorji predstavljali zagotovo nepogrešljiv del specialistov, revizorjevih veščakov.

Kdo poroča? (nadaljevanje)

- Za leto 2024 so bile zavezane k poročanju o trajnostnosti v Sloveniji tiste družbe, ki so že bile zavezane po pretekli direktivi o nefinančnem poročanju, torej:
 - velike družbe, ki so subjekti javnega interesa in imajo povprečno več kot 500 zaposlenih, in
 - obvladujoče družbe (skupine), ki skupaj z odvisnimi družbami dosegajo kriterije za velike družbe ter imajo prav tako v skupini več kot 500 zaposlenih.
- To je določeno v prehodnih določbah ZGD-1M za poročevalce, ki so bili že prej pod obveznostjo iz nefinančnega poročanja.

Kaj je poročanje o trajnostnosti?

- **Trajnostno poročanje** (ang. *sustainability reporting*) je proces, s katerim družbe javno razkrivajo informacije o svojem vplivu na okolje, družbo in gospodarstvo. Gre za poročila, ki presegajo zgolj finančne rezultate, saj zajemajo tudi nefinančne kazalnike, ki kažejo, kako družbe delujejo v širšem družbenem, okoljskem in upravljavskem kontekstu.
- **Osrednji namen** trajnostnega poročanja je zagotoviti **transparentnost**. Družbe s tem **deležnikom** – vlagateljem, zaposlenim, potrošnikom, lokalnim skupnostim, regulatorjem ter drugim – omogočijo vpogled v svoje okoljske, družbene in upravljavske prakse.

Kaj je poročanje o trajnostnosti?

- Med ključne teme, ki jih družbe običajno vključijo, sodijo:
 - **okoljski vidiki:** poraba energije in vode, emisije toplogrednih plinov, ravnanje z odpadki, uporaba naravnih virov, krožno gospodarstvo.
 - **družbeni vidiki:** pravice zaposlenih, varnost in zdravje pri delu, enakost spolov, spoštovanje človekovih pravic, vpliv na lokalne skupnosti.
 - **upravljavski vidiki:** etično poslovanje, protikorupcijski ukrepi, struktura upravljanja, preglednost odločanja.

Za družbe precej drugačne teme, kot so obravnavne pri računovodskem poročanju!

- Namen revizije je potrditi, da so razkritja o trajnostnosti **resnična, popolna in skladna z zahtevami ESRS**.
- Revizor mora presoditi, ali družba ustrezno poroča o svojih vplivih na okolje, družbo in upravljanje ter ali so uporabljene metode merjenja in izračuni skladni z določili evropske zakonodaje.
- Omenjeno mora revizor opraviti skladno z **določili Mednarodnega standarda poslov dajanja zagotovil 3000 (prenovljen) - Posli dajanja zagotovil, razen revizij ali preiskav računovodskih informacij*** iz preteklosti s pridobitvijo omejene ravni zagotovila (*ang. limited assurance*)

*MSZ 3000 (prenovljen)

- Revizor informacijskih sistemov predstavlja pomembno podporo tako pripravljalcem, kot tudi revizorjem trajnostnostnih poročil.
- Gre za dve različni vlogi, zato v nadaljevanju izpostavljam vsako vlogo ločeno kot del posamezne ekipe glede na perspektivo, s katere sodeluje.
 1. Revizor informacijskih sistemov kot del ekipe pripravljavcev poročil
 2. Revizor informacijskih sistemov kot del ekipe zunanjega revizorja

IT revizor s svojim znanjem lahko pomembno prispeva pri vključenosti v naslednja področja:

a) pregled učinkovitosti informacijskih rešitev, ki zbirajo podatke za pripravo poročil o trajnostnosti

Primer: Sodelovanje IT oddelka in IT revizorja pri uvedbi informacijskega sistema za trajnostno poročanje

Družba XYZ d.o.o. je želela izboljšati kakovost in preglednost svojih trajnostnih poročil, zato se je odločila za uvedbo integrirane informacijske platforme, ki bo omogočala samodejno zbiranje podatkov o porabi energije, emisijah CO₂, odpadkih in varnosti pri delu.

V fazi načrtovanja je IT oddelek analiziral obstoječe sisteme in ugotovil, da trenutni ERP in poročila, pripravljena z orodjem MS Excel ne omogočajo zanesljive konsolidacije podatkov. Skupaj z zunanjim ponudnikom so izbrali rešitev za trajnostno poročanje, ki omogoča integracijo z obstoječimi merilnimi napravami in finančnimi sistemi.

Že v tej fazi je bil vključen IT revizor, ki je preveril:

- ali izbrana rešitev omogoča sledljivost podatkov in revizijske sledi,
- ali ponudnik izpolnjuje varnostne standarde,
- ter ali sistem zagotavlja zaščito osebnih podatkov skladno z zakonodajo.

Hkrati je tudi svetoval pri izbiri IT rešitve.

Po implementaciji je IT revizor sodeloval pri testiranju prenosa podatkov iz merilnikov v informacijski sistem, preveril, ali avtomatski preračuni emisij delujejo pravilno, in ocenil zanesljivost varnostnih kopij.

b) oceno ustreznosti notranjih kontrol in procesov validacije

Primer: Vloga IT revizorja pri preverjanju notranjih kontrol v informacijskih sistemih

- Družba XYZ d.o.o., ki deluje v kemični panogi, uporablja integrirani ERP sistem, preko katerega potekajo ključni poslovni procesi — od nabave surovin in finančnega poročanja do zbiranja podatkov o porabi energije, količini odpadkov in emisijah za trajnostno poročanje.
- Ker družba pripravlja poročilo o trajnostnosti skladno z evropsko direktivo CSRD, se je odločila preveriti, ali informacijski sistem vsebuje dovolj zanesljive notranje kontrole, ki preprečujejo napake ali manipulacije s podatki.

V pregled je bil vključen IT revizor, ki je skupaj z IT oddelkom izvedel naslednje:

- pregledal je implementirane kontrole dostopov: revizor je preveril, ali imajo uporabniki, ki vnašajo okoljske podatke, omejene pravice (npr. samo za vnos, ne pa tudi za brisanje ali spreminjanje zapisov).
- testiral delovanja validacijskih pravil: izvedel je testni vnos podatka o porabi energije, ki presega dovoljene meje, da preveri, ali sistem samodejno prikaže opozorilo.
- presodil postopek odobritve (avtorizacije): preveril je, ali sistem zahteva potrditev vnesenih podatkov s strani odgovorne osebe, preden se uporabijo v poročilu.

- Preveril, ali obstajajo ustrezne revizijske sledi: analiziral je, ali sistem beleži, kdo in kdaj je spreminjal posamezne vrednosti ter ali se te spremembe hranijo v arhivu.

Rezultat sodelovanja je bil izboljšan nadzor nad kakovostjo in sledljivostjo podatkov, kar je družbi omogočilo pripravo zanesljivega trajnostnega poročila, hkrati pa zmanjšalo tveganje za napake v poročilu o trajnostnosti.

Primer: Zagotavljanje sledljivosti podatkovnih tokov za kazalnik “sestava uprave in nadzornega sveta po spolu”

- Družba XYZ, finančna družba z več kot 500 zaposlenimi, mora v skladu z ESRS S1 in ESRS G1 razkriti kazalnik o sestavi uprave in nadzornega sveta po spolu, vključno z deležem žensk v vodstvenih položajih. Ti podatki se pridobivajo iz kadrovskega informacijskega sistema, ki vsebuje osebne podatke zaposlenih, ter se nato konsolidirajo v poročilo o trajnostnosti.
- Vodstvo družbe je pri pripravi poročila ugotovilo, da ni povsem jasno, od kod prihajajo uporabljeni podatki in kdo je odgovoren za njihovo potrjevanje – kar je predstavljalo tveganje za točnost in popolnost poročila o trajnostnosti.

Primer: Zagotavljanje sledljivosti podatkovnih tokov za kazalnik “sestava uprave in nadzornega sveta po spolu”

Zato je bil v proces vključen IT revizor, ki je:

- analiziral podatkovni tok – sledil je poti podatkov od vnosa v kadrovski informacijski sistem (kjer se beležijo osnovni podatki zaposlenih), prek baze upravljavskih funkcij v kadrovski službi, do končne tabele, ki se uporablja za poročanje o trajnostnosti;
- preveril sledljivost sprememb – ugotovil, da kadrovski informacijski sistem ne beleži dovolj natančnih revizijskih sledi za spremembe statusa zaposlenih (npr. spremembe funkcij ob napredovanju);
- določil odgovorne osebe – skupaj z vodjo kadrovske službe je pripravil matriko odgovornosti, ki določa, kdo vnaša, preverja in potrjuje podatke o članih uprave in nadzornega sveta;
- svetoval glede transparentnosti – priporočil je, da se v poročilu jasno navede vir podatkov (kadrovski informacijski sistem), datum posodobitve in uporabljeno metodologijo.

d) preverjanje uporabe pravih metodologij in izračunov, zlasti v avtomatiziranih sistemih

Vloga IT revizorja pri svetovanju o implementaciji preverjanja pravih metodologij in izračunov v avtomatiziranih sistemih je ključna za zagotavljanje integritete in zanesljivosti podatkov v digitalnem okolju.

Z interdisciplinarnim znanjem iz IT, revizije in upravljanja tveganj IT revizor družbi pomaga vzpostaviti ustrezne notranje kontrole, ki zagotavljajo pravilnost, sledljivost in skladnost izračunov skozi procesni del informacijskega sistema.

Družba XYZ, ki deluje na področju zdravstvene opreme, pripravlja trajnostno poročilo skladno z ESRS S1 – Lastna delovna sila. Za poročanje uporablja kadrovski informacijski sistem in analitično podporo temu sistemu, ki samodejno izračunava več socialnih kazalnikov, med drugim:

- stopnjo fluktuacije zaposlenih,
- povprečno število ur usposabljanja na zaposlenega,
- delež zaposlenih, ki so vključeni v programe varnosti in zdravja pri delu,
- delež zaposlenih s pogodbami, sklenjenimi za določen čas.

Vodstvo družbe je zaznalo tveganje, da avtomatizirani algoritmi morda niso usklajeni z metodologijami, določenimi v internih politikah in ESRS standardih.

Primer: Vloga IT revizorja pri preverjanju avtomatiziranih izračunov socialnih kazalnikov

IT revizor je bil vključen kot svetovalec in je:

- pregledal logiko in metodologijo izračunov (algoritmov) – preveril je, ali kadrovski informacijski sistem uporablja pravilne definicije in časovne intervale pri izračunu fluktuacije in usposabljanj.
- skupaj z IT oddelkom testiral pravilnost izračunov – izvedel je test s simuliranimi podatki (npr. 100 zaposlenih, 5 odhodov, 3 novi zaposlitve) in primerjal rezultat sistema s ročnim izračunom, da potrdi pravilnost izračuna/algoritma.
- presojal skladnost z ESRS S1 – preveril, ali so izračuni skladni s standardom glede načina merjenja (npr. ali je uporabljena ustrezna metodologija).
- svetoval o vzpostavitvi notranjih kontrol – predlagal je uvedbo revizijske sledi za vsako spremembo metodologije izračuna in avtomatizirano obvestilo, če pride do nenavadnih odstopanj pri kazalnikih.

Skladno z določili 12. odstavka MSZ 3000 (prenovljen) so **dokazi** »informacije, ki jih uporabi praktik pri oblikovanju svojega sklepa. Dokazi zajemajo tako informacije, ki jih vsebujejo ustrezni informacijski sistemi, če obstajajo, in druge informacije.«

Revizor, ki revidira poročilo o trajnostnosti se tako **lahko odloči**, ali bo v plan revizijskih postopkov vključil tudi zanašanje na delovanje informacijskega sistema, ki je podpora pripravljavcem poročila o trajnostnosti.

a) sodelovanje pri načrtovanju in izvedbi revizijskih postopkov, kjer so informacijski sistemi ključni za pridobivanje dokazov o točnosti in popolnosti razkritij v trajnostnem poročilu

Njegove ključne naloge so:

- identifikacija ključnih informacijskih sistemov in aplikacij, ki se uporabljajo za zajem in obdelavo podatkov, ki so osnova za pripravo poročila o trajnostnosti (npr. ERP sistemi, okoljski informacijski sistemi, orodja za zbiranje podatkov o energiji, idr.);
- analiza povezav med sistemi in tokov podatkov (*ang. data flow mapping*), da se razume, kje v procesu lahko pride do izgube, spremembe ali napačne pretvorbe podatkov;
- presoja tveganj napačnega poročanja zaradi pomanjkljivosti v informacijskih sistemih in splošnih računalniških kontrolah; in
- določitev obsega in narave revizijskih testov, ki bodo izvedeni z uporabo podatkov iz informacijskih sistemov.

Primer:

V družbi, ki poroča o emisijah CO₂, IT revizor v **fazi načrtovanja** ugotovi, da se podatki o porabi goriva **zbirajo prek avtomatiziranih senzorjev, povezanih z energetske informacijskim sistemom**. Na podlagi tega revizijska ekipa načrtuje testiranje popolnosti in točnosti prenosa teh podatkov v sistem za trajnostno poročanje in preverjanje kontrolnih mehanizmov, ki preprečujejo ročne spremembe.

b) pomoč glede tveganj informacijske tehnologije, ki lahko vplivajo na zanesljivost trajnostnega poročanja

Prvi korak je, da IT revizor skupaj z revizijsko ekipo identificira IT tveganja, povezana s procesi zbiranja in poročanja trajnostnih podatkov.

To vključuje tveganja, kot so napake v avtomatiziranih preračunih emisij, izguba podatkov zaradi pomanjkljivih varnostnih kopij, nepooblaščen dostop ali manipulacija podatkov, pomanjkljivo beleženje sprememb (manjkajoče revizijske sledi), odvisnost od zunanjih ponudnikov IT storitev (npr. oblačnih rešitev), kibernetiske grožnje, ki bi lahko vplivale na razpoložljivost ali integriteto podatkov.

Primer:

IT revizor ugotovi, da družba uporablja zunanjo aplikacijo za izračun emisij toplogrednih plinov, vendar ni pogodbenih določil o varnostnih kopijah in zaščiti podatkov. To predstavlja tveganje izgube ali spremembe podatkov, ki bi lahko vplivala na popolnost poročila o trajnostnosti.

- IT revizor nato presodi, kako posamezno tveganje lahko vpliva na kakovost in zanesljivost trajnostnih informacij.
- Pri tem upošteva verjetnost nastanka tveganja, potencialni vpliv na trajnostno poročilo, obstoječe kontrolne mehanizme in njihovo učinkovitost.

- Primer:
Če sistem za merjenje emisij CO₂ ni zaščiten pred ročnimi popravki podatkov, je tveganje za napačno poročanje visoko. IT revizor zato priporoči testiranje revizijskih sledi in preverjanje avtorizacijskih kontrol, preden se podatki uporabijo pri oblikovanju trajnostnega poročila.

c) presoji zanesljivosti informacijskih sistemov in aplikacij, ki se uporabljajo za zbiranje, obdelavo in poročanje podatkov o trajnostnih kazalnikih

Ocena zanesljivosti in integritete informacijskih sistemov: IT revizor presoja, ali informacijski sistemi delujejo skladno s predvidenimi zahtevami in ali zagotavljajo zanesljivo obdelavo trajnostnih podatkov.

To vključuje preverjanje, ali so sistemi stabilni, redno vzdrževani in zaščiteni pred morebitnimi tehničnimi ali varnostnimi incidenti, ki bi lahko vplivali na točnost in razpoložljivost podatkov

- **Primer:**

Družba uporablja informacijski sistem za spremljanje porabe energije po proizvodnih linijah. IT revizor preveri, ali se ob posodobitvah programske opreme (npr. spremembi algoritmov za izračun porabe) vodi dokumentacija o spremembah, kdo jih je odobril in kdaj so bile implementirane. Tako se prepreči, da bi neodgovorne ali nenadzorovane spremembe vplivale na točnost poročanih podatkov o porabi energije.

Pregled kontrol okolja informacijske tehnologije:

Pomemben del presojanja zanesljivosti informacijskih sistemov predstavlja analiza splošnih računalniških kontrol, kot so kontrole dostopa, kontrole sprememb programskih rešitev, varnostne kopije in postopki za obnovitev po izpadu sistema.

IT revizor preverja, ali družba uporablja ustrezne mehanizme za zaščito podatkov pred nepooblaščenim dostopom, izgubo ali spremembo, ter ali obstajajo učinkoviti postopki za varno arhiviranje in obnavljanje podatkov.

Primer:

V družbi, ki poroča o emisijah CO₂, IT revizor preveri, ali so podatki o porabi goriva in električne energije zaščiteni z ustreznimi pravicami dostopa — npr. da lahko podatke vnašajo samo pooblaščene osebe, ne pa tudi uporabniki iz drugih oddelkov. Prav tako preveri, ali se dnevno izdelujejo varnostne kopije baz podatkov, in ali obstaja načrt za obnovo po morebitnem izpadu sistema (ang. disaster recovery plan).

d) pregledu notranjih kontrol v informacijskih sistemih, povezanih s pridobivanjem trajnostnih podatkov (npr. nadzora nad vnosom podatkov, dostopnimi pravicami, avtorizacijami, revizijskimi sledmi ipd.)

IT revizor preverja, ali so v informacijskih sistemih vzpostavljene vhodne in obdelovalne kontrole, ki zmanjšujejo tveganje napačnega, nepopolnega ali nepooblaščenega vnosa podatkov.

IT revizor ocenjuje tudi **kontrole avtorizacije**, s katerimi se potrjuje točnost in popolnost podatkov pred njihovo vključitvijo v poročilo. Preverja, ali obstajajo formalizirani postopki za odobritev ključnih trajnostnih kazalnikov, ali so določene odgovorne osebe za pregled in potrditev podatkov ter ali sistem omogoča elektronske evidence o odobritvah.

e) ocena integritete, točnosti in popolnosti podatkov, ki se prenašajo med različnimi informacijskimi viri

- IT revizor preveri, ali so podatki, ki jih družba uporablja za trajnostno poročanje, **celoviti, pravilni in dosledni v vseh fazah prenosa** — od zajema podatkov v operativnih sistemih (npr. merilnih napravah, ERP sistemih) do končne konsolidacije v trajnostnih poročilih.
- To vključuje **sledenje poti podatkov** (*ang. data lineage*), preverjanje avtomatiziranih preračunov, primerjavo med izvirno in poročano vrednostjo ter odkrivanje morebitnih izgub, podvajanj ali napačnih pretvorb podatkov.

- Trajnostno poročanje je postalo nepogrešljiv del **sodobnega korporativnega upravljanja in transparentnosti poslovanja**.
- Z uveljavitvijo evropske **direktive CSRD** ter **standardov ESRS** so družbe v Evropski uniji zavezane ne le k razkrivanju finančnih informacij, temveč tudi k celovitemu poročanju o svojih vplivih na okolje, družbo in upravljanje.
- Takšno poročanje pa zahteva visoko raven zanesljivosti in sledljivosti podatkov, kar je mogoče zagotoviti le z **učinkovitim delovanjem informacijskih sistemov** in ustreznimi notranjimi kontrolami.

Njegovo interdisciplinarno znanje, ki **združuje razumevanje informacijske tehnologije, revizijskih postopkov in upravljanja tveganj**, omogoča celovit pristop k preverjanju in izboljševanju procesov zbiranja, obdelave in poročanja trajnostnih podatkov.

V prihodnjih letih se bo pomen IT revizorjev še povečal, saj bo digitalizacija procesov poročanja in uporaba naprednih tehnologij (kot so umetna inteligenca in avtomatizacija) zahtevala **dodatno strokovno presojo tveganj, točnosti in skladnosti podatkov**.

IT revizor bo tako postal nepogrešljiv člen pri zagotavljanju zanesljivosti informacij, na podlagi katerih podjetja ne le izpolnjujejo zakonske obveznosti, temveč gradijo tudi zaupanje vlagateljev, regulatorjev in širše javnosti.

Kontakt:

Nina Kravanja Novak

nkravanjanovak@deloittece.com

Tel. št.: 051 280 003

