Upravljani zahtevki po storitvah in incidentih v podjetju Telekom Slovenije

COBIT DSS02

Poslovni kontekst

Trenutna situacija v Telekom Sloveniji

Kje v podjetju danes nastajajo težave?

V Telekom Sloveniji se incidenti in zahtevki po IT storitvah obravnavajo preko **nepovezanih komunikacijskih kanalov**:

- Telefonski klici na različne številke IT oddelka
- E-poštna sporočila na osebne naslove IT strokovnjakov
- Sporočila preko Microsoft Teams (v zasebnih pogovorih)
- Neformalne zahteve "na hodniku" ali v pisarni
- Včasih celo SMS ali WhatsApp sporočila poznanim IT sodelavcem

Kaj zaposleni počnejo ročno, neurejeno ali ad hoc?

IT tehniki:

- Ročno beležijo incidente v Excel tabele ali osebne beležke
- Vsak tehnik ima svoj sistem prioritizacije
- Informacije o aktivnih incidentih so raztresene po e-poštnih predalih
- Ni centralnega pregleda odprtih zahtevkov
- Predaja informacij med izmenami poteka ustno ali preko Teams sporočil
- Pri kompleksnejših incidentih ni jasne dokumentacije korakov reševanja

Poslovni uporabniki:

- Ne vedo, kam pravilno nasloviti problem
- Iščejo "bližnjice" preko osebnih kontaktov
- Pošiljajo enake zahtevke večkrat preko različnih kanalov
- Nimajo vpogleda v status svojega zahtevka
- Ne poznajo realnih rokov reševanja

Kje prihaja do napak, zamud, nesporazumov?

1. **Izgubljeni zahtevki**: E-pošta se izgubi v mapi, Teams sporočilo ostane neprebrano, telefonski klic ni dokumentiran
2. **Podvojeno delo**: Več tehnikov hkrati dela na istem problemu, ker ni centralne evidence
3. **Kritični incidenti zamujajo**: Brez prioritizacije se zgodi, da se tehniku najprej javi s težavo manj kritičen uporabnik
4. **Eskalacije ne delujejo**: Ko tehnik ne zmore rešiti problema, ni jasno, komu ga posredovati
5. **Ni učenja iz preteklosti**: Ista težava se reši večkrat znova, ker ni baze znanja
6. **Konflikti z uporabniki**: "Jaz sem vam pa že včeraj poslal..." – ni dokazov o prejemu
7. **Nemogoče poročanje**: Vodstvo ne ve, koliko incidentov je bilo, kakšni so trendi, kje so ozka grla

Konkretni primeri iz Telekom Slovenije:

- **Primer 1 – Mrežni izpad**: Uporabnik iz prodajnega centra v Mariboru javi izpad omrežne povezave. Klic pride na centralo, operater ga preusmeri na IT. IT tehnik obljubi, da bo preveril. Čez 2 uri uporabnik ponovno kliče – nihče ni prišel. Izkaže se, da je bil tehnik na terenu in informacija ni bila posredovana kolegom. Prodajni center je bil 4 ure brez sistema.
- **Primer 2 – Zaprosilo za dostop**: Nova zaposlena v kadrovskem oddelku potrebuje dostop do HR sistema. Pošlje e-pošto IT managerju, ta posreduje tehniku, tehnik čaka na potrditev kadrovske, kadrovski direktor je na dopustu. Po 2 tednih je zaposlena še vedno brez dostopa.
- **Primer 3 – Problem z VPN**: 15 uporabnikov iz terena poroča o težavah z VPN povezavo. Vsak kliče posebej, vsak dobi drugačen nasvet, nihče ne vidi, da gre za sistemski problem na strežniku.

Kaj se zgodi, če odgovornosti niso jasne?

- **"To ni moja naloga" sindrom**: Tehniki se izogibajo prevzemu težavnih zahtevkov
- **Zaposleni ne vedo, koga poklicati**: Klici krožijo po organizaciji
- **Vodja IT ne more oceniti obremenitve**: Ne more utemeljiti potrebe po dodatnih virih
- **Ni odgovornosti za rezultat**: Če gre kaj narobe, ni jasno, kdo je odgovoren
- **Slabo zadovoljstvo uporabnikov**: Percepcija, da "IT nikoli ne dela, kar bi moral"
- **Regulatorna tveganja**: Pri izpadih telekomunikacijskih storitev AKOS zahteva dokumentacijo odzivnih časov – ta ne obstaja

1.2 Namen in cilji procesa DSS02

Kaj proces omogoča

Strukturirano sprejemanje in obravnavanje zahtevkov

- Enoten vstopni kanal (Service Desk) za vse IT zahtevke
- Avtomatična kategorizacija in usmerjanje zahtevkov
- Centralizirana evidenca vseh aktivnih in zaključenih zahtevkov
- Sledljivost celotnega življenjskega cikla zahtevka od prijave do zaključka

Prioritizacijo in upravljanje na podlagi posla

- Razlikovanje med incidenti (prekinitve) in zahtevki po storitvah (spremembe, dostopi)
- Prioritizacija glede na vpliv na poslovanje (kritične storitve Telekom Slovenije: billing, CRM, omrežna infrastruktura)
- SLA (Service Level Agreement) za različne kategorije zahtevkov
- Eskalacijski mehanizmi za kritične primere

Koordinacijo reševanja

- Jasna dodelitev zahtevkov ustreznim tehnikom ali skupinam
- Preglednost statusa za vse vpletene
- Učinkovita komunikacija med podpornimi nivoji (L1, L2, L3)
- Možnost sodelovanja več strokovnjakov pri kompleksnih incidentih

Kaj proces izboljša

Odzivnost IT službe

- Skrajšanje časa prvega odziva z **X ur na 15 minut** (za kritične incidente)
- Zmanjšanje časa reševanja standardnih zahtevkov z **Y dni na 2 dni**
- Hitrejša identifikacija sistemskih težav (več incidentov istega tipa)

Preglednost in nadzor

- Real-time dashboard odprtih zahtevkov za IT vodstvo
- Metrike učinkovitosti: število rešenih zahtevkov, povprečni čas reševanja, stopnja reševanja na prvem nivoju
- Identificiranje ponavljajočih se težav, ki kažejo na potrebo po preventivnih ukrepih
- Podatki za utemeljitev kadrovskih in investicijskih odločitev

Komuniciranje z uporabniki

- Avtomatsko potrjevanje prejema zahtevka
- Obveščanje o napredku (status se je spremenil)
- Ocena zadovoljstva po zaključku
- Self-service portal za preverjanje statusa

Znanje in učenje organizacije

- Baza znanja z rešitvami pogostih težav
- Dokumentacija neobičajnih incidentov
- Možnost učenja novih tehnikov iz zgodovine
- Zmanjšanje odvisnosti od posameznikov

Produktivnost

- Zmanjšanje časa, ki ga uporabniki izgubijo zaradi čakanja
- Zmanjšanje časa, ki ga IT tehniki porabijo za administrativne naloge
- Zmanjšanje podvojenega dela
- Večja osredotočenost na pomembne naloge

Kaj proces ščiti

Poslovno kontinuiteto

- Hiter odziv na kritične incidente, ki lahko prekinejo poslovanje (npr. izpad billing sistema)
- Preventiva: zgodnja identifikacija težav, preden prerastejo v krize
- Strukturiran pristop k reševanju, ki zmanjša tveganje eskalacije problema

Kakovost storitev

- Zagotavljanje dogovorjenih ravni storitev (SLA compliance)
- Dosledno obravnavanje vseh uporabnikov (ni favoriziranja)

- Profesionalen pristop, ki krepi zaupanje v IT

Informacijsko varnost

- Sledljivost dostopov in sprememb (audit trail)
- Kontroliran postopek dodeljevanja dostopov preko formalnih zahtevkov
- Dokumentacija varnostnih incidentov za namen forenzične analize

Regulatorne zahteve

- Dokumentacija za potrebe AKOS (regulatorja telekomunikacij)
- Evidenca izpadov kritičnih sistemov
- Dokazila o skladnosti s poslovnimi pravili in standardi

Stroškovna učinkovitost

- Zmanjšanje stroškov zaradi podaljšanih izpadov
- Optimizacija razporeditve IT virov
- Preprečevanje nepotrebnih stroškov zaradi improvizacij in nujnih ukrepov

Ugled podjetja

- Notranje: zadovoljni zaposleni imajo boljše delovne pogoje
- Zunanje: zanesljiva IT podpora omogoča kakovostne storitve za končne stranke Telekom Slovenije
- Profesionalna podoba IT oddelka kot podpore poslovanju, ne ovire

Glavni koraki procesa (15 korakov)

Korak 1: Prijava zahtevka/incidenta

Kdo: Uporabnik (zaposleni v Telekom Sloveniji)
Kaj se zgodi:

- Uporabnik prijavi težavo ali zahtevo preko enega od kanalov:
  - **Self-service portal** (spletna aplikacija)
  - **Telefonski klic** na enotno številko Service Desk (080 1234)
  - **E-pošta** na servicedesk@telekom.si

- **Avtomatsko odkrivanje** (monitoring sistemi)

COBIT Management Practice: DSS02.01 – Definiranje klasifikacije incidentov in zahtevkov po storitvah

V praksi:

- Uporabnik izbere kategorijo iz vnaprej pripravljenega seznama (omrežje, aplikacije, hardware, dostopi, e-pošta)
- Pri telefonskem klicu operater uporabniku pomaga kategorizirati težavo
- Sistem sam ponudi pogosta vprašanja (FAQ) za hitro samopomoč

Dokumenti:

- **Zahtevek/incident ticket** (generiran z unikatno številko, npr. INC-2025-00123)

Korak 2: Začetna validacija in beleženje

Kdo: Service Desk operater (Level 1)
Kaj se zgodi:

- Operater preveri popolnost informacij
- Zabeleži vse ključne podatke:
  - Kontakt uporabnika
  - Lokacija (katera poslovna enota)
  - Opis težave
  - Storitev, ki je prizadeta
  - Čas nastanka težave

COBIT Management Practice: DSS02.02 – Zapisovanje, kategorizacija in prioritizacija zahtevkov in incidentov

V praksi:

- Uporaba strukturiranega obrazca v Service Desk orodju
- Obvezna polja: kontakt, kategorija, opis (min. 20 znakov)
- Če uporabnik kliče po telefonu, operater beleži podatke v realnem času
- Sistem avtomatsko zabeleži čas prijave (timestamp)

Dokumenti:

- **Incident Record** (popoln zapis v ITSM sistemu)
- **Potrditvena e-pošta** uporabniku z številko ticket-a

Korak 3: Kategorizacija in prioritizacija

Kdo: Service Desk operater (Level 1)
Kaj se zgodi:

- **Kategorizacija:** Dodelitev ustrezne kategorije (npr. Omrežje → VPN → Povezava ne dela)
- **Določitev prioritete** na podlagi matrike:

Vpliv	Nujnost	Prioriteta	SLA čas odziva
Kritičen	Visoka	P1 (Kritična)	15 minut
Visok	Visoka	P2 (Visoka)	1 ura
Srednji	Srednja	P3 (Srednja)	4 ure
Nizek	Nizka	P4 (Nizka)	24 ur

COBIT Management Practice: DSS02.02 (nadaljevanje)

V praksi – primeri prioritizacije:

- **P1:** Popoln izpad billing sistema (ne moremo izdajati računov) = KRITIČNO
- **P2:** Izpad VPN za 20 terenskih tehnikov = VISOKO
- **P3:** Težava s tiskalnikov v podružnici Celje = SREDNJE
- **P4:** Zaprosilo za namestitev dodatne programske opreme = NIZKO

Odločitvena točka:

- Ali je incident major (vpliva na >50 uporabnikov ali kritično storitev)?
    - **DA** → Aktivira se Major Incident Process (posebni protokol)
    - **NE** → Proces nadaljuje standardno

Korak 4: Pregled baze znanja

Kdo: Service Desk operater (Level 1)
Kaj se zgodi:

- Operater pregleda bazo znanja (Knowledge Base) za podobne pretekle primere
- Išče Known Errors in standardne rešitve
- Če najde rešitev → poskusi jo aplicirati takoj po telefonu ali poda navodila uporabniku

COBIT Management Practice: DSS02.04 – Preiskovanje, diagnozo in dodelitev incidentov

V praksi:

- Iskanje po ključnih besedah v Knowledge Base
- Primer: "VPN povezava ne dela" → najde članek "Kako resetirati VPN klienta"
- Operater uporabnika vodi skozi korake

Dokumenti:

- **Povezava na KB članek** (zabeleži se v incident record)

Korak 5: Poskus takojšnje rešitve (First Call Resolution)

Kdo: Service Desk operater (Level 1)
Kaj se zgodi:

- Če je rešitev znana in enostavna, operater poskuša rešiti takoj:
  - Reset gesla
  - Restart storitve
  - Preverjanje osnovnih nastavitev
  - Vodenje uporabnika po korakih

COBIT Management Practice: DSS02.05 – Reševanje in okrevanje po incidentih

V praksi – cilj:

- **First Call Resolution (FCR) = 60%** zahtevkov rešenih že na prvem kontaktu
- Tipične rešitve L1: gesla, osnovne napake, nastavitve

Odločitvena točka:

- Ali je incident rešen na Level 1?
  - **DA** → Skok na Korak 13 (Zaprtje)
  - **NE** → Nadaljuje na Korak 6 (Eskalacija)

Korak 6: Eskalacija na Level 2

Kdo: Service Desk operater (Level 1)
Kaj se zgodi:

- Če operater ne more rešiti, incident **eskalira na Level 2** (specializirane skupine):
  - **Omrežna skupina** (network team)
  - **Sistemska skupina** (server & infrastructure)
  - **Aplikacijska skupina** (business applications)
  - **Desktop podpora** (end-user devices)

COBIT Management Practice: DSS02.04 (nadaljevanje) – Dodelitev incidentov

V praksi:

- Operater v ITSM sistemu dodeli incident specifični skupini
- Doda povzetek raziskave ("Preveril sem X, Y, Z – ni pomagalo")
- Sistem avtomatsko obvesti odgovorno skupino (e-pošta + SMS za P1/P2)

Dokumenti:

- **Assignment Record** (zapis dodelitve)
- **Work Notes** (kaj je bilo že narejeno)

Korak 7: Sprejem in pregled s strani Level 2

Kdo: Specialist Level 2 (npr. sistemski administrator)
Kaj se zgodi:

- Specialist prevzame incident iz čakalne vrste svoje skupine
- Pregleda vse zbrane informacije
- Kontaktira uporabnika, če potrebuje dodatne podatke

- Opravi naprednejšo diagnostiko

COBIT Management Practice: DSS02.04 – Preiskovanje in diagnoza

V praksi:

- Specialist uporablja napredna orodja (remote access, log analysis, network monitoring)
- Dostopa do sistema uporabnika (s soglasjem) za diagnostiko
- Preverja logs, metrics, alerts

Korak 8: Identifikacija vzroka

Kdo: Specialist Level 2/3
Kaj se zgodi:

- Specialist identificira **root cause** (osnovni vzrok) težave
- Določi, ali gre za:
    - **Incident** (enkratna motnja) → reši se takoj
    - **Problem** (ponavljajoča se težava) → zabeleži se kot Problem Record za kasnejšo analizo

COBIT Management Practice: Povezava s DSS03 (Problem Management)

V praksi:

- Če specialist ugotovi, da je isti incident že tretjič v tem tednu → ustvari Problem Record
- To omogoči, da se kasneje analizira osnovni vzrok in najde trajna rešitev

Odločitvena točka:

- Ali lahko specialist reši sam?
    - **DA** → Nadaljuje na Korak 9
    - **NE** → Eskalira na Level 3 ali External Vendor

Korak 9: Implementacija rešitve

Kdo: Specialist Level 2/3
Kaj se zgodi:

- Specialist izvede rešitev:
  - Popravek konfiguracije
  - Restart storitve
  - Patch/update
  - Zamenjava hardvera
  - Sprememba nastavitev

COBIT Management Practice: DSS02.05 – Reševanje in okrevanje

V praksi:

- Vse spremembe se beležijo v incident record
- Pri P1/P2 incidentih specialist sproti obvešča uporabnika
- Če je potrebna načrtovana prekinitev (planned downtime), se koordinira z Change Management (DSS04)

Dokumenti:

- **Resolution Notes** (kaj je bilo narejeno)
- **Change Record** (če je bila potrebna sprememba v produkciji)

Korak 10: Verifikacija rešitve

Kdo: Specialist Level 2/3 + Uporabnik
Kaj se zgodi:

- Specialist preveri, da rešitev deluje
- Kontaktira uporabnika za potrditev:
  - "Ali zdaj lahko normalno delate?"
  - "Ali je težava odpravljena?"

COBIT Management Practice: DSS02.05 (nadaljevanje)

V praksi:

- Pri kritičnih incidentih: specialist ostane dosegljiv še naslednjih 30 minut za preverjanje
- Pri zahtevkih za nove storitve: uporabnik mora potrditi, da je prejel, kar je zahteval

Odločitvena točka:

- Ali uporabnik potrjuje, da je težava rešena?
    - **DA** → Nadaljuje na Korak 11
    - **NE** → Nazaj na Korak 8 (dodatna diagnoza)

Korak 11: Kategorizacija rešitve in posodobitev baze znanja

Kdo: Specialist Level 2/3 ali Service Desk operater
Kaj se zgodi:

- Specialist dokumentira rešitev v standardizirani obliki
- Če je rešitev nova ali uporabna za prihodnost → ustvari ali posodobi KB članek
- Označi tip rešitve (workaround, permanent fix, configuration change)

COBIT Management Practice: DSS02.07 – Sledenje statusu in izdelovanje poročil

V praksi:

- Vsak rešen incident doprinese k bazi znanja
- KB članki morajo biti napisani jasno, korak-za-korakom
- To omogoči, da naslednjič isti incident reši že Level 1

Dokumenti:

- **Knowledge Base Article** (nov ali posodobljen)
- **Solution Category** (v incident record)

Korak 12: Posodobitev CMDB (Configuration Management Database)

Kdo: Specialist ali CMDB skrbnik
Kaj se zgodi:

- Če je incident vplival na konfiguracijske elemente (CI), se posodobi CMDB:

- Zamenjava strežnika
- Nov IP naslov
- Posodobljena verzija software
- Spremenjena konfiguracija

COBIT Management Practice: Povezava z DSS01 (Manage Operations) in BAI10 (Manage Configuration)

V praksi:

- CMDB vsebuje evidenco vseh IT sredstev v Telekom Sloveniji
- Ažurnost CMDB je kritična za učinkovito reševanje prihodnjih incidentov
- Primer: Če strežnik TEL-SRV-BILL-01 pade, specialist iz CMDB vidi, katere storitve so odvisne od njega

Korak 13: Zaprtje incidenta

Kdo: Service Desk operater ali Specialist
Kaj se zgodi:

- Incident se formalno **zapre** v ITSM sistemu
- Status: "Resolved" → "Closed"
- Zabeleži se:
  - Čas zaprtja
  - Končna rešitev
  - Porabljen čas (work hours)
  - Root cause (če je poznan)

COBIT Management Practice: DSS02.06 – Zapiranje zahtevkov za storitev in incidentov

V praksi:

- Incident NE SME biti zaprt, dokler uporabnik ne potrdi rešitve
- Avtomatska zaprtja: če uporabnik 3 dni ne odgovori na prošnjo za potrditev, sistem avtomatsko zapre incident (z obvestilom)

Dokumenti:

- **Incident Closure Report** (zapis zaprtja)

Korak 14: Anketa zadovoljstva

Kdo: Sistem (avtomatsko)
Kaj se zgodi:

- Uporabnik prejme kratko anketo zadovoljstva (4 vprašanja):
  - Kako ocenjujete odzivni čas? (1-5)
  - Kako ocenjujete strokovnost? (1-5)
  - Ali je težava trajno rešena? (DA/NE)
  - Komentar (opcijsko)

COBIT Management Practice: DSS02.07 – Sledenje statusu in izdelovanje poročil

V praksi:

- Anketa se pošlje avtomatsko 1 uro po zaprtju incidenta
- Rezultati so vidni IT vodstvu v dashboard-u
- Negativne ocene (≤2) sprožijo avtomatično obvestilo vodji Service Desk

Dokumenti:

- **Customer Satisfaction Score (CSAT)**

Korak 15: Analiza trendov in poročanje

Kdo: Service Desk Manager / IT Manager
Kaj se zgodi:

- **Tedensko:** Pregled KPI-jev (število incidentov, SLA compliance, CSAT)
- **Mesečno:** Analiza trendov (kateri tipi incidentov se ponavljajo)
- **Kvartalno:** Strateško poročilo vodstvu o stanju IT storitev

COBIT Management Practice: DSS02.07 – Sledenje statusu in izdelovanje poročil

V praksi – KPI dashboard vsebuje:

- Število odprtih/zaprtih incidentov (po prioriteti)

- SLA compliance rate (% incidentov rešenih v SLA roku)
- First Call Resolution rate
- Povprečni čas reševanja (MTTR – Mean Time To Resolution)
- Top 10 kategorij incidentov
- CSAT povprečje

Dokumenti:

- **Weekly/Monthly Service Report**
- **Trend Analysis Report**
- **Improvement Recommendations** (za management review)

Odločitvene točke (Decision Points)

Proces ima **5 ključnih odločitvenih točk**:

DP1: Major Incident? (po Koraku 3)

- **Vprašanje:** Ali incident vpliva na >50 uporabnikov ali kritično storitev?
- **DA:** Aktivira se Major Incident Process (posebna eskalacija, krizna skupina, direktna komunikacija z vodstvom)
- **NE:** Standardni proces

DP2: Rešljivo na L1? (po Koraku 5)

- **Vprašanje:** Ali je operater L1 rešil incident?

- **DA:** Skok na zaprtje (Korak 13)
- **NE:** Eskalacija na L2 (Korak 6)

DP3: Potrebna eskalacija na L3/Vendor? (po Koraku 8)

- **Vprašanje:** Ali specialist L2 lahko reši sam?
- **DA:** Implementira rešitev (Korak 9)
- **NE:** Eskalira na L3 ali dobavitelja

DP4: Uporabnik potrjuje rešitev? (po Koraku 10)

- **Vprašanje:** Ali je uporabnik potrdil, da težava ne obstaja več?
- **DA:** Zaprtje (Korak 13)
- **NE:** Vrnitev na diagnostiko (Korak 8)

DP5: Ponavljajoča se težava (Problem)? (po Koraku 8)

- **Vprašanje:** Ali je ta incident del večjega ponavljajočega se problema?
- **DA:** Ustvari Problem Record (povezava z DSS03)
- **NE:** Reši kot enkratni incident

Dokumenti in zapisi

Obvezni dokumenti v procesu:

1. **Incident/Service Request Ticket**
    a. Unikatna ID številka
    b. Kategorija, prioriteta, status
    c. Opis, kontakt, časovnica
    d. Kompletna zgodovina aktivnosti
2. **Work Notes / Activity Log**
    a. Vse akcije, ki so bile izvedene
    b. Čas in izvajalec vsake akcije
    c. Komunikacija z uporabnikom
3. **Knowledge Base Article**
    a. Standardizirane rešitve
    b. Korak-za-korakom navodila

    c. Povezani incidenti
4. **SLA Record**
    a. Target resolution time
    b. Actual resolution time
    c. SLA status (Met / Breached)
5. **Customer Satisfaction Survey**
    a. Ocena uporabnika
    b. Komentarji
6. **Service Reports**
    a. Tedensko/mesečno poročilo
    b. KPI dashboard
    c. Trend analiza

1.4 Vloge in odgovornosti v procesu DSS02

Lastništvo in upravljanje procesa

Process Owner (Lastnik procesa): IT Service Delivery Manager

Ime vloge v Telekom Sloveniji: Vodja IT storitev za uporabnike

Odgovornosti lastnika procesa:

- **Definicija procesa**: Določa, kako proces deluje, kdo je vključen, kakšni so standardi
- **Optimizacija**: Nenehno izboljševanje procesa na podlagi metrik in povratnih informacij
- **SLA Management**: Določa in pregleduje service level agreements
- **Eskalacijski protokoli**: Definira, kdaj in kako se eskalira
- **Poročanje vodstvu**: Mesečna poročila o učinkovitosti procesa IT direktorju
- **Budget za proces**: Odgovoren za stroške delovanja Service Desk
- **Izbor orodij**: Odloča o ITSM platformi in podpornih orodjih
- **Trening in razvoj**: Zagotavlja usposabljanje za Service Desk ekipo

Poročanje: Neposredno IT direktorju

KPI-ji, za katere je odgovoren:

- SLA compliance rate (cilj: >90%)
- Customer satisfaction score (cilj: >4.2/5)
- First Call Resolution rate (cilj: >60%)
- Average resolution time

Process Manager (Upravitelj procesa): Service Desk Manager

Ime vloge v Telekom Sloveniji: Vodja Service Desk

Odgovornosti:

- **Dnevno vodenje**: Operativno vodenje Service Desk ekipe
- **Scheduling**: Razporeditev dežurstev, pokrivanje odsotnosti
- **Monitoring**: Spremljanje odprtih incidentov, identifikacija zamud
- **Coaching**: Mentorstvo Service Desk operaterjev
- **Quality assurance**: Preverjanje kakovosti zaprtih incidentov (random sample 10%)
- **Incident reviews**: Tedenske preglede težjih primerov z ekipo
- **Vendor coordination**: Koordinacija z zunanjimi dobavitelji za eskalacije
- **Urgentne eskalacije**: Prve kontakt za nujne situacije izven delovnega časa

Poročanje: Vodji IT storitev za uporabnike

Izvršilne vloge (Executors)

Level 1 Support

1. Service Desk Operater

Število: 6 oseb (rotacija: 2 osebe na izmeno, pokrivanje 8:00-18:00)

Odgovornosti:

- Sprejem vseh zahtevkov (telefon, portal, e-pošta)
- Registracija in kategorizacija

- Prva linija reševanja (FCR cilj: 60%)
- Eskalacija na L2, če ne more rešiti v 15 minutah
- Komunikacija z uporabniki (status updates)
- Dokumentacija v ITSM sistemu

Profil:

- Izkušnje: 1-3 let v IT podpori
- Certifikat: ITIL Foundation (zaželeno)
- Jeziki: Slovenščina (fluent), Angleščina (basic)

Tipične naloge:

- Reset gesel
- Unlock AD računov
- Osnovne težave z e-pošto
- Printer connectivity
- VPN osnovne težave
- Software instalacije (iz kataloga)

Level 2 Support – Specializirane skupine

2. Sistemski Administrator (Server & Infrastructure)

Število: 8 oseb

Odgovornosti:

- Reševanje težav s strežniki (Windows, Linux)
- Active Directory upravljanje
- Storage in backup težave
- Virtualizacija (VMware)
- Escalation point za L1

Tipične eskalacije:

- Server performance issues
- AD group policy težave

- Backup failures
- Disk space critical alerts

3. Omrežni Inženir (Network Specialist)

Število: 4 osebe

Odgovornosti:

- Omrežne težave (LAN, WAN, VPN)
- Firewall in security
- Connectivity issues
- Network monitoring alerts

Tipične eskalacije:

- Site-to-site VPN down
- Network outages
- Routing issues
- Bandwidth problems

4. Aplikacijski Specialist – Business Applications

Število: 6 oseb (razdeljeni po aplikacijah)

Specializacije:

- **SAP Specialist** (2 osebe): Finance, HR moduli
- **CRM Specialist** (2 osebi): Salesforce
- **Billing Specialist** (2 osebi): Telekomunikacijski billing sistem

Odgovornosti:

- Application-specific težave
- User access management
- Integracije med sistemi
- Application performance

Tipične eskalacije:

- SAP transaction errors
- CRM data sync issues
- Billing calculation problems

5. Desktop Support Specialist

Število: 5 oseb (2 osrednja lokacija Ljubljana, 3 terenske podpore za podružnice)

Odgovornosti:

- PC, laptop hardware težave
- Mobilne naprave (iOS, Android)
- On-site podpora
- Hardware zamenjave
- Software instalacije (kompleksnejše)

Tipične eskalacije:

- Hardware failures
- Complex software conflicts
- On-site visit requirements

Level 3 Support & External

6. Senior Sistemski Arhitekt

Število: 2 osebi

Odgovornosti:

- Kompleksne infrastrukturne težave
- Architecture decisions
- Vendor escalation management
- Root cause analysis (major incidents)

Kdaj se vključi:

- Major incidents (P1)
- Ponavljajoči se problemi brez rešitve
- Architecture change decisions

7. External Vendor Support Coordinator

Ime vloge: Koordinator za zunanje dobavitelje Število: 1 oseba (part-time, običajno del vloge Vodje IT nabave)

Odgovornosti:

- Odpiranje vendor tickets
- Sledenje SLA z vendors
- Koordinacija vendor on-site visits
- Vendor contract management

Vendors, s katerimi koordinira:

- Microsoft (Azure, M365)
- SAP Support
- Cisco TAC
- Dell/HP Hardware Support
- Telco carriers

Podporne vloge

8. Problem Manager

Število: 1 oseba (50% delež časa, kombinacija z drugimi nalogami)

Odgovornosti:

- Analiza ponavljajočih se incidentov
- Root cause analysis
- Problem records management
- Known error database
- Preventivne akcije

Kdaj se vključi:

- Ko se isti incident pojavi >3x v mesecu
- Po major incidentu (post-incident review)
- Mesečni trend review

9. Knowledge Manager

Število: 1 oseba (30% delež časa, kombinacija z Service Desk Operater Senior)

Odgovornosti:

- Vzdrževanje Knowledge Base
- Quality review KB articles
- Trainings za novo gradivo
- KB metrics (usage, effectiveness)

10. CMDB Administrator

Število: 1 oseba (30% delež časa, običajno kombinacija z vlogo Configuration Manager)

Odgovornosti:

- Vzdrževanje Configuration Management Database
- CI (Configuration Item) updates
- CMDB data quality
- Relacije med CI-ji

Odločevalci in odobri telji

11. IT Direktor

Odgovornosti v procesu DSS02:

- **Odobravanje major changes** (če incident zahteva urgentno spremembo na produkciji)

- **Budget decisions** (dodatni viri, orodja)
- **Eskalacije iz business strani** (če uporabnik iz managementa ni zadovoljen)
- **Strategic direction** (kvartalski review procesa)

Kdaj se vključi:

- Major incidents (P1) – obvezno obveščanje
- SLA breaches nad kritičnim pragom
- Eskalacije od business direktorjev
- Budget approvals

12. Business Unit Manager (Vodja poslovne enote)

Primeri: Direktor prodaje, Direktor financ, Direktor marketinga

Odgovornosti:

- **Prioritizacija** business-critical incidentov iz svoje enote
- **Approvals** za zahtevke, ki presegajo standard (npr. special access)
- **Escalation point** če uporabnik ni zadovoljen z reševanjem

Kdaj se vključi:

- Business-critical incident vpliva na njihovo enoto
- Zahtevek zahteva business justification
- User complaints z njihove strani

13. Information Security Officer (ISO)

Odgovornosti v procesu:

- **Approval** za dostope do občutljivih sistemov
- **Incident involvement** pri security-related incidentih
- **Compliance checks** pri nestandardnih zahtevkih

Kdaj se vključi:

- Security incidents (data breach, suspicious activity)

- Privileged access requests
- Compliance-sensitive zahtevki

14. HR Business Partner

Odgovornosti:

- **Approval** za IT dostope novim zaposlenim
- **Revokacija dostopov** ob odhodu zaposlenega
- **Verification** upravičenosti dostopa do HR sistemov

Kdaj se vključi:

- Onboarding/offboarding procesi
- Zamenjava vloge zaposlenega (role change)
- HR system access requests