Obvladovanje tveganj pri oddajanju storitev v zunanje izvajanje (outsourcing) in predstavitev Tematske zahteve »Third Party Topical requirement«

Pozavarovalnica Sava, d.d.
Polonca Jug Mauko | mag. Miha Ozimek

02. junij 2026

Predstavitev avtorjev

Polonca Jug Mauko, PNR, PDNR

Notranja revizija, Pozavarovalnica Sava, d.d.

- Vodi službo notranje revizije, nosilka ključne funkcije notranje revizije Zavarovalne skupine Sava, Save Re in Zavarovalnice Sava
- Predstavlja izkušnje z izvajanjem zunanjega izvajanja in revidiranjem zunanjega izvajanja po zakonodajnih zahtevah in tematski zahtevi standarda

mag. Miha Ozimek, PRIS, CISA, CIA, ISO/IEC 27001, ISO 22301

Notranja revizija, Pozavarovalnica Sava, d.d.

- Skrbi za področje notranje revizije v okviru IT
- Praktične izkušnje s cloud, SaaS in DORA
- Predstavlja **IT del**: ICT outsourcing,

Pregled vsebine

1

Uvodne misli

Zakaj outsourcing zavarovalniško industrijo zanima vse bolj

Trendi · Tveganja · Regulatorni pritisk

2

Splošni del, predstavitev Tematske zahteve

Regulativa, načela, življenjski cikel pogodbe, Tematska zahteva »Third Party Topical Requirement« na primeru

Solvency II · EIOPA · AZN · GIAS

3

IT del

ICT outsourcing, kibernetska varnost, DORA

Cloud · SaaS · Subcontracting

4

Zaključek

Ključna sporočila in razprava

Lessons learned · Q&A

Zakaj nas ta tema vse bolj zadeva

Zunanje izvajanje ni več periferno – postaja jedro poslovanja

Vedno več

delovnih procesov se v zavarovalništvu opira na zunanje izvajalce – izločeni posli ZSS (znotraj skupine/zunaj)

Mdr. funkcija informacijske tehnologije, informacijske varnosti, gospodarjenja s finančnimi instrumenti, skladnost, aktuarske funkcije, obdelave škodnih primerov.

2025 - 2026

DORA je postala v celoti zavezujoča, RTS so se začeli izvajati

Operativna digitalna odpornost ni več projekt – je merilo dnevnega delovanja.

Vedno bolj natančno določeni procesi za zagotavljanje odpornosti poslovanja

Povišana

zaznava incidentov pri tretjih osebah v zadnjih 3 letih

Kibernetski napadi, izpadi oblaka in odvisnost od enega ponudnika postajajo sistemsko tveganje.

Outsourcing ni več zgolj operativna odločitev – je strateško tveganje, ki ga moramo aktivno upravljati.

Kaj sploh je zunanje izvajanje – izločen posel?

Zzavar-1 – izločen posel:

Izločeni posel je funkcija oziroma aktivnost zavarovalnice, dana v zunanje izvajanje, ki je ključna oziroma pomembna za poslovanje zavarovalnice. Zunanje izvajanje pomeni kakršen koli dogovor med (po)zavarovalnico in prevzemnikom storitev, ki je nadzorovani ali nenadzorovani subjekt, v skladu s katerim prevzemnik storitev neposredno ali posredno opravlja proces, storitev ali dejavnost, ki bi jo sicer opravljala (po)zavarovalnica sama.

Pomembno: ne glede na to, ali je izvajalec del skupine ali zunanji partner.

✓ JE izločen posel	✕ NI izločen posel
• Notranja revizija / ključne funkcije • Aktuarski izračuni pri zunanjem partnerju • Cloud / SaaS aplikacije • Gospodarjenje s finančnimi instrumenti • Likvidacija škod pri partnerski družbi • IT podpora in razvoj	• Najem pisarn in stavbnih storitev • Nakup standardne programske opreme • Enkratno svetovanje (npr. pravno mnenje) • Klasično pošiljanje in dostava • Komunalne storitve

Pomembna zakonodaja in smernice

Solvency II direktiva

EU regulativa za zavarovalnice

- Člen 49: izvajalec mora omogočiti nadzor
- Stalna odgovornost zavarovalnice
- Pisni dogovor s ključnimi pogoji

AZN sklep o sistemu upravljanja

Slovenski nadzornik

- Predhodno obvestilo AZN za pomembne pogodbe
- Pisna politika zunanjega izvajanja

ZZavar-1 in EIOPA smernice

Zakonska podlaga in evropska praksa

- ZZavar-1: ureditev zunanjega izvajanja
- EIOPA smernice o ICT outsourcingu
- EIOPA smernice o sistemu upravljanja

DORA (Uredba 2022/2554)

Operativna odpornost & ICT (od 17.1.2025)

- Strožja pravila za ICT izvajalce
- Register ICT dogovorov v EU formatu
- Testiranje odpornosti in odzivanje

Trije temeljni principi zunanjega izvajanja

1

Stalna odgovornost

- Tudi po oddaji zunanjemu izvajalcu odgovornost ostane na zavarovalnici
- Uprava ne sme/ne more prenesti svoje skrbnosti
- Ne sme se poslabšati kakovost upravljanja zavarovalnice
- "Outsourcing ni outsource-and-forget"

2

Ohranjen nadzor

- Zunanje izvajanje ne sme ovirati nadzora AZN
- Izvajalec mora omogočiti revizijo in inšpekcijo
- Dostop do podatkov in prostorov

3

Brez škode zavarovancem

- Storitve za stranke morajo ostati enako kakovostne, ustrezne in stalne
- Zaščita osebnih podatkov in zaupnosti
- Nadaljevanje poslovanja ob izpadu

Pomembno vs. običajno zunanje izvajanje

Pomembna funkcija

Zahteve nadzornika:

- Predhodno obvestilo AZN – pisna podrobna analiza izločenega posla, osnutek pogodbe posredovati 6 tednov pred sklenitvijo
- Strožja izhodna strategija (exit plan)
- Pisna politika in stalen monitoring
- Pogodbeni pogoji po SII čl. 49, Zzavar-1

Tipični primeri:

- *Notranja revizija, skladnost, aktuarska funkcija, funkcija upravljanja tveganj (ključne funkcije)*
- *Investicijsko upravljanje*
- *Ključne ICT storitve (core sistemi)*

Običajno zunanje izvajanje

Zahteve nadzornika:

- Vključeno v register zunanjega izvajanja
- Osnovna pisna pogodba
- Redno spremljanje izvajalca
- Brez predhodnega obvestila AZN

Tipični primeri:

- *Čiščenje in vzdrževanje prostorov*
- *Pisarniške storitve*
- *Standardna IT podpora (helpdesk)*
- *Tisk in pošiljanje korespondence*

Življenjski cikel zunanjega izvajanja

1 Analiza potreb	2 Izbira izvajalca	3 Pogodba in pristop	4 Izvajanje in nadzor	5 Izstop ali sprememba
• Poslovna utemeljitev • Ocena tveganj in pomembnosti • Notranja zmožnost vs. outsourcing	• Due diligence • Tehnične in finančne reference • Skladnost in varnost	• SLA in KPI-ji • Klavzule po SII čl. 49, 4.6. poglavje Zzavar-1 • Pravica do nadzora in revizije	• Stalno spremljanje SLA • Periodični pregledi • Poročanje upravi	• Vnaprej določen exit plan • Prenos podatkov in storitev • Kontinuiteta poslovanja

Analiza procesa in due diligence

1. Analiza procesa

- Ali je smiselno oddati zunaj?
- Ali gre za pomembno (kritično) funkcijo?
- Stroškovna analiza in analiza tveganj
- Razpoložljivost znanja v hiši
- Skladnost s strategijo družbe

2. Due diligence izvajalca

- Finančna stabilnost in lastništvo
- Reference in dosedanje izkušnje
- Tehnične zmogljivosti in certifikati
- ICT varnost (ISO 27001, IEC 62443)
- Lokacija obdelave podatkov (GDPR)

Due diligence ni enkraten dogodek — periodično preverjanje vsaj enkrat letno za pomembne funkcije.

Pogodba in ključne klavzule (Solvency II, čl. 49)

1 Predmet in obseg
Natančen opis storitev, KPI in raven kakovosti (SLA).

2 Pravica do nadzora
Dostop AZN, notranje revizije in pooblaščenih revizorjev.

3 Varstvo podatkov
GDPR, lokacija obdelave, ukrepi varovanja, podpogodbeniki.

4 Poročanje in incidenti
Periodična poročila, takojšnja eskalacija incidentov.

5 Sub-outsourcing
Predhodno soglasje za bistvene podpogodbenike.

6 Izstopna strategija
Razlogi za odpoved, prehod podatkov, kontinuiteta.

Spremljanje izvajalca in poročanje

KPI

- Razpoložljivost storitve (npr. 99,9 %)
- Čas odziva in reševanja
- Število incidentov mesečno
- Točnost obdelave podatkov

SLA

- Določene ravni storitev s pragovi
- Pogodbene kazni pri prekršitvi
- Mesečna SLA poročila
- Eskalacijski postopek

Nadzor

- Letni pregled in re-due-diligence
- On-site preverjanje (po potrebi)
- Spremljanje finančnega zdravja
- Pregled sub-outsourcing

Cloud ponudnik s 99,5 % razpoložljivostjo namesto pogodbenih 99,9 % — pogodbena kazen + analiza vzroka + plan ukrepov v 30 dneh.

Posebne teme: konflikti, sub-outsourcing, čezmejnost

Konflikt interesov

- Izvajalec dela še za konkurente
- Lastniške/osebne povezave
- Identificirati pred sklenitvijo pogodbe

Primer:

Skupna IT družba opravlja outsourcing za dve konkurenčni zavarovalnici.

Sub-outsourcing

- Izvajalec naprej oddaja delo tretji osebi
- Predhodno soglasje zavarovalnice
- Veriga odgovornosti mora ostati jasna

Primer:

Glavni izvajalec šifrira podatke pri pod-izvajalcu izven EU.

Čezmejnost

- Izvajalec ali podatki izven EU/EGP
- Standardne pogodbene klavzule (SCC)
- Tveganje zaradi tujih jurisdikcij

Primer:

Hyperscale cloud z regijo Frankfurt + replika v ZDA — dodatne klavzule.

Tematska zahteva

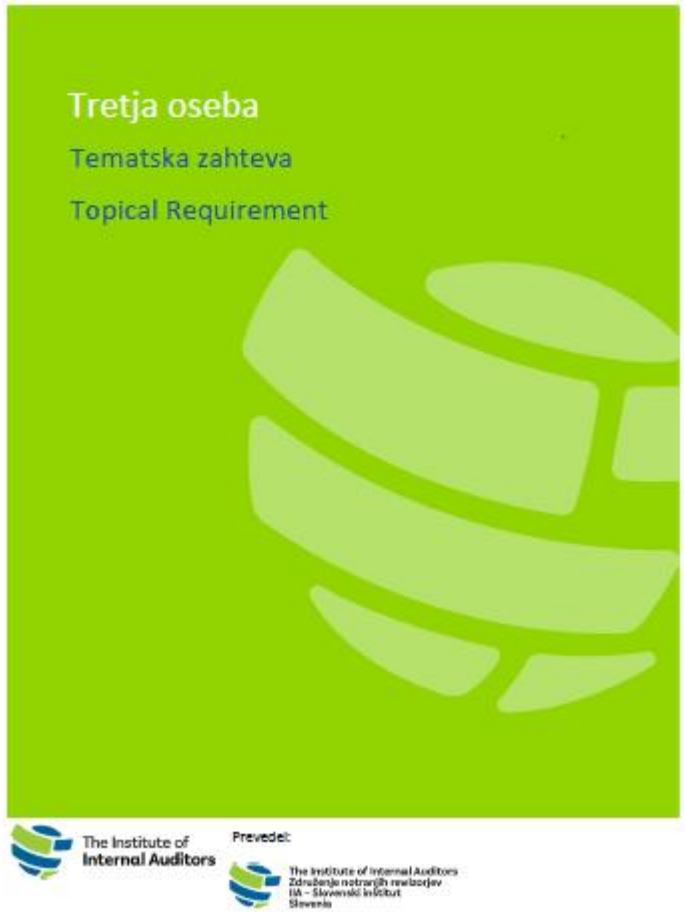
https://www.theiia.org/en/standards/2024-standards/topical-requirements/

https://www.theiia.org/en/standards/2024-standards/topical-requirements/third-party/

Veljavna od 15. septembra 2026.

Minimalna izhodišča za revidiranje.

Izraz "tretja oseba" je lahko opredeljen in uporabljen različno glede na panogo ali druge kontekste. Notranjim revizorjem je zagotovljena prožnost in se morajo pri prilagajanju tematske zahteve opredelitvi tretje osebe v izvorni organizaciji zanašati na svojo strokovno presojo.



Glavna tveganja pri zunanjem izvajanju – primer zunanje izvajanje NR, lahko se uporabi kot samoocenitev delovanja

Strateško/Ugled

Nepravilna izbira partnerja škoduje ugledu in dolgoročni konkurenčnosti.

Pravno / Skladnostno

Neskladje z AZN/EIOPA/SII, kazni regulatorja, slabe pogodbene klavzule

Operativno tveganje

Izvajalec ne dostavi v dogovorjenem času ali kakovosti; izpadi procesov.

Koncentracija

Preveč ključnih storitev pri istem izvajalcu (vendor lock-in, single point of failure).

Sub-outsourcing

Izvajalec naprej oddaja delo brez vedenja zavarovalnice; izguba nadzora.

Zaupnost podatkov / kibernetska varnost

Razkritje občutljivih podatkov strank, GDPR kršitve, izguba zaupanja.

Glavna tveganja pri zunanjem izvajanju

Finančna tveganja

Plačilna nesposobnost, prevare

Tveganje informacijske tehnologije

Pomanjkanje storitev za podporo kritičnih nalog

ESG tveganja

Vpliv zunanjega izvajalca na ESG

Geopolitična tveganja

Vojne, politična nestabilnost

Etika

Pomanjkanje integritete, navzkrižje interesov, podkupnine

UPRAVLJANJE TRETJIH OSEB

A) Formalni pristop

Način kako se določi da se izbere tretjo osebo. Standardiziran in jasno določen proces. Cost-benefit analiza. Poslovodska ocena tveganj in kontrol. Pričakovanja deležnikov. Viri za obvladovanje delovanja v odnosu do tretje osebe – pogodba, upravljanje, nadzor.

B) Vzpostavljene politike

Vsebujejo opredelitev, oceno in obvladovanje odnosov in tveganj s tretjimi osebami v celotnem življenjskem ciklu tretjih oseb. Usklajenost z regulativo, redno posodabljajo.

C) Opredeljene so vloge in odgovornosti

Kdo izbira, usmerja, vodi, se sporazumeva in spremlja tretje osebe ter kdo mora biti obveščen o dejavnostih tretjih oseb. Ustrezne kompetence. Redna izobraževanja. Etika, ESG.

D) Pravila postopanja za sporazumevanje

Opredeljena so pravila za sporazumevanje z ustreznimi deležniki, ki vključujejo pravočasno poročanje o stanju uspešnosti, tveganjih in skladnosti (zlasti o kršitvah zakonov in predpisov) prednostno razvrščenih tretjih oseb.

UPRAVLJANJE TRETJIH OSEB – primer kaj vsebuje Politika

B) Vzpostavljene politike - zahteva Zzavar-1, 171. člen, 2. odstavek

Zavarovalnica v zvezi z izločenimi posli sprejme akt, s katerim določi pristop k izločenem poslu in postopke izvajanja izločenih poslov za čas trajanja pogodbe o izločenem poslu, kar vključuje zlasti:

1. kriterij določitve, ali je funkcija oziroma aktivnost ključna oziroma pomembna;
2. način izbora prevzemnika izločenega posla ustrezne kakovosti in način oziroma pogostost ocenjevanja njegovih rezultatov oziroma izvajanja storitev;
3. metode in postopek spremljanja skladnosti in učinkovitosti izvajanja izločenega posla;
4. pogoje, ki jih izpolnjuje prevzemnik izločenega posla;
5. druge sestavine, ki se vključijo v pogodbo s prevzemnikom izločenega posla

OBVLADOVANJE TVEGANJ TRETJIH OSEB

A) Procesi za obvladovanje tveganj

Procesi za obvladovanje tveganj tretjih oseb in njihovih storitev so standardizirani in vseobsegajoči, vključujejo opredeljene vloge in odgovornosti ter zadostno obravnavajo ključna tveganja, pomembna za organizacijo. Izvajajo se korektivni ukrepi za vsa odstopanja.

B) Tveganja se redno prepoznajo in ocenjujejo

Tveganja se redno prepoznajo in ocenjujejo. Odzivi na tveganja so prav tako razvrščeni in razvrščeni po pomembnosti. Ocena tveganj se redno pregleduje in posodablja.

C) Odzivi na tveganja

Odzivi na tveganja so ustrezni in natančni ter sorazmerni z razvrstitvijo. Odzivi na tveganj se izvajajo, pregledujejo, potrjujejo, spremljajo, ocenjujejo in po potrebi prilagajajo.

D) Vzpostavljeni procesi za obvladovanje in po potrebi stopnjevanje težav

Proces obravnavanja pritožb /težav, ovrednoteni vplivi na poslovanje in po potrebi izvede nadaljnje ukrepe, odpravo ali prekinitev

KONTROLE TRETJIH OSEB – po pomembnosti

A) Zanesljiv proces skrbnega pregleda za pridobivanje in izbiro

Vzpostavljen proces, dokumentiran, opis in utemeljitev potrebe po odnosu s tretjo osebo in njegovo naravo.

B) Sklepanje pogodb in odobritev

Sklepanje pogodb in odobritev se izvajata v skladu s politikami in postopki organizacije za obvladovanje tveganj tretjih oseb ter vključujeta sodelovanje med ustreznimi deli organizacije.

C) Pregled in odobritev končnih pogodb

Končne pogodbe ali sporazume pregledajo in odobrijo vsi relevantni deležniki (pravna služba, skladnost, računovodstvo…), podpišejo jih pooblaščene osebe obeh strani in se varno shranijo. Za vsako pogodbo je odgovoren vodja ali skrbnik pogodbe.

D) Seznam vseh razmerij s tretjimi osebami

Vodi se natančen, popoln in trenuten seznam vseh razmerij s tretjimi osebami, na primer v centraliziranem sistemu za vodenje pogodb (Register pogodb v dokumentarnem sistemu, Register izločenih poslov)

KONTROLE TRETJIH OSEB – po pomembnosti

E) Dokumentirani procesi uvajanja

Vzpostavljeni in upoštevani so dokumentirani procesi uvajanja, da se tretjim osebam omogoči izpolnjevanje pogojev pogodbe ali sporazuma.

F) Procesi stalnega spremljanja, KPI

Obstajajo procesi stalnega spremljanja, s katerimi se ovrednoti, ali tretje osebe v celotnem življenjskem ciklu delujejo v skladu s pogoji pogodbe ali sporazuma in ali izpolnjujejo svoje pogodbene obveznosti. Procesi vključujejo preverjanje zanesljivosti zagotovljenih informacij ter obdobno in vsakokratno ponovno vrednotenje uspešnosti, kadar se sporazum spremeni.

G) Pravila postopanja za sprožitev korektivnih ukrepov

Tretja oseba ne izpolni pričakovanj ali predstavlja povečano ali nepričakovano tveganje. Pravila postopanja vključujejo stopnjevanje incidentov glede na resnost, izvajanje pregledov po incidentu in analiziranje temeljnega vzroka incidentov.

H) Spremljajo se datumi

Spremljajo se datumi izteka in podaljšanja pogodb, po potrebi pa se sprejmejo ukrepi za podaljšanje. Pregled delovanja tretje osebe, tveganja, pogodbena določila.

KONTROLE TRETJIH OSEB – po pomembnosti

I) Formaliziran načrt prekinitve pogodbe – izhodna strategija

Izvede se formaliziran načrt prekinitve pogodbe, ki upošteva, da se zagotovi ustrezna obravnava pogodbenih zahtev, ki vključujejo časovni okvir in pričakovanja. Procesi vključujejo, kako:

- Prekinite pogodbo s tretjo osebo.
- Po potrebi zamenjajte tretjo osebo.
- Ponovno dodelite skrbništvo in vrnite ali uničite občutljive podatke organizacije, shranjene pri tretji osebi.
- Tretji osebi odvzamete dostop do sistemov, orodij in prostorov.

KONTROLE TRETJIH OSEB – delovni program, priloga B

https://www.theiia.org/globalassets/site/standards/topical-requirements/third-party/third_party_tr_user_guide_english.pdf

Appendix B. Optional Documentation Tool

Internal auditors are expected to exercise professional judgment in determining the applicability of the requirements based on the risk assessment and appropriately document the exclusions of certain requirements. The Topical Requirement can be documented in the internal audit plan or in the engagement workpapers based on the auditor's professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. The printable form below provides one option for documenting conformance with the Third-Party Topical Requirement, but its use is not mandatory.

Third-Party Governance

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
A. A formal approach is established, implemented, and periodically reviewed to determine whether to contract with a third party. The approach includes appropriate criteria for defining and assessing the resources necessary and available to meet objectives by providing a product or service.		
B. Policies and procedures are established to define, assess, and manage relationships and risks with third parties throughout the third-party life cycle. The policies and procedures are aligned with applicable regulatory requirements and are periodically reviewed and updated to strengthen the control environment.		
C. The organization's third-party management roles and		

Vloga notranje revizije in prehod na IT del

Kaj preverja notranja revizija?

- Skladnost s politiko izločenih poslov/pravilnikom
- Popolnost in ažurnost registra izločenih poslov
- Ustreznost pogodbenih klavzul (SII čl. 49, Zzavar-1, DORA)
- Postopki due diligence in odobritve
- Spremljanje izvajalca: KPI, SLA, incidenti
- Izhodna strategija in testi nadomestnih scenarijev

Prehod: IT zunanje izvajanje

Splošna pravila veljajo tudi za ICT, vendar DORA prinaša dodatne, strožje zahteve.

- Cloud, SaaS, ICT podpora
- Kibernetska tveganja in incidenti
- Operativna odpornost in TLPT testi
- Praktični primeri iz prakse

Zakaj IT zahteva poseben pristop?

DORA, cloud, kibernetska varnost, ICT incidenti, sub-outsourcing in koncentracijsko tveganje — vse to nadgrajuje splošna pravila zunanjega izvajanja.

DORA: pet stebrov operativne odpornosti

I

Upravljanje ICT tveganj

Politika, ogrodje, vloge in odgovornosti

II

Poročanje incidentov

Klasifikacija, roki, vsebina poročil ESA

III

Testiranje odpornosti

Letna testiranja, TLPT za pomembne subjekte

IV

ICT tretje osebe

Register, due diligence, izhodne strategije

V

Izmenjava informacij

Prostovoljna izmenjava o kibernetskih grožnjah

Veljavnost od 17. januarja 2025 — neposredno uporabna v vseh državah članicah EU

Cloud v zavarovalništvu: IaaS, PaaS, SaaS

IaaS

Infrastruktura kot storitev — najem strežnikov, mreže, storage.

Primer:

AWS EC2, Azure VM za testno okolje.

Nadzor zavarovalnice:

Velik (mi upravljamo OS in aplikacije).

PaaS

Platforma za razvoj in tek aplikacij — DB, runtime, integracije.

Primer:

Azure SQL DB za podatkovno skladišče.

Nadzor zavarovalnice:

Srednji (mi le aplikacije in podatki).

SaaS

Programska oprema kot storitev — končna aplikacija prek brskalnika.

Primer:

Microsoft 365, HRM portal, CRM v cloudu.

Nadzor zavarovalnice:

Omejen (le konfiguracija in uporabniki).

Varnostna tveganja IT outsourcinga

Vdori in zlonamerna koda

- Phishing prek izvajalca
- Ransomware napadi
- Zlonamerni notranji akter

Izguba zaupnosti podatkov

- Nepooblaščen dostop
- Razkritje tretjim
- Neustrezno šifriranje

Razpoložljivost

- Izpadi pri izvajalcu
- DDoS napadi
- Pomanjkljiv disaster recovery

Skladnost in suverenost

- GDPR pri prenosu izven EU
- Lokalna zakonodaja
- Pomanjkljiva forenzika

Ključni obrambni ukrepi

Tehnični

- MFA in zero-trust
- Šifriranje at rest in in transit
- Sistematični patch management

Organizacijski

- Segregation of duties
- Politike dostopov
- Izobraževanje uporabnikov

Pogodbeni

- SLA za odzivni čas na incident
- Pravica do varnostne revizije
- Obveznost prijave incidentov

Nadzorni

- Stalen monitoring (SIEM)
- Penetration testing
- Tabletop vaje skupaj z izvajalcem

Pogodbene zahteve za ICT izvajalce

DORA člen 30: minimalni pogodbeni elementi za ICT storitve

Opis storitev
Jasen opis ICT storitev, lokacij obdelave podatkov

Roki in odpoved
Polni opis pogojev podpisa, podaljšanja in odpovedi

SLA in metrike
Storitvene zaveze, KPI in posledice neizpolnjevanja

Varstvo podatkov
GDPR, dostop, šifriranje, varnostni standardi

Pravice nadzora
Pravica do revizije, dostop nadzornika in regulatorja

Sub-outsourcing
Pogoji za podizvajalce, soglasje, register

Lokacija EU/tretje države
Določba o jurisdikciji in pravu obdelave

Izhodna strategija
Načrt izstopa, prenos podatkov, sodelovanje izvajalca

Operativna odpornost in TLPT testiranje

Operativna odpornost

- Sposobnost ohranjanja kritičnih storitev ob motnjah
- BCP in DRP morata vključevati ICT izvajalce
- Redno testiranje scenarijev ob izpadih
- RTO in RPO definirana pogodbeno
- Soodvisnost: zavarovalnica + izvajalec + sub-izvajalec

TLPT - Threat-Led Penetration Testing

- Obvezno za pomembne finančne entitete (DORA)
- Najmanj enkrat na 3 leta
- Pokriva tudi ključne ICT izvajalce
- Red team simulira realnega napadalca
- Rezultati v poročilu nadzorniku

Incidenti in poročanje ICT

DORA prag poročanja: pomemben ICT incident

KORAK 1

Začetna prijava

Najpozneje v 4 urah

- Identifikacija incidenta
- Klasifikacija po DORA
- Prijava AZN in CSIRT (SI-CERT)

KORAK 2

Vmesno poročilo

Najpozneje v 72 urah

- Obseg in vpliv incidenta
- Vzroki, prizadeti sistemi
- Trenutni status izvajanja ukrepov

KORAK 3

Končno poročilo

Najpozneje v 30 dneh

- Ključni vzroki (RCA)
- Sprejeti ukrepi
- Izkušnje za prihodnost

Vloga zunanjega izvajalca: pogodbeno mora pomagati pri kategorizaciji, dati podatke za poročilo in sodelovati pri forenziki - to mora biti pisno dogovorjeno PRED incidentom.

Sub-outsourcing in tveganje koncentracije

Podizvajanje

- ICT izvajalec uporablja podizvajalce (npr. cloud)
- Zavarovalnica mora vedeti za celotno verigo
- Pisno soglasje pri pomembnih sub-izvajalcih
- DORA: register vključuje vse ravni verige
- Pravica do veta in odpovedi ob spremembi

Tveganje koncentracije

- Isti ponudnik (npr. AWS/Azure) pri veliko entitetah
- Sistemski izpad bi prizadel cel sektor
- EU - DORA označuje "critical TPPs"
- Geografska koncentracija (vsi v isti regiji)
- ‚Multi-region Cloud' strategija kot odgovor

PRIMER IZ PRAKSE

Cloud ponudnik X je imel izpad regije 12 ur - 3 evropske zavarovalnice istočasno brez polic v sistemu. Le ‚Multi-Region Cloud' je nekatere zaščitil. Sektorska koncentracija je realno tveganje, ne hipotetično.

Primer iz prakse: SaaS CRM

SCENARIJ

SaaS CRM za prodajno mrežo

- Globalni SaaS ponudnik (ZDA-based)
- Podatki o strankah, pogodbah, ponudbah
- Integracija z core polic.sistemom
- Mobilna aplikacija za zastopnike
- Cena: licenčni model na uporabnika

Pomembne klavzule v pogodbi

- Lokacija obdelave: EU regija (Frankfurt) - ne ZDA
- GDPR Standard Contractual Clauses (SCC)
- Pravica do varnostne revizije ali SOC 2 Type II poročilo

Kontrolni mehanizmi

- Mesečno spremljanje SLA (uptime ≥ 99,9 %)
- Letni penetracijski test, dostop do izvodov
- Stalen monitoring uporabe (privilegirani dostopi)

Izhodna strategija

- Izvoz vseh podatkov v standardnem formatu (CSV, JSON)
- Paralelno delovanje pri menjavi ponudnika
- Dokumentirana migracija na alternativni CRM

Primer iz prakse: migracija v cloud IaaS

SCENARIJ: Migracija sekundarnih sistemov (DWH, analitika) v cloud IaaS - 12-mesečni projekt

Faza 1: Priprava	Faza 2: Pilot	Faza 3: Migracija	Faza 4: Stabilizacija
MESECI 1-3	MESECI 4-6	MESECI 7-10	MESECI 11-12
Analiza in priprava	**Pilot na ne-kritičnem sistemu**	**Postopna migracija**	**Stabilizacija in nadzor**
• Klasifikacija podatkov • DPIA in tveganja • Izbira cloud regije EU • Pogodba in SCC	• Test funkcionalnosti • Test varnosti (pentest) • Test SLA in performans • Vključitev NR	• Migracija po podsistemih • Vzporedno delovanje • Spremljanje incidentov • Posodobitev BCP	• Optimizacija stroškov • Letni audit • Posodobitev registra • Poročilo upravi in AZN

Izkušnje iz prakse: IT outsourcing

01

Pogodba je prvi nadzor

Vse, kar ni v pogodbi, kasneje skoraj nemogoče izterjati - investirajte v pravni pregled pred podpisom.

02

Izhodni načrt ni vedno opcija

Pripravite ga PRED migracijo, ne ob izpadu. Realističen test izhoda vsaj enkrat letno.

03

Spremljajte podizvajalce

Pogodbeno zahtevajte register podizvajalcev in obvestilo ob menjavi - tudi cloud ponudniki imajo podizvajalec.

04

Koncentracija je tveganje

Multi-cloud ali multi-region ni samo IT odločitev - je strateška odpornostna izbira.

05

Testirajte odpornost

Tabletop vaje skupaj z izvajalci, ne samo interno. Realni TLPT testi razkrijejo, kar dokumenti zamolčijo.

06

Vključite NR že na začetku

Notranja revizija mora sodelovati pri due diligence in pri pripravi pogodbe, ne le ob letnem pregledu.

Zaključek: 5 ključnih sporočil

1

Odgovornost ostane na vas

Tudi po oddaji storitve uprava in vodstvo ohranjata polno odgovornost.

2

Regulativa je jasna in stroga

Solvency II, ZZavar-1, AZN smernice in DORA postavljajo trden okvir.

3

Pomembne funkcije zahtevajo več

Strožja due diligence, predhodno obvestilo AZN, izstopna strategija.

4

Nadzor ni enkraten — je stalen

KPI, SLA, periodična poročila in revizijska pravica niso opcija.

5

DORA dvigne letvico za ICT

Register, testiranje odpornosti, poročanje incidentov — že velja.

Hvala.

Za dodatne informacije:

polonca.jugmauko@sava-re.si, miha.ozimek@sava-re.si

SAVA INSURANCE GROUP

V družbi dobrih ljudi

www.sava-re.si