Oblikovano: Ne Drugače za prvo stran

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

OBVLADOVANJE INCIDENTOV V INFORMACIJSKI TEHNOLOGIJI V FARMACEVTSKI DRUŽBI

Ljubljana, september 2008 **MARKO TUK**

Oblikovano: Ne Drugače za prvo stran

Oblikovano: Tabulatorji: 5,28 cm, Levo

IZJAVA

Študent Marko Tuk izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Tomaža Turka, in da dovoljujem objavo svojega diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne **Podpis: _____**

Kazalo

Uvod 1
1 Zbirka napotkov za upravljanje in uvajanje storitev ITIL 2
1.1 Kratka predstavitev farmacevtskega podjetja 2
1.2 Zbirka napotkov za upravljanje in uvajanje Storitev IT (ITIL) 3
1.3 Podpora storitvam 5
1.4 Upravljanje incidentov (angl. Incident Management) 7
2 Izvedba upravljanja incidentov v sistemu SAP v farmacevtskem podjetju 11
2.1 Potek uvedbe procesa upravljanja z incidenti 11
2.2 Splošna specifikacija upravljanja incidentov v farmacevtskem podjetju 14
2.2.1 Namen 14
2.2.2 Pogoji 14
2.2.3 Procesna tokova 15
2.2.4 Opis procesa 15
2.3 Splošni postopek upravljanja incidentov v sistemu SAP v farmacevtskem podjetju 18
2.3.1 Pristojnosti in odgovornosti v procesu 18
2.3.2 Kratek opis procesa 19
2.3.3 Časovni intervali in nalogi (*angl. ticket*) 20
2.4 Splošni postopek upravljanja tehničnih incidentov v farmacevtskem podjetju 22
2.4.1 Organizacijska struktura centra za podporo uporabnikom (CPU) 22
2.4.2 Opis procesa 23
3 Skladnost upravljanja incidentov s SOX zahtevami 27
3.1 SOX (Sarbanes-Oxley) zakon in razlogi za njegov sprejem 27
3.2 Cilji SOX-a 28
3.3 Vpliv SOX zakona na Slovenijo 29
3.4 Vpliv SOX zakona na informacijsko tehnologijo 30
3.5 Pregled skladnosti upravljanja incidentov z zahtevami SOX zakona v farmacevtskem podjetju 32
3.5.1 Sprotni pregled skladnosti upravljanja incidentov v SAP sistemu s SOX zahtevami 35
3.5.2 Sprotni pregled skladnosti upravljanja tehničnih incidentov s SOX zahtevami. 37
3.6 Ocena vpeljave ter izvajanje procesa upravljanja z incidenti 40
Sklep 42
Literatura in viri 44

Izbrisano: 10
Izbrisano: 10
Izbrisano: 13
Izbrisano: 13
Izbrisano: 13
Izbrisano: 14
Izbrisano: 14
Izbrisano: 16
Izbrisano: 16
Izbrisano: 17
Izbrisano: 18
Izbrisano: 20
Izbrisano: 20
Izbrisano: 21
Izbrisano: 24
Izbrisano: 24
Izbrisano: 25
Izbrisano: 26
Izbrisano: 27
Izbrisano: 29
Izbrisano: 31
Izbrisano: 33
Izbrisano: 36
Izbrisano: 38
Izbrisano: 40

Oblikovano

Kazalo slik

Slika 1: Celovito okolje ogrodja ITIL 4
Slika 2: Rezultati in posredniki 5
Slika 3: Proces podpore storitvam 6
Slika 4: Eskalacija incidenta 9
Slika 5: Proces upravljanja incidentov 9
Slika 6: Potek reševanja incidentov preko ključnega uporabnika 12
Slika 7: Potek reševanja preko storitvenega centra »Help Desk« 13
Slika 8: Veriga računovodskega poročanja 29
Slika 9: Splošni postopek upravljanja z incidenti v sistemu SAP s SOX kontrolnimi točkami 34
Slika 10: Splošni postopek upravljanja s tehničnimi incidenti s SOX kontrolnimi točkami 35
Slika 11: Magic in SOX kontrolne točke 37
Slika 12: Help Desk aplikacija in SOX kontrolne točke 39

Izbrisano: 11
Izbrisano: 12
Izbrisano: 26
Izbrisano: 30
Izbrisano: 31
Izbrisano: 33
Izbrisano: 35

Uvod

V času globalizacije in hitrega razvoja je za podjetje ključnega pomena dobra organiziranost vseh poslovnih procesov, saj le-ta pomeni večjo učinkovitost in prihranek pri stroških. Ker pa so ti procesi večinoma pokriti z informacijsko tehnologijo, je ključnega pomena tudi dobro organiziran informacijski oddelek. To področje najbolje pokriva zbirka napotkov za upravljanje in uvajanje storitev v IT (*angl. Information Technology Infrastructure Library*, v nadaljevanju ITIL), ki jo je razvil angleški vladni organ Central Computer and Telecommunications Agency (v nadaljevanju CCTA), zato večina podjetij po celem svetu stremi k njeni uvedbi.

ITIL daje le okvirne napotke, kako naj podjetje uvede te standarde v organiziranost upravljanje informacijske tehnologije, podjetje samo pa mora natančno definirati delovne postopke, po katerih bo izvajalo to upravljanje. Tu se pojavi problem, kako določiti mejo med hitrostjo in zapletenostjo postopkov, tako da bo zadovoljen uporabnik in da hkrati ne bo ogrožena sledljivost vseh operacij ter varnost informacijskega sistema.

Za zagotavljanje poslovnega uspeha je bistveno nemoteno in brezhibno delovanja poslovnega informacijskega sistema, ki povečini pokriva že večino procesov in funkcij v podjetju, če ne že celotnega poslovanja. Za zagotavljanje tega imamo na razpolago kar nekaj možnosti:

- upravljanje z incidenti,
- upravljanje s problemi,
- upravljanje s spremembami,
- upravljanje izdaj,
- upravljanje konfiguracije.

Vsa ta upravljanja pa sestavljajo podpore storitvam.

Ker farmacevtsko podjetje posluje na trgu ZDA, kjer pa se zahteva, da vsa podjetja, in zaradi narave svojih izdelkov farmacevtska še posebno, izvajajo notranjo kontrolo po Sarbanes-Oxley zakonu (v nadaljevanju SOX), četudi nima sedeža v ZDA.

SOX zakon je dobil ime po njunih sestavljavcih, Paulu S. Sarbanesu in Michaelu G. Oxleyu. ZDA so uvedle SOX zakon zaradi padca Enronove korporacije leta 2001, ki je bila takrat sedma največja korporacija v ZDA, in predstavlja najobsežnejše reforme na področju računovodskih in revizorskih standardov.

Namen diplomske naloge je predstaviti, kako je omenjeno farmacevtsko podjetje uvedlo ITIL standarde na področju upravljanja z incidenti in kako so jih povezali s SOX zakonom. Poleg tega bom ocenil tudi uspešnost procesa uvedbe upravljanja incidentov ter delovanje le-tega v praksi.

Izbrisano: Kazalo slik¶
¶
Slika 1: Celovito okolje ogrodja ITIL . 4¶
Slika 2: Rezultati in posredniki . 5¶
Slika 3: Proces podpore storitvam . 6¶
Slika 4: Eskalacija incidenta . 9¶
Slika 5: Proces upravljanja incidentov . 9¶
Slika 6: Potek reševanja incidentov preko ključnega uporabnika . 11¶
Slika 7: Potek reševanja preko storitvenega centra »Help Desk« . 12¶
Slika 8: Veriga računovodskega poročanja . 26¶
Slika 9: Splošni postopek upravljanja z incidenti v sistemu SAP s SOX kontrolnimi točkami . 30¶
Slika 10: Splošni postopek upravljanja s tehničnimi incidenti s SOX kontrolnimi točkami . 31¶
Slika 11: Magic in SOX kontrolne točke . 33¶
Slika 12: Help Desk aplikacija in SOX kontrolne točke . 35¶
Prelom strani

Oblikovano: Na sredini

Komentar [tt1]: Ali res ocenjuješ in kje? Na koncu uvoda rečeš, da boš opisal, kako se podjetje loteva izvajanja zakona ter izvaja samokontrolo. Ocena ponavadi zajema več kriterijev, ki so lahko različno uteženi, navadno ni le opis stanja.

V prvem delu diplomske naloge se bom osredotočil predvsem na upravljanje z incidenti, vendar bom na kratko razložil tudi vse zgoraj omenjene procese, saj jih zaradi prevelike prepletenosti med njimi ne morem povsem izpustiti. Omenil pa bom tudi, kakšen način upravljanja z incidenti so uvedli v farmacevtskem podjetju.

V drugem delu diplomske naloge se bom osredotočil na pregled – skladnost upravljanja incidentov s SOX-om . V tem delu bom navedel razloge za uvedbo tega zakona in posledice, ki jih je imela sama uvedba na Slovenijo in na informatiko.

V zadnjem delu diplomske naloge bom opisal, na kakšen način se je farmacevtsko podjetje lotilo izvajanja zakona SOX in kako izvaja notranjo samokontrolo, da ostaja v skladu z zahtevami tega zakona.

1 Zbirka napotkov za upravljanje in uvajanje storitev ITIL

1.1 Kratka predstavitev farmacevtskega podjetja

Podjetje se ukvarja s proizvodnjo in prodajo zdravil. Ima štiri proizvodne objekte v Sloveniji ter še dva proizvodna objekta v tujini, in sicer na Poljskem ter v Romuniji. Poleg tega ima več kot 20 predstavništev, razpršenih po celi Evropi, Aziji ter Združenih državah Amerike (v nadaljevanju ZDA). Zaposluje 2.816 delavcev.

Podjetje je leta 2002 uvedlo nov ERP program po imenu SAP, ki mu je omogočil hitrejši razvoj ter hitrejšo rast. Kljub temu uporablja podjetje tudi dodatne programe na posameznih oddelkih, ki so bili razviti znotraj ter izven podjetja, za upravljanje s področji, ki jih SAP ni pokril.

Leta 2002 je podjetje prevzel Novartis, ki je s tem postalo tudi del skupine Sandoz. Tako je vstopilo v kolektiv, ki šteje 23.000 zaposlenih po celem svetu, zato je tudi Sandoz začel projekt SHAPE (**S**andoz **Ha**rmonized **P**rocesses in **E**RP), različico programa SAP, ki bo poenotila ključne procese v vseh podjetjih v skupini Sandoz.

Podjetje je razdeljeno na oddelke in eden izmed njih je tudi oddelek za informatiko, ki ima zaposlenih okoli 50 ljudi in je razdeljen še na pododdelke:

- storitveni center (angl. Help Desk),
- infrastruktura,
- SAP aplikacije,
- ostale poslovne aplikacije,
- ITQM (IT Quality management).

V prihodnosti načrtujejo, da bodo oddelek za informatiko zaupali zunanjim izvajalcem.

1.2 Zbirka napotkov za upravljanje in uvajanje Storitev IT (ITIL)

V tem poglavju bom na kratko predstavil vse procese, ki so zajeti v ITIL standardih ter povezanost med posameznimi procesi. Osredotočil se bom predvsem na predstavitev modula podpore storitvam ter upravljanju z incidenti.

ITIL (*angl. IT infrastructure library*) je okvir najboljše prakse in najpogosteje uporabljen in sprejet pristop k upravljanju storitev IT na svetu (Uvodna predstavitev ITIL, 2006). Metodologijo je sredi 80-ih let prejšnjega stoletja razvil britanski vladni urad OGC (*angl. Office of Government Commerce*). ITIL je sestavljen iz celovite zbirke dokumentov z napotki in opisi za uvajanje in kakovostno upravljanje s storitvami, ki temeljijo na uporabi informacijske tehnologije in izvirajo iz tako imenovanih najboljših praks (*angl. Best Practices*) upravljanja s storitvami IT. Metodologija je rezultat sodelovanja mednarodnih strokovnjakov tako iz javnega kot tudi iz privatnega sektorja v gospodarstvu. Uporabniki ITIL-a so strokovnjaki za informacijsko tehnologijo, ki se ukvarjajo s storitvami IT in potrebujejo podroben vpogled v procese in postopke upravljanja storitev IT zaradi želje po dobrem upravljanju (The Office of Government Commerce, pridobljeno julija 2007).

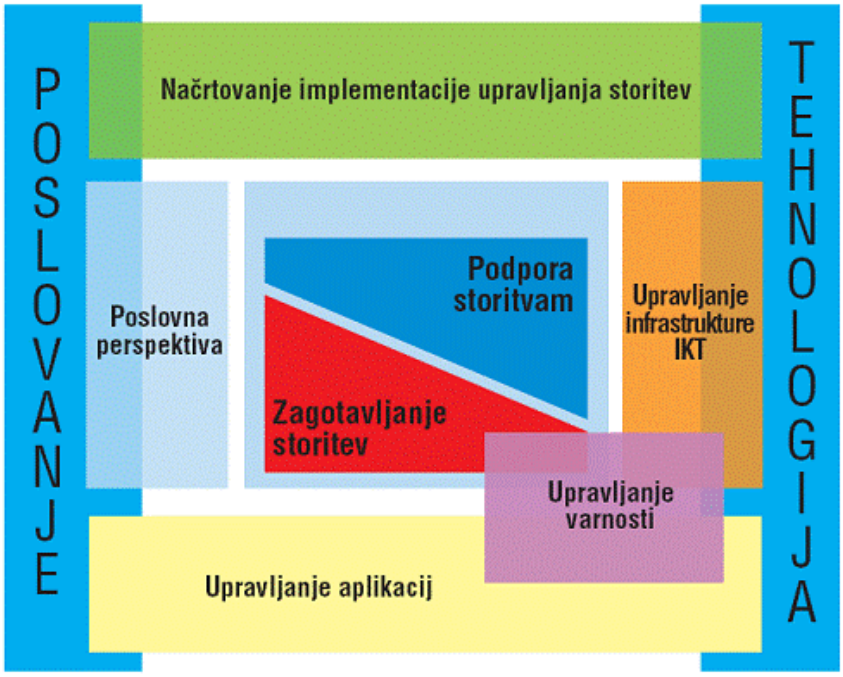
Procesi ITIL pokrivajo področji upravljanja in vzdrževanja storitev IT na strukturiran način, kar omogoča hiter, pregleden in nadzorovan razvoj IT, s tem pa je zagotovljeno ustrezno okolje, ki prinaša stabilnejšo in zmogljivejšo delovanje storitev IT. Na ta način je zagotovljena razpoložljivost IT podpore tudi za ostala ključna funkcijska področja delovanja organizacije. Upravljanje IT tako predstavlja nepogrešljivi del poslovanja organizacije, ki ga je potrebno voditi učinkovito in produktivno ter ga usmerjati v skladu s cilji organizacije (ITIL – The key to Managing IT Services – Best Practices for Service Support, 2003 , ITIL – The key to Managing IT Services – Best Practices for Service Delivery, 2003).

ITIL-ova osrednja modula sta (ITIL – The key to Managing IT Services – Best Practices for Service Delivery, 2003):

- Podpora storitvam (*angl. Service Support*), ki zajema predvsem okvir dnevnega operativnega dela in uporabniško podporo IT storitvam.
- Zagotavljanje storitev (*angl. Service Delivery*), ki pokriva procese, potrebne za načrtovanje in dostavo kakovostnih storitev IT, in je dolgoročno usmerjen v izboljšanje kakovosti IT storitev.

V sliki 1 je prikazana povezava obeh osrednjih modulov v celotno ogrodje ITIL z relacijami med moduli, tehnologijo in poslovnimi subjekti. Iz slike je razvidno, da sta jedro ITIL podpora storitvam in zagotavljanje storitev. Poslovna stran je bolj prilagojena poslovnemu vidiku, upravljanje infrastrukture pa bolj tehnologiji.

Slika 1: Celovito okolje ogrodja ITIL



Vir: Uvodna predstavitev ITIL, 2006.

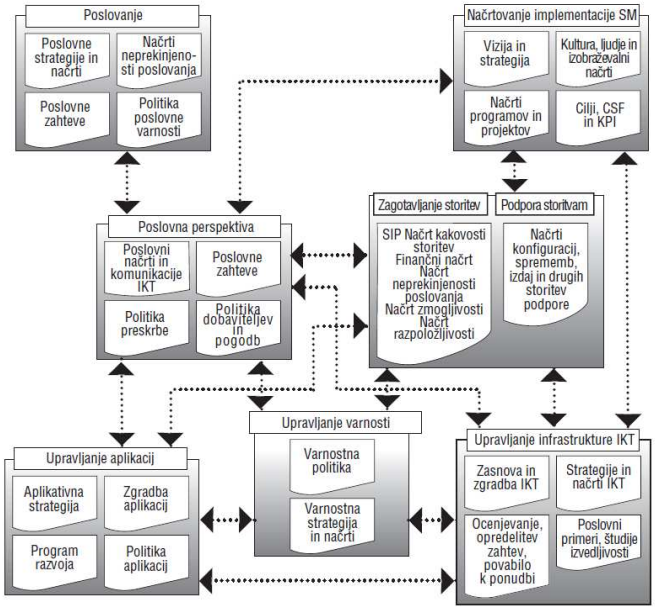
ITIL metodologija pa poleg zgoraj naštetih modulov vključuje še ostale module, ki so potrebni za optimizacijo Storitev IT (Uvodna predstavitev ITIL, 2006):

- Upravljanje z informacijsko-komunikacijsko tehnologijo (*angl. ICT Infrastructure Management*) pokriva vse vidike upravljanja z ICT infrastrukturo, od začetne identifikacije poslovnih potreb preko celotnega procesa izdelave/izbire do testiranja, namestitve, razvoja in vseh ostalih potrebnih operacij, ki vodijo do optimizacije ICT komponent in storitev IT.
- Načrtovanje implementacije upravljanja storitev (*angl. Planning to Implement Service Management*) preiskuje probleme in naloge pri načrtovanju, implementaciji in izboljšanju storitev v organizaciji. Obravnava tudi probleme z organizacijskimi spremembami in spremembami v kulturi organizacije, poleg tega pa še razvoj vizije in strategije po najbolj primerni metodi za posamezen pristop.
- Upravljanje aplikacij (*angl. Application Management*) opisuje, kako ravnati z aplikacijami od začetne poslovne spremembe preko vseh stanj v razvojnem ciklu aplikacije do konca njene življenjske dobe. Osredotoči se na dejstvo, da so IT projekti in IT strategije tesno povezane s tistimi na poslovni strani. Ta pogled omogoča kar najboljši izkoristek naložb v aplikacije.
- Poslovna perspektiva (*angl. The Business Prospective*) svetuje in daje napotke za pomoč IT osebju, da lažje razume, kako lahko bolje uskladi in uporabi storitve in vloge in s tem pripomore, da so poslovni vidiki izpolnjeni v čim večji meri.

- Upravljanje varnosti (*angl. Security Management*) se ukvarja s procesom načrtovanja in upravljanja določene ravni varnosti za informacije in storitev IT, vključno z vsemi vidiki ravnanja ob varnostnih incidentih. Vključuje tudi analizo tveganj, potencialnih nevarnosti in predlogov implementacije ob sprejemljivih stroških.

Slika 2 prikazuje povezanost, obseg in rezultate posameznih modulov zbirke ITIL. Puščice med posameznimi moduli prikazujejo, na katerih področjih izven matičnega procesa posameznega modula se uporabljajo rezultati. Zaradi velike povezanosti sta zagotavljanje storitev in podpora storitvam prikazani kot en sam modul.

Slika 2: Rezultati in posredniki



Vir: itSMF; Uvodna predstavitev ITIL 2006.

1.3 Podpora storitvam

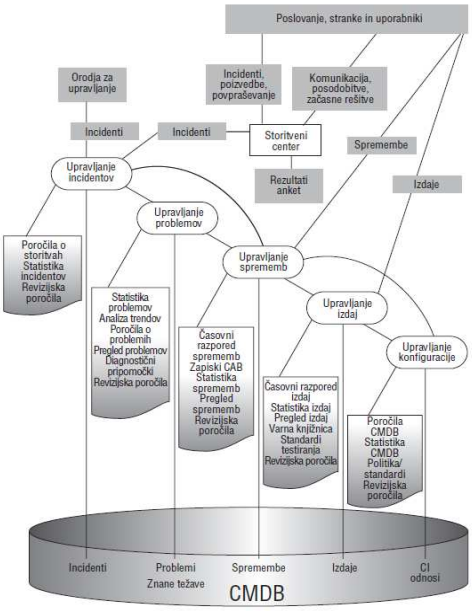
Primarna naloga podpore storitvam je, da zagotavlja, da imajo informatiki dostop do pravih orodij in storitev, ki podpirajo nemoteno delovanje vsem uporabnikom informacijsko-komunikacijske tehnologije. Podporo storitvam sestavlja šest ključnih sklopov, ki tvorijo primerno podporno okolje, na podlagi katerega ima organizacija zagotovljeno nemoteno izvajanje storitev. Ti sklopi so: upravljanje incidentov, upravljanje problemov, upravljanje sprememb, upravljanje konfiguracije in upravljanje izdaj (verzij). Poleg tega definira tudi storitveni center (*angl. Service Desk*), preko katerega se uporabniki vključujejo v proces podpore storitvam, tako da:

- prijavijo napako na sistemu,

- predlagajo spremembo obstoječega sistema,
- zahtevajo nadgradnjo sistema,
- se odločijo za dodatno poizvedbo.

Slika 3 prikazuje celoten proces podpore storitvam in povezave med posameznimi sklopi samega procesa. Prikazan je način vstopanja uporabnikov v proces podpore storitvam preko storitvenega centra.

Slika 3: Proces podpore storitvam



Vir: itSMF; Uvodna predstavitev ITIL 2006.

Storitveni center (*angl. Service Desk*) je sklop podpore storitvam, s katerim se opredeli in zagotovi način komunikacije med uporabniki in IT oddelkom. Pri tem seveda ne smemo pozabiti na razna orodja, s katerimi lahko na hiter in enostaven način upravljamo z informacijami in ukrepi za vzpostavljanje normalnega nivoja storitev. V okviru tega sklopa moramo zagotavljati del določb, ki so opredeljene v dogovorih o nivojih zagotavljanja storitev (*angl. Service Level Agreement,* kratica SLA).

Upravljanje incidentov (*angl. Incident Management*) je proces, s katerim se zagotavlja čim hitrejša odprava prijavljenega incidenta. Na hitrost reševanja incidenta vpliva njegova pomembnost, ki je določena z »vplivom incidenta« na sistem in »nujnostjo odprave« le-tega. Naloga upravljanja incidentov je odkrivanje, beleženje, razvrščanje in primarna podpora pri incidentih.

Upravljanje problemov (*angl. Problem Management*) je proces, ki omogoča odkrivanje vzrokov za incidente, ki so zabeleženi v podatkovni bazi znanja storitvenega centra. Upravljanje problemov tudi dopolnjuje sam proces upravljanja incidentov, saj prevzema v reševanje večje incidente ter beleži vse začasne rešitve in »hitre popravke« kot znane napake. V okviru tega postopka se oblikujejo tudi zahteve za spremembo (*angl. Request for Change*, kratica RFC), ki so namenjene odpravi problemov.

Upravljanje sprememb (*angl. Change Management)* je centraliziran proces, ki zagotavlja standardizacijo postopkov in metod za upravljanje sprememb, s čimer želimo doseči manjši vpliv na poslovanje ter čim manjše pojavljanje incidentov med uvajanjem sprememb. Upravljanje sprememb je nepogrešljiv del podpore storitvam, saj lahko s tem podjetja upravljajo in spremljajo neko spremembo skozi vse življenjske faze – od njenega nastanka in beleženja do filtriranja, vrednotenja, kategorizacije, odobritve, časovnega razporeda uvedbe, izdelave, testiranja, uvedbe, pregleda in zaključka.

Upravljanje izdaj (*angl. Release Management*) je proces, ki skrbi za uvajanje novih izdelkov ali storitev in s tem zagotavlja, da se upoštevajo vsi vidiki (tako tehnični kot ne-tehnični) vpliva na novo vpeljanih verzij. Tako se zagotovi stabilnost in kakovost izdelkov ali storitev. Skrbi tudi za vse pravne in pogodbene obveznosti, povezane s strojno ali programsko opremo, ki se uporablja v organizaciji. Za vsako verzijo se tako vodi Baza veljavne strojne opreme (*angl. Definite Hardware Store*) in Knjižnica veljavne programske opreme (*angl. Definite Software Library*), ki predstavljata ključni zbirki edine veljavne opreme, ki se sme uporabljati v okviru informacijskega sistema.

Upravljanje konfiguracij (*angl. Configuration Management*) je osnova za uspešno upravljanje storitev IT, saj podpira vse druge procese, ker vključuje celotno znanje iz prejšnjih procesov ter jih shranjuje v Podatkovno bazo upravljanja konfiguracij (*angl. Configuration Management DataBase*, kratica CMDB). V to bazo podatkov so vključena tudi druga sredstva v organizaciji, ki so potrebna za uspešno upravljanje storitev, znana tudi kot konfiguracijski elementi (*angl.Configuration Ite,;* kratica CI). CI predstavljajo ključne sestavne dele celotne infrastrukture in zajemajo delovne postaje, strežnike, tiskalnike, omrežne elemente, organizacijske sheme, programsko dokumentacijo, SLA-je in podobno.

1.4 Upravljanje incidentov (angl. Incident Management)

Upravljanje incidentov je del storitev IT (ITSM). Primarni cilj upravljanja incidentov je, da v najkrajšem možnem času vzpostavi normalno delovanje informacijskega sistema in zmanjša vpliv na poslovanje podjetja. Na ta način skrbi, da je informacijski sistem vedno dostopen in da lahko zagotavljamo kakovostne storitve brez večjih prekinitev. 'Normalno delovanje storitev' je definirano v dogovoru o ravni storitev (SLA), ki ga vsako podjetje sklene z notranjim ali zunanjim izvajalcem, ki skrbi za delovanje informacijskega sistema.

Definicija incidenta v ITIL terminologiji:

> » *Vsak dogodek, ki ni del standardnega delovanja storitve in ki utegne povzročiti prekinitev ali zmanjšanje kvalitete neke storitve.* Ustaljen postopek ITIL-a je, *da v najkrajšem možnem času vzpostavi normalno delovanje sistema in minimalizira vpliv na poslovanje podjetja ali uporabnika po ekonomični ceni«*
> (Incident Management, pridobljeno avgusta 2007)

Kritični faktorji uspeha so:

- ohranjati kvaliteto storitev IT,
- ohranjati zadovoljstvo strank,
- reševati incidente v okviru dogovorjenih rokov.

Ključne aktivnosti upravljanja incidentov so:

- odkrivanje in zapisovanje incidentov,
- klasifikacija,
- omogočanje primarne pomoči pri reševanju incidentov,
- določanje prioritete incidentov glede na njihov vpliv in pomembnost,
- raziskovanje in diagnoza incidentov,
- rešitev incidenta in vzpostavitev normalnega delovanja v okviru SLA,
- zaprtje incidenta,
- ohranjanje lastništva, nadzora, sledenja in komunikacije o incidentu,
- seznanjanje vodstva z informacijami o kakovosti upravljanja incidentov in operacijah.

Incidenti so rezultati napak v IT infrastrukturi. Vzroki incidentov so lahko očitni in se jih da rešiti brez nadaljnjih preiskav, popravil, nadomestnih rešitev ali zahteve za spremembo (RFC) za odstranitev napake. Incident vstopa v proces preko storitvenega centra, računalniških operacij, omrežja, itd., kjer ga poskušamo s ključnimi aktivnostmi, naštetimi zgoraj, razrešiti.

Incidenti, ki se jih ne da rešiti v sklopu centra za pomoč uporabnikom, se dodelijo specializirani tehnični podporni skupini. Rešitev ali nadomestna rešitev naj bi bila vzpostavljena v najkrajšem možnem času, in sicer z namenom, da se znova vzpostavi normalno stanje storitve.

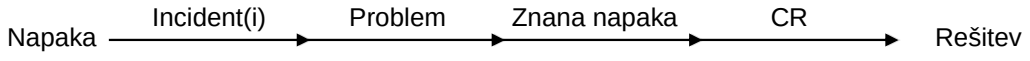
Incidenti, ki so rezultat okvar ali napak v okviru standardne računalniške strojne in programske opreme, so posledica dejanskih ali možnih odklonov od načrtovanega delovanja omenjene opreme. Incidente se ocenjuje glede na vpliv, tako dejanski kot tudi potencialni, ki jih imajo na nudene storitve uporabnikom. Vzrok za incident je lahko očiten in se mu lahko posvetimo brez nadaljnjega poizvedovanja, tako da izvedemo popravilo, začasno rešitev ali pa zahtevo za spremembo, da odstranimo napako. V teh primerih se lahko incidenta (t.j. vpliva

ali možnega vpliva na stranko) lotimo zelo hitro, mogoče tudi brez neposrednega iskanja osnovnega vzroka incidenta (*angl. the underlying cause of the incident*), t.j. problema.

V drugih primerih je problem osnovni vzrok za incident ter kazalec, da gre za neznano napako, ki jo je zato potrebno poiskati.

Rezultat uspešne rešitve problema je identifikacija osnovne napake, ko pa najdemo začasno rešitev in/ali razvijemo zahtevo za spremembo, se problem lahko spremeni v znano napako.

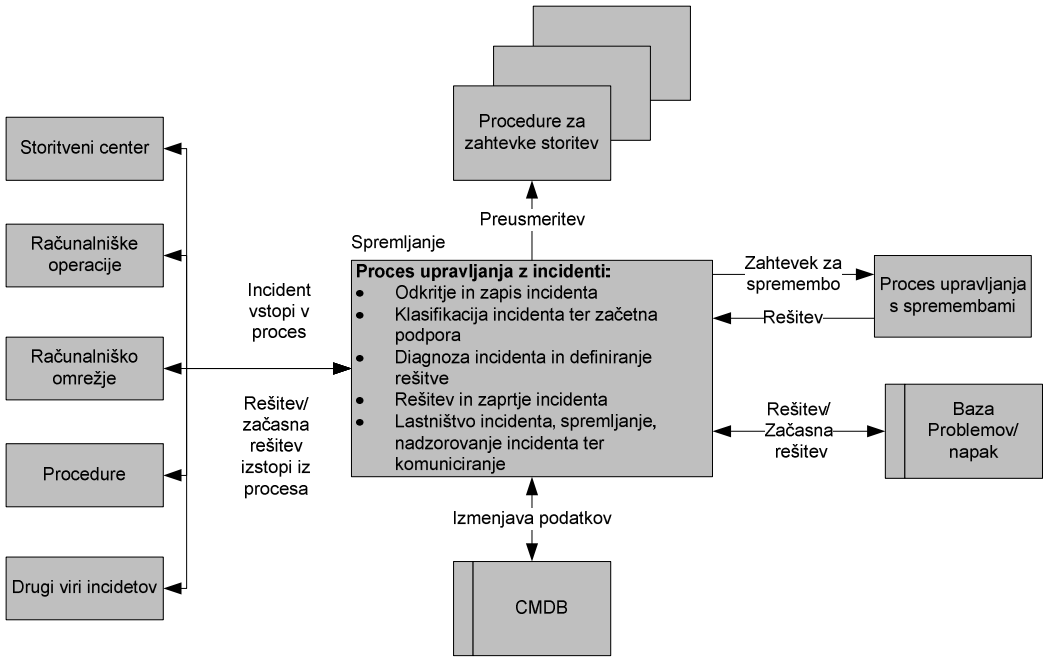
Slika 4: Eskalacija incidenta



Vir: Interna dokumentacija,2006.

Zahteva po dodatni storitvi se ne šteje za incident, ampak predstavlja zahtevo za spremembo.

Slika 5: Proces upravljanja incidentov



Vir: Best Practices for Service Support, 2003

Slika prikazuje delovanje procesa upravljanja incidentov. Prikazuje tudi vse vstopne in izstopne elemente in procese, ki so vključeni v proces upravljanja incidentov. Iz slike je prav tako razvidno, kako je proces upravljanja incidentov tesno povezan s procesom upravljanja

napak ter s procesom upravljanja sprememb, lepo pa je prikazan tudi pretok informacij iz in v CMDB.

2 Izvedba upravljanja incidentov v sistemu SAP v farmacevtskem podjetju

V tem poglavju bom predstavil, kako so v farmacevtskem podjetju uvedli upravljanje z incidenti, navedel, kakšen proces upravljanja z incidenti so izbrali , ter ga opisal. Posebnost tega podjetja je, da so izbrali dva različna procesa za reševanje tehničnih incidentov (reševanje incidentov, povezanih z računalniško opremo (angl. *Hardware*) ter incidentov, povezanih z vsemi programi, razen s SAP-om) ter reševanje incidentov v sistemu SAP.

2.1 Potek uvedbe procesa upravljanja z incidenti

Zaradi vse večjega obsega poslovanja ter počasnosti razreševanja incidentov (uporabniki niso vedeli, na koga naj se obrnejo, da bo rešil njihov incident), so se v farmacevtskem podjetju po dolgem razmisleku odločili, da bodo začeli postopno vpeljevati ITIL standarde, saj so v njih videli najboljšo rešitev, kako izboljšati in pospešiti proces upravljanja z incidenti v njihovem podjetju.

Naprej so uvedli storitveni center (*angl. Help Desk*), nato pa postopoma še proces upravljanja z incidenti v sistemu SAP, tako da imajo sedaj dva ločena procesa. Proces upravljanja z incidenti v sistemu SAP se ukvarja samo z incidenti, ki so nastali v sistemu SAP, medtem ko storitveni center rešuje incidente, povezane s strojno opremo, informacijskim omrežjem in programsko opremo, ki je bila razvita znotraj podjetja.

Same implementacije storitvenega centra so se lotili tako, da so:

- zagotovili tehniko, potrebno za storitveni center (*angl. Help Desk*),
- zgradili lastno bazo podatkov in programsko rešitev storitveni center (*angl. Help Desk*) v okolju Lotus Notes,
- testirali aplikacijo storitveni center (*angl. Help Desk*),
- najeli osebje (agente), ki so ga testirali, ali je dovolj usposobljeno, da lahko pomaga uporabnikom,
- kupili programsko opremo za klicni center (*angl. Call Center*),
- izobrazili agente za delo z aplikacijo storitveni center (*angl. Help Desk*),
- obveščali uporabnike o storitvah storitvenega centra (*angl. Help Desk*),
- izobrazili uporabnike, kako ravnati, ko se pojavi težava v zvezi z delovanjem Storitev IT, oziroma jih naučili, kako ravnati pri odkrivanju incidenta.

Kot sem omenil že zgoraj, so v podjetju leta 2002 uvedli nov ERP sistem, imenovan SAP, zato dotedanji proces upravljanja incidentov (storitveni center) ni več ustrezal novim potrebam in so ga v začetku leta 2007 spremenili. To so izvedli tako, da so vzeli splošni postopek materinskega podjetja ter ga prilagodili svojim potrebam. Odločili so se, da se

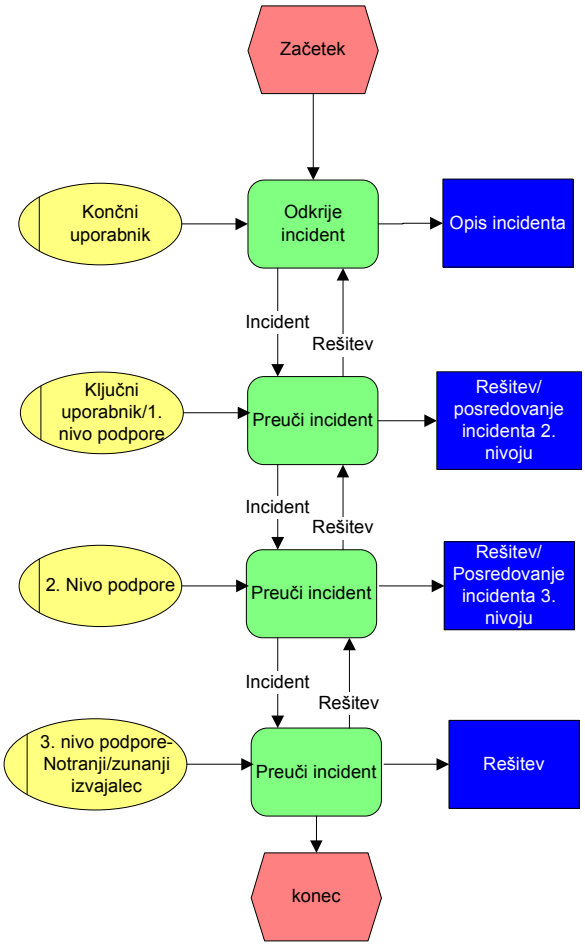
zaradi različne vpletenosti v operacije poslovnih procesov uporabijo dva različna procesna toka, in sicer:

- **procesni tok preko ključnega uporabnika (farmacevtsko podjetje ga uporablja za reševanje SAP incidentov)**. Incident vstopa v proces upravljanja z incidenti samo preko ključnega uporabnika, ki prihaja iz poslovne organizacije podjetja (financ, nabave, prodaje ipd.). Ta najprej preveri, ali gre res za incident ali morda samo za neznanje uporabnika. Če se izkaže, da gre za incident, se incident prijavi storitvenemu centru ali 2. nivoju podpore, kot to prikazuje slika 6.

Slika 6: Potek reševanja incidentov preko ključnega uporabnika

Komentar [e2]: kaj pravzaprav slika prikazuje? Nekega procesnega toka se v resnici ne vidi, le okvirna "zgradba"

Podobno velja za sliko spodaj.

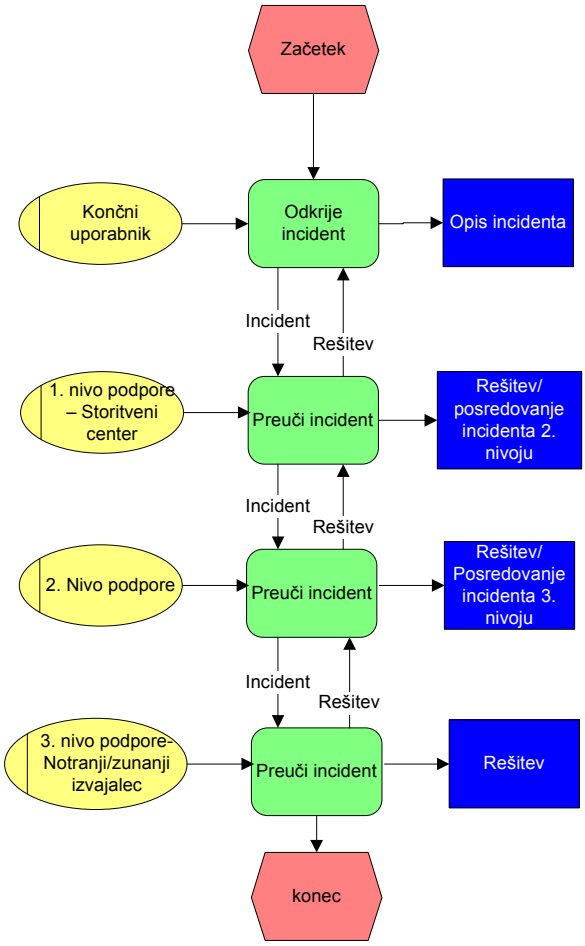


Vir: Interna dokumentacija farmacevtskega podjetja,2006.

- **procesni tok preko storitvenega centra (farmacevtsko podjetje ga uporablja za reševanje vseh tehničnih incidentov in programske opreme, razen SAP-a)**.

Incident vstopa v proces upravljanja z incidenti preko storitvenega centra. Prijavo incidenta lahko prijavi vsak uporabnik preko interneta, elektronske pošte, telefona ipd.

Slika 7: Potek reševanja preko storitvenega centra »Help Desk«



Vir: Interna dokumentacija farmacevtskega podjetja,2006.

Ob tem so se srečali z novim izzivom, in sicer, kako povezati oba procesa. To so rešili tako, da agent, ki ga uporabnik pokliče na storitveni center in ki ugotovi, da je incident, ki mu je bil posredovan, procesno-vsebinska napaka v informacijskem sistemu SAP, incident zapre in pokliče uporabnika ter ga napoti na ključnega uporabnika, ki mu lahko pomaga.

Implementacija obeh procesov je potekala ločeno. Proces storitvenega centra je doživel samo prenovo, medtem ko so morali proces upravljanja incidentov v sistemu SAP povsem na novo vzpostaviti.

Implementacija upravljanja incidentov v sistemu SAP je potekala na naslednji način:

- opredelili so splošni postopek (s pomočjo splošnega postopka materinskega podjetja),
- izbrali so programsko opremo,

- obvestili uporabnike (preko e-pošte, intraneta), da se bo uvedel nov način prijavljanja incidentov,
- izobrazili so informatike in ključne uporabnike o delovanju nove programske opreme in jih seznanili z novim splošnim postopkom,
- izobrazili so uporabnike po novem splošnem postopku.

2.2 Splošna specifikacija upravljanja incidentov v farmacevtskem podjetju

V nadaljevanju bom predstavil splošni postopek za upravljanje z incidenti, ki so ga pripravili v farmacevtskem podjetju in s katerim so določili okvir za reševanje vseh incidentov, tako tehničnih kot tudi programskih. S tem so hoteli določiti nekakšen splošni okvir za izdelavo dejanskega poteka procesa upravljanja z incidenti, katerega vam bom natančneje predstavil v točkah 3.3. ter 3.4.

2.2.1 Namen

Najprej so opredelili, kaj naj bi proces upravljanje z incidenti sploh obsegal in kakšen bi bil njegov namen.
Vse to so opredelili kot proces, v katerem se ukvarjamo z incidenti, ki so:

- napake v delovanju IT sistemov,
- napake v IT sistemu,
- vse ostalo, kar povzroča kakršnokoli odstopanje od normalnega delovanja IT sistema

Z njimi se ukvarjamo na natančno določen način, zato da:

- vzpostavimo normalno delovanje sistema v najkrajšem možnem času,
- zmanjšamo negativne vplive na poslovanje,
- ohranjamo dogovorjeno raven kakovosti in razpoložljivosti storitev.

Poleg tega so v proces upravljanje incidentov vključili tudi reševanje vseh vrst uporabniških vzdrževalnih zahtev (npr. vprašanje v zvezi z funkcionalnostjo IT sistema).

2.2.2 Pogoji

Nadalje so opredelili osnovne pogoje, ki jih mora vsebovati proces upravljanja z incidenti, ti pa so:

- Vsi incidenti morajo biti zapisani in akcije glede njih izvedene. Dokumentacija, ki spremlja incident, mora vsebovati vsaj naslednje podatke:
  - opis incidenta,
  - datum nastanka incidenta,
  - akcije, ki so bile izvedene pri reševanju incidenta,

    - ime osebe, ki je reševala incident,
    - datum rešitve incidenta,
    - referenca na zahtevo za spremembo v primeru, da je za rešitev incidenta potrebna sprememba.
- Incidenti se lahko po potrebi stopnjujejo notranje in/ali zunanje. Pravila stopnjevanja so določena.
- Zahteva za spremembo, ki je bila sprožena zaradi incidenta, sledi postopku upravljanja sprememb.
- Upravljanje incidentov pokriva tudi skrb za varnostne incidente.
- Dnevnik incidentov je potrebno redno pregledovati. S tem zagotovimo identifikacijo incidenta in upravljanje problemov znotraj IT sistema.

2.2.3 Procesna tokova

Opredelili so tudi dva različna procesna tokova za reševanje incidentov v podjetju, ki sem ju omenil že v točki 3.1, in sicer procesni tok preko ključnega uporabnika ter ključni tok preko storitvenega centra.

Procesni tok preko ključnega uporabnika se v farmacevtskem podjetju uporablja izključno za reševanje incidentov, ki so se zgodili v SAP-u. Ta sistem je namreč veliko primernejši za reševanje incidentov informacijskih sistemov, ki so zelo prepleteni s poslovnim sistemom, saj zagotavlja, da se na 2. nivo podpore prijavljajo res le dejanski incidenti, kajti ključni uporabnik pred tem prijavo preveri in ugotovi, ali gre res za incident ali pa zgolj za neznanje uporabnika.

Procesni tok preko storitvenega centra pa se po drugi strani v farmacevtskem podjetju uporablja predvsem za reševanje tehničnih incidentov, kajti le s tem sistemom lahko omogočimo vsakemu uporabniku hitro in kvalitetno rešitev, saj mu incidenta ni potrebno najprej prijavljati ključnemu uporabniku.

2.2.4 Opis procesa

Procesni tok za upravljanje incidentov in uporabniško podporo mora vsebovati naslednje procesne korake:

- registracija zahteve
- rešitev zahteve (samo za »service desk« podporni model)
- dodelitev zahteve
- 2. nivo podpore za rešitev zahteve
- 3. nivo podpore za rešitev zahteve
- pregled dnevnika incidentov

Registracija zahteve

Incident je registriran z dokumentiranjem opisa napake, odpovedi, odstopa ali zahteve za podporo uporabniku in datumom, kdaj se je incident zgodil oziroma smo ga opazili. Z registracijo se naredi tudi vpis v dnevnik incidentov.

Rešitev zahteve

Ta procesni korak pride v poštev samo takrat, ko uporabimo procesni tok preko storitvenega centra. 1. nivo podpore poizkuša incident rešiti, in če je to mogoče izvesti v določenem časovnem okviru, rešitev dokumentira v dnevnik incidentov (opis, datum in ime agenta 1. nivoja, ki je reševal incident), informira uporabnika o rešitvi in incident zapre. Če pa 1. .nivo podpore incidenta ne more rešiti, ga posreduje 2. nivoju podpore. To se naredi v procesnem koraku 'dodelitev zahtev'.

Dodelitev zahteve

Po registraciji ali v primeru, da 1. nivo podpore ni sposoben rešiti incidenta, ga prevzame odgovorni agent 2. nivoja. Dodelitev zahteve se vpiše v dnevnik incidentov.

2. nivo podpore za rešitev zahteve

V tem koraku agent ali skupina 2. nivoja podpore poskuša rešiti prevzeti incident. Če ga uspešno reši, se rešitev zapiše v dnevnik incidentov, 2. nivo podpore obvesti uporabnika o rešitvi in incident se zapre. V primeru, da rešitev incidenta potrebuje spremembo na IT sistemu, se mora narediti zahteva za spremembo in rešitev sledi procesu upravljanja sprememb. Številka zahteve za spremembo mora biti zavedena v dnevnik incidentov.

Če 2. nivo podpore ugotovi, da dodelitev zahteve ni bila pravilno izvedena ali da ni bila potrebna, to zavede v dnevnik incidentov in jo vrne nazaj na 1. nivo.

V primeru, da 2. nivo podpore ugotovi, da ne bo mogel rešiti incidenta v določenem časovnem okviru, ga dodeli 3. nivoju podpore. Ali je 3. nivo podpore notranji ali zunanji ponudnik storitev, je odvisno od procesa upravljanja incidentov, kar je definirano v dogovoru o ravni storitev (SLA-ju).

3. nivo podpore za rešitev zahteve

V primeru, da je 3. nivo podpore zunanji ponudnik storitev, 2. nivo podpore v dnevnik incidentov zavede, kako je 3. nivo podpore rešil incident, obvesti uporabnika in zapre incident.

V primeru, da je 3. nivo podpore notranji ponudnik rešitev, sam zavede rešitev, datum in ime agenta 3. nivoja podpore v dnevnik incidentov, obvesti uporabnika in zapre incident. Če rešitev incidenta potrebuje spremembo na IT sistemu, se mora pripraviti zahteva za spremembo in rešitev sledi procesu upravljanja sprememb. Številka zahteve za spremembo mora biti zavedena v dnevnik incidentov.

Pregled dnevnika incidentov

Dnevnik incidentov se mora periodično pregledovati (vsaj enkrat na leto; doba je določena za vsak IT sistem posebej), da se odkrijejo morebitni ponavljajoči se incidenti ali uporabniške zahteve (problemi). Rezultati pregleda so definirani postopki reševanja problemov, ki se jih nato tudi izvede.

2.3 Splošni postopek upravljanja incidentov v sistemu SAP v farmacevtskem podjetju

V tem poglavju bom natančneje predstavil, kako so v farmacevtskem podjetju zasnovali splošni postopek reševanja incidentov preko procesnega toka in preko ključnega uporabnika.

Pri reševanju si v farmacevtskem podjetju pomagajo s programom Magic, ki ga je razvilo podjetje IBM. Ta program je narejen za upravljanje z incidenti po ITIL standardih. Natančneje ga bom opisal v točki 4.5.3.2., kjer sem dodal tudi kopijo zaslona (Print Screen) tega programa.

2.3.1 Pristojnosti in odgovornosti v procesu

Na začetku je bilo potrebno opredeliti vse nastopajoče subjekte v tem procesu in jim določiti naloge, ki jih morajo izvesti v primeru odkritja in reševanja incidenta. V procesu so opredelili tri subjekte:

- **Končni uporabnik** je odgovoren, da v primeru nepravilnosti oziroma težav pri izvajanju poslovnega procesa v SAP-u o tem obvesti ključnega uporabnika**.**

- **Ključni uporabnik** (superuser – 1. nivo pomoči) je odgovoren za izvajanje procesa, podprtega z informacijskim sistemom SAP v okviru oddelka in med oddelki, ter odpravo procesnih oziroma vsebinskih napak. V primeru identifikacije incidenta v sistemu SAP je odgovoren za pravilen vnos prijave incidenta v program Magic, ki ga uporabljajo za prijavo, reševanje ter sledenje incidentom, ter tudi za natančen opis letega. V primeru visoke prioritete (1. in 2. stopnje) predhodno telefonsko obvesti ERP kompetenčni center in evidentira komunikacijo. Sodeluje pri odpravi incidenta

- **ERP CC EE kompetenčni center** (lastnik incidenta – 2. nivo pomoči) je odgovoren, da napako na osnovi prijave v program Magic odpravi v sodelovanju s ključnimi uporabniki in ustrezno ažurira informacije o incidentu (opis aktivnosti, zaključek incidenta).

2.3.2 Kratek opis procesa

Prijava incidenta

Ko končni uporabnik odkrije incident, ga najprej prijavi ključnemu uporabniku, ki ga poskuša sam odpraviti, in če najde rešitev, o tem obvesti končnega uporabnika. Če pa ga ključni uporabnik ne more rešiti, zbere vse potrebne informacije o incidentu ter ga posreduje na 2. nivo podpore (kompetenčnemu centru), tako da ga zavede v programsko opremo Magic. Ta preveri pri ključnemu uporabniku, ali je bil isti incident že prijavljen, in se nato odloči, ali bo odprl nov incident ali pa ga povezal z že obstoječim.

Klasifikacija incidenta

Oseba SAP EE kompetenčnega centra mora najprej na hitro oceniti incident ter ga, če je le mogoče, rešiti preko telefona, če ga ne more rešiti, pa po potrebi zbere dodatne informacije o incidentu. Nato oseba SAP EE kompetenčnega centra skupaj s ključnim uporabnikom določi stopnjo nujnosti ter okvirni datum za rešitev incidenta ter vnese vse ključne podatke o incidentu v nalog (angl. ticket). Oseba SAP EE kompetenčnega centra nato identificira določeno skupino (prodaja, finance, nabava...) na 2. nivoju podpore, ji nalog dodeli v lastništvo ter ga shrani. S tem ko shranijo nalog , ta preide v status »OPEN« in teči prične reakcijski čas. Nalog je tudi avtomatično posredovan skupini ter ključnemu uporabniku.

V primeru, da gre za incident 1. ali 2. stopnje urgentnosti, mora ključni uporabnik o tem obvestiti določeno skupino preko telefona, da tako zagotovi kratek reakcijski čas.

Član določene skupine sam sebi dodeli nalog , kar ga postavi za lastnika naloga. S tem dejanjem preide nalog v stanje »WIP« (Work In Progress). Hkrati se ključnemu uporabniku pošlje avtomatsko elektronsko pošto o spremembi stanja. Lastnik naloga lahko dodeli nalog drugim članom skupine, vendar še vedno ostane lastnik tega naloga.

Definiranje rešitve incidenta

Trenutni pooblaščenec naloga naredi diagnozo incidenta ter definira rešitev za osnovni problem incidenta. V primeru, da sam incidenta ne more rešiti, ga lahko posreduje drugemu članu skupine znotraj podjetja v 2. ali 3. nivoju podpore ali pa ga posreduje primernemu zunanjemu izvajalcu.

Rešitev in zaprtje incidenta

V primeru, da pooblaščenec reši incident, ga ta zavede v program Magic ter obvesti ključnega uporabnika. Ključni uporabnik nato skupaj s končnim uporabnikom izvede testiranje rešitve incidenta in če sta zadovoljna z rešitvijo, to javita pooblaščencu naloga in incident se lahko zapre.

Prehod iz incidenta v spremembo

Če je potrebna zahteva za spremembo, je potrebno začeti s postopkom upravljanja sprememb, kot je to določeno v internem dokumentu »Splošni postopek o upravljanju sprememb«. Pooblaščenec naloga v nalog vpiše številko zahteve za spremembo in v nalogu nastavi stanje ZAPRTO (*angl. CLOSED*).

Natančnejši opis postopka reševanja incidentov si lahko ogledate v prilogi 1., medtem ko si lahko v prilogi 2 ogledate ERP diagram procesa upravljanja z incidenti v sistemu SAP v farmacevtskem podjetju

2.3.3 Časovni intervali in nalogi (*angl. ticket*)

Kot smo videli pri opisu postopka za reševanje incidentov, merimo za vsak incident naslednja dva časovna intervala:

- **Reakcijski čas**. To je čas, ki začne teči po zapisu naloga, zaključi pa se, ko agent SAP EE kompetenčnega centra določi sebe za lastnika naloga in s tem prevzame lastništvo nad incidentom.

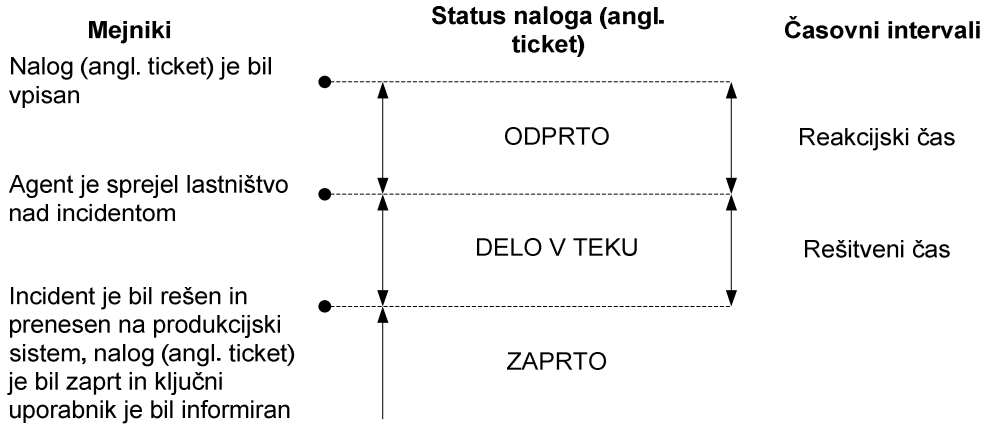
- **Rešitveni čas.** To je čas, ki se začne, ko se zaključi reakcijski čas, zaključi pa se, ko se rešitev incidenta prinese na produkcijski sistem, ko je ključni uporabnik o tem obveščen in se spremeni status naloga v stanje ZAPRTO (*angl. CLOSED*).

Statusi

Nalogi gredo skozi naslednje statuse:

Status naloga	Opis
ODPRTO (OPEN)	Dodeljen je, ko je nalog zapisan.
DELO V TEKU (WIP)	(Work in Progres) Dodeljen je, ko nekdo prevzame lastništvo nad incidentom.
V ČAKANJU (ON HOLD)	Dodeljen je le v izjemnih primerih, kot so: • rešitev incidenta je blokirana za dlje časa, ker uporabniki niso posredovali vseh informacij ali dokumentacije • proces je zaustavljen na prošnjo uporabnika Ko spremenimo status iz ON HOLD na WIP, moramo prej spremeniti dogovorjeni čas za izvedbo (*angl. due date*).
ZAPRTO (CLOSED)	Dodeljen je, ko je incident rešen in je rešitev prenesena na produkcijski sistem, rešitev dokumentirana, nalog zaprt in ključni uporabnik informiran.

Povezave med časovnimi intervali in statusi nalogov so naslednje:



Kot vidimo iz zgornje slike, sta status naloga in časovni interval povezana z mejniki. Pri mejniku »Nalog je bil vpisan« dobi nalog status »ODPRTO« in teči mu začne reakcijski čas. Pri mejniku »Agent je sprejel lastništvo nad incidentom« dobi incident status »DELO V TEKU« in teči začne rešitveni čas. Pri mejniku, »Incident je bil rešen …« dobi nalog status »ZAPRTO« ter rešitveni čas preneha teči.

Kategorizacija stopenj urgentnosti se uporablja za klasifikacijo incidenta, ki ga na začetku skupaj opredelita ključni uporabnik ter oseba iz SAP EE kompetenčnega centra, preden zapišeta incident v nalog in ga dodelita agentu v reševanje. Stopnja urgentnosti je zelo pomembna, saj z njo določimo, v kakšnem časovnem okviru naj bo neki incident rešen.

Stopnja urgentnosti	Opis
1	Incident ima merljiv, velik vpliv na poslovanje, kritične resurse ali procese **brez takojšne nadomestne rešitve**.
2	Incident ima vpliv na poslovanje, kritične resurse ali procese **z omejeno nadomestno rešitvijo**.
3	Incident ima vpliv na poslovanje, toda ima zadostno nadomestno rešitev, da je poslovanje mogoče z malimi omejitvami za omejeno časovno dobo.
4	Incident ima manjši vpliv na procese ali na uporabnika (vseeno je prepoznan kot napaka delovanja). Uporabniki lahko delajo z okvaro za kratko omejeno časovno dobo.
5	Incident nima vpliva na procese ali uporabnike (vseeno je prepoznan kot napaka v delovanju). Uporabniki lahko delajo z okvaro.

2.4 Splošni postopek upravljanja tehničnih incidentov v farmacevtskem podjetju

Kot sem omenil že zgoraj, je farmacevtsko podjetje ločilo reševanje SAP incidentov ter reševanje ostalih incidentov, zaradi same prepletenosti procesnega toka s poslovnim procesom in zaradi učinkovitejšega reševanje le-teh.

2.4.1 Organizacijska struktura centra za podporo uporabnikom (CPU)

Tako kot pri procesnem toku preko ključnega uporabnika so tudi tukaj najprej definirali subjekte, ki nastopajo v procesu, ter vse nivoje podpore. Ti so:

1. nivo podpore:

- agenti CPU (sodelavci IT-ja znotraj oddelka CPU)
- koordinator CPU
- skrbnik baze znanja

2. nivo podpore:

- sodelavci IT-ja – skrbniki za aplikacije in tehnične sisteme

3. nivo podpore:

- vodstvo IT-ja
- zunanji sodelavci in podjetja – skrbniki za aplikacije in tehnične sisteme

2.4.2 Opis procesa

Prijava incidenta in odprtje naloga

Uporabniki lahko prijavljajo incidente na sledeče načine:

- telefonsko
- osebno
- po elektronski pošti
- preko intranetne vnosne forme

Vsak CPU agent mora na vseh nivojih podpore zabeležiti vsako prijavo incidenta v »Help Desk« aplikacijo. V primeru prijave incidenta preko intranetnega obrazca ali preko elektronske pošte, mora CPU agent na 1. nivoju podpore obdelati zahtevo, tudi če uporabnika ni dobil. Ta ne sme ostati odprta, da ne bi ostali agentje mislili, da se morajo lotiti reševanja iste vloge.

Prijava incidenta in odprtje naloga za informacijski sistem SAP

Ob prijavi incidenta CPU agentu je ta na 1. nivoju odgovoren le za odpravo napak 1. nivoja (inicializacija gesla, odblokiranje uporabnika, rešitev tehničnih ali sistemskih težav ob uporabi sistema SAP in strojne ali programske opreme).

V primeru prijave incidenta na CPU, za katerega se med procesom reševanja izkaže, da je procesno-vsebinske narave, se postopa po naslednjih korakih:

- elektronsko sporočilo, ki vsebuje opis incidenta, dosedanje korake, morebitne posnetke ekrana (*angl. screen shots*) in številko incidenta se pošlje ključnemu uporabniku in v vednost tudi končnemu uporabniku, ki je prijavil incident,
- CPU agent v odprti incident prenese vsebino elektronskega sporočila z datumom in imenom ključnega uporabnika kot rešitev ter zaključi incident.

Kategorizacija storitev CPU

Storitve CPU delimo glede na kategorizacijo prioritete na:

- incidente
- naloge

Incidenti zahtevajo čimprejšnji odziv in posredovanje (tehnično pomoč ali svetovanje), saj okvara ali problem onemogoča uporabnikom normalno delovanje.

Naloge so ostale storitve, za katere CPU agent v dogovoru z uporabnikom določi rok, do kdaj naj bodo izvedene. Sem spadajo naročanje, montiranje in selitve računalniške opreme in organizacija računalniških izobraževanj.

Vsaka uporabniška zahteva je zasnovana glede na razpoložljiva sredstva, število prijav in glede na potrebe podjetja. Z določitvijo prioritete posameznim zahtevam lažje določimo vire za njeno reševanje.

Tabela 1: Stopnje prioritet

Prioriteta	Opis	Reakcijski čas	Čas reševanja
1 – kritično	Napake, ki kritično vplivajo na poslovni proces – odpoved strežnika	Takoj	Isti dan, razen če velikost napake to onemogoča
2 – nujno	Napake, ki vplivajo na poslovni proces (strojna ali programska napaka) – odpoved tiskalnikov v proizvodnji, odpoved mrežnega stikala…	Največ 1 ura	Isti dan, razen če velikost napake to onemogoča
3 – pomembno	Napake, ki bistveno ne vplivajo na poslovni proces: vse vrste incidentov, ki uporabnikom onemogočajo normalno delo	Največ 2 uri	Isti dan
4 – nizka	Napake, ki ne vplivajo na poslovni proces: vse vrste incidentov, ki uporabnikom onemogočajo normalno delo, ki pa jih ne moremo takoj rešiti zaradi nedosegljivost uporabnika	V dogovoru z uporabnikom	Isti dan oz. v dogovoru z uporabnikom
5 – kontrola	Nadzor delovanja funkcionalnosti	Periodično ali v dogovoru z uporabnikom	Isti dan oz. v dogovoru z uporabnikom
6 – drugo	Ostale storitve: naročanje računalniške opreme in organizacija računalniških izobraževanj,	V dogovoru z uporabnikom	Isti dan oz. v dogovoru z uporabnikom
7 – distribucija	Distribucija strojne opreme: montiranje in selitve računalniške opreme	V dogovoru z uporabnikom	V dogovoru z uporabnikom

*Prioritete od **1 do 4** opredeljujejo **incidente**, prioritete **od 5 do 7** pa **naloge.**

Vir: Interna dokumentacija, 2006.

Posredovanje naloge - eskalacija

Po izpolnjeni zahtevi se določi izvajalca. Če zna izvajalec sam rešiti incident, si sam dodeli nalogo, v nasprotnem primeru pogleda v Bazo znanja. Če še vedno ne zna rešiti naloge, jo posreduje drugemu agentu na istem ali višjem nivoju. Pri posredovanju izpolni opcijska polja:

- »Additional description«
  - v to opcijsko polje vpišemo podroben opis napake.
  - v primeru, ko nalogo posredujemo izvajalcem na drugo lokacijo, se mora v to polje obvezno vpisati lokacija uporabnika.
- »Additional contacts«: če nalogo posredujemo izvajalcem na drugo lokacijo, se mora v to polje obvezno vpisati interna telefonska številka uporabnika.

V primeru, ko agent na 2. nivoju posreduje začasno rešitev agentu na 1. nivoju, se odprti nalog posreduje agentu, ki je podal začasno ali trajno rešitev. Agent na 1. nivoju podpore pa mora odpreti nov nalog z enako vsebino in kot rešitev vpisati posredovano začasno ali stalno rešitev ter ime agenta, ki jo je posredoval.

Lastništvo naloge

Agent, ki odpre nalogo, postane tudi njen lastnik. V primeru, da jo dodeli samemu sebi, mora stremeti k temu, da jo reši v predpisanem roku, ki je naveden zgoraj v tabeli stopnje prioritet.

V kolikor pa je nalogo posredoval drugemu agentu, mora dnevno pregledovati odprte naloge v »Help Desk« aplikaciji in obveščati izvajalce, ki nalog še niso zaključili, da jih razrešijo v najkrajšem možnem času.

Rešitev naloge

Ko agent reši nalogo in dobi tudi potrditev od uporabnika, da je njegov incident res rešen, mora v aplikacijo »Help Desk« vpisati:

- podroben opis postopka reševanja incidenta,
- na kakšen način je rešil nalogo:
  - preko telefona,
  - osebno,
  - s priklopom na uporabnikov računalnik.
- dejansko število ur, porabljenih za razrešitev incidenta. Najmanjši možen vpisan čas je 0,1 ure.

V prilogi 3 si lahko pogledate ERP diagram procesa upravljanja s tehničnimi incidenti v farmacevtskem podjetju.

3 Skladnost upravljanja incidentov s SOX zahtevami

V tem poglavju bom na kratko predstavil SOX (Sarbanes-Oxley) zakon, razloge za njegov sprejem in njegov vpliv na informacijsko tehnologijo ter na Slovenijo oz. Evropsko Unijo. Predstavil bom tudi izvajanja tega zakona v farmacevtskem podjetju in to, kako so njegovo izvajanje implementirali v proces upravljanja z incidenti. Na koncu poglavja bom podal tudi oceno uvedenega procesa upravljanja z incidenti v farmacevtskem podjetju.

3.1 SOX (Sarbanes-Oxley) zakon in razlogi za njegov sprejem

Že iz samega naslova zakona je razviden njegov namen: »Zakon za točno in zanesljivo računovodsko poročanje korporacij naložbenikom ter drugim uporabnikom računovodskih poročil v skladu z zakoni o vrednostnih papirjih« (Mehle, 2005, str. 3). Z njimi naj bi tako preprečili, da bi menedžerji uporabljali nedovoljene ali pa vsaj dvomljive računovodske operacije, kar je bila posledica pomanjkanja notranjih kontrol nad samim poslovanjem v podjetju, pomanjkanjem nadzora nadzornih svetov nad menedžerji ter predvsem sodelovanja med revizorji in menedžerji (Kovačič, 2002, str. 2). To pa so hoteli doseči z reformiranjem računovodske revizijske panoge in zaostritvijo korporacijskega upravljanja.

Zakon SOX se imenuje po svojih avtorjih: Paul S. Sarbanesu, senatorju v Združenih državah Amerike, in Michaelu G. Oxleyu, ameriškemu kongresniku.

SOX zakon je bil sprejet 23. januarja 2002, v veljavo pa je stopil 30. junija 2002 na ozemlju ZDA. Večina zakona je stopila v veljavo takoj po sprejetju, le posamezna poglavja so stopila v veljavo kasneje, ko so zasnovali pravila in postavili pogoje, pomembnei za posamezna poglavja.

Sprejetje SOX zakona pomeni največjo zakonodajno reformo kapitalskega trga v ZDA po letu 1934, ko je bil sprejet zakon o vrednostnih papirjih (Section 404, Practical Guidance for Management, 2004, str. 12).

SOX zakon je nastal kot odgovor na številne računovodske in revizijske škandale, ki so prišli na plan na začetku 21. stoletja v zelo uglednih ameriških podjetjih, kot so Enron, Worldcom, HealthSouth, Xerox, Dynegy, Adelphia, Global Crossing itd. To je povzročilo veliko nezaupanje v kapitalske trge, katerega posledice se niso čutile samo v ZDA, ampak tudi na ostalih razvitih trgih po celem svetu (Benedek, 2002).

3.2 Cilji SOX-a

S SOX zakonom so v ZDA hoteli predvsem znova pridobiti zaupanje naložbenikov, ki se je razblinilo po propadih zgoraj naštetih podjetij. To so zakonodajalci hoteli doseči s petimi ukrepi (Samec, 2003, str. 3):

- strožje reguliranje transakcij menedžmenta in nadzornega sveta, ki lahko pripelje do konflikta interesov,
- nadzorna funkcija nadzornega sveta se izboljšuje z revizijskim odborom,[1]
- strožje definiranje neodvisnosti revizorjev, posebej z uvedbo odbora za javno nadzorstvo revizijskih družb,[2]
- zaveza družb o stalnem poročanju, pri čemer je vsebina teh poročil občutno bolj nadzorovana,
- uvedba strožjih določil o osebni odgovornosti članov nadzornega sveta in izvršnega direktorja ter finančnega direktorja.

Poleg teh, zgoraj naštetih razlogov so si zakonodajalci z zakonom prizadevali obnoviti tudi verodostojnost računovodskih izkazov in poročil, tako da so v SOX zakonu definirali višjo stopnjo odgovornosti, zanesljivosti in preglednosti. Za hitrejšo povrnitev zaupanja javnosti v poročila navajata DiPiazza in Eccles (2002, str. 15) posebno poročevalsko verigo, katere člani so:

- menedžment, ki pripravi ali odobri informacije, namenjene investitorjem in drugim deležnikom,
- nadzorni svet, ki zastopa interese deležnikov in je v njihovem imenu odgovoren za nadzor nad delovanjem menedžmenta,
- neodvisni revizorji, ki jamčijo za pravilnost računovodskih izkazov in drugih informacij, posredovanih na kapitalske trge,
- distributorji informacij, ki povzamejo informacije in jih posredujejo drugim v uporabo,
- zunanji analitiki, ki poleg informacij, pridobljenih s strani menedžmenta, uporabijo še lastne analize za priporočila investitorjem,
- investitorji in drugi deležniki, ki so končni uporabniki informacij.

Vsi zgoraj našteti »člani« verige poročanja po SOX-u so tudi grafično predstavljeni na spodnji sliki.

[1] Audit Committee
[2] Public Company Accounting Oversight Board - PCAOB

Slika 8: Veriga računovodskega poročanja

Poslo-vodstvo	Odbor direktorjev, nadzorni odbor (z revizijskim odborom vred)	Neodvisni revizorji	Poslovni poročevalci	Poslovni analitiki	Naložbeniki in drugi uporabniki rač. izkazov
Postavljavec standardov in/ali zakonodaje in tržne sile					

Vir: FEE, 2003, str. 6.

Za vse zgoraj naštete člene verige morajo veljati naslednja načela:

- **Transparentnost**: podjetja so dolžna zagotoviti delničarjem in drugim deležnikom informacije, potrebne za odločanje, te pa morajo biti transparentne, kar pomeni, da prikazujejo realno sliko finančnega položaja podjetja, realne rezultate računovodskih transakcij, realno sliko denarnega toka in realno sliko drugih vidikov poslovanja.
- **Odgovornost**: vsak člen v zgoraj predstavljeni verigi poročanja po SOX-u mora prevzeti odgovornost, da bo v sodelovanjem z drugimi člani v verigi opravil svojo nalogo.
- **Poštenost**: transparentnost in odgovornost sta odvisni od poštenosti ljudi, da naredijo pravo stvar in ne le tistega, kar je dopustno. To načelo je osnova za zaupanje javnosti v finančna poročila.

3.3 Vpliv SOX zakona na Slovenijo

Družbeno-politična in pravna ureditev v ZDA se razlikuje od tovrstnih ureditev v Evropi, zato ne moremo preprosto prenašati ameriških predpisov in pravnih modelov v naše pravno in družbeno okolje, kar je pomenilo prvo omejitev uvedbe SOX zakona v Evropi, kot druga pa nastopa dejstvo, da se države v Evropski uniji med sabo zelo razlikujejo tako v stopnji gospodarskega razvoja, družbeni ureditvi, zgodovinskem okolju in vrednostnem okolju kot tudi v položaju in razvoju revizijske stroke.

Pri ureditvi javnega nadzora v Sloveniji bo potrebno upoštevati tako družbeno okolje kot tudi položaj revizijske stroke v družbi (Odar, 2004, str. 173). V Sloveniji SOX zakonodaja ne bo temelj za spremembo revizijske stroke, ampak bo to osma smernica Evropske unije, ki jih je le-ta sprejela po padcu Enrona, da bi preprečila podobne afere na svojem ozemlju.

Čeprav osma smernica Evropske unije ne omenja nerevizijskih storitev, ki jih revizijske družbe ne smejo opravljati, tako kot SOX, so nekatera revizijska podjetja v Sloveniji, kot je videti, vseeno upoštevala določbe SOX-a. To pa pomeni, da so družbe ločile revizijske storitve od nerevizijskih, na primer:

- z organizacijsko strukturo v podjetju,

- z odprodajo nerevizijskih storitev – kot dela podjetja drugim družbam ali z oblikovanjem novega podjetja, ki ponuja nerevizijske storitve,
- z vodenjem stroge evidence, da se istemu podjetju ne ponudi hkrati revizijskih in nerevizijskih storitev ter da se ne izbira naključnih podjetij kjerkoli po svetu.[3]

Na podlagi SOX zakona so bili pripravljeni tudi »Standardi, ki se nanašajo na revizijski odbor družbe, katere vrednostni papirji kotirajo na organiziranem ameriškem trgu«[4]. Bistvo teh standardov je prepoved kotiranja vrednostnih papirjev, katerih izdajatelj ne uskladi svojega poslovanja z zakonom. Te zahteve se nanašajo na neodvisnost članov revizijskega odbora in na njihovo odgovornost za računovodsko prakso podjetja. Te standarde morajo upoštevati tudi vsa slovenska podjetja, ki želijo ali pa že kotirajo na ameriški borzi.

3.4 Vpliv SOX zakona na informacijsko tehnologijo

SOX zakon je namenjen kontroli področja računovodskih poročil in notranjih kontrol, a posredno vpliva tudi na informacijsko tehnologijo, ki je najpomembnejša pri podpori izvajanja poslovnih procesov, zato ni čudno, da je največ prilagoditev prišlo ravno na informacijsko-tehnološkem področju. Nekateri strokovnjaki so udarec zahtev, ki jih je prinesla nova zakonodaja, primerjali celo s problemom leta 2000 (Schultz, 2004, str. 1). Kako veliko spremembo je prinesla zakonodaja, pa pove tudi predvidevanje Logana in Mogulla (2003, str. 3), da bodo podjetja do leta 2005 za področje informacijske tehnologije v povprečju namenila več kot 2 milijona dolarjev.

Informacijski sistemi se uporabljajo za ustvarjanje, spreminjanje, brisanje, shranjevanje, iskanje in prenos podatkov, zato morajo imeti vgrajene kontrole, ki zagotavljajo, da so podatki zanesljivi. Če so informacijski sistemi ranljivi, imajo dostop do podatkov nepooblaščene osebe, kar pomeni, da obstaja verjetnost, da so računovodski podatki nepravilni, saj se ne ve, ali je prišlo do ponarejanja podatkov ali ne. Za zmanjšanje tveganja, da se to zgodi, moramo povečati varnost na vseh ključnih sistemih. Po raziskavi iz leta 2004 (The SarbanesOaxley Act of 2002, 2005) je bilo 50% vseh napadov na podjetja izvedenih znotraj podjetja. Namen napadov je bil različen, od dostopanja zaposlenih do področij, za katere niso imeli pooblastil, do industrijskega vohunstva.

Zaupanje v računovodska poročila je odvisno predvsem od integritete informacijskega sistema in procesov, ki podpirajo računovodske podatke, zato mora revizor preveriti sledeče (Kim, 2003, str. 13):

[3] Po SOX-u revizijska podjetja ne smejo ponuditi revizijskih in nerevizijskih storitev isti stranki. Ker pa mnoge revizijske hiše delujejo po celem svetu in imajo tudi stranke podružnice, predstavništva in povezana podjetja, morajo revizijske družbe voditi natančno evidenco o tem, s katerim podjetjem sodelujejo, saj se lahko v nasprotnem primeru krši zakon.

[4] Standards relating to listed company Audit Committe

- če imajo zaposleni pravilna pooblastila pri procesih, s katerimi se uvedejo postopki za odobritev transakcij,
- ali so ločene funkcije, s katerim se doseže preprečitev zlonamernih postopkov pooblaščanja,
- ali so kontrole, ki zagotavljajo, da gredo vse spremembe skozi dokazan pooblaščen postopek, učinkovito nastavljene,
- ali je dokumentacija o vseh spremembah na pooblastilih in na informacijski strukturi pravilno vodena,
- ali se izvaja dokumentiranje izjem ali sprememb, narejenih izven okvira zajetih sprememb, ter ali se izvaja dokumentiranje vseh ad hoc popravkov.

V zakonu sicer ni izrecno določeno, katere tehnologije mora podjetje uporabljati, da bo zagotovilo ustreznost informacijskih sistemov, vendar pa določa, da so procesi, ki podpirajo osnovne procese ali pa skrbijo za računovodske procese, podvrženi nadzoru revizorjev in regulatorjem. Zaradi neupoštevanja določil SOX zakona so zagrožene visoke denarne kazni, zato je v interesu menedžmenta, da je skladnen z zakonom. Ta zahteva predvsem natančnost in popolnost vseh informacij, ne glede na to ali gre za interne informacije ali pa poročila, ki so namenjena investitorjem ali drugi zainteresirani javnosti. Podjetja morajo omogočiti enostaven vpogled v vse pomembnejše dogodke, ki bodo imeli pomembne posledice za bodoče poslovanje podjetja. Hkrati pa nam mora informacijski sistem omogočati sledljivost izvajanja operacij za vsakega uporabnika, razmejevanje dolžnosti ter izvajanje avtomatiziranih kontrol. Edino v tem primeru lahko podjetje doseže najvišjo stopnjo razvitosti sistema notranjih kontrol.

Vedeti je potrebno, da pravi odgovor na SOX zahteve ne leži v tehnologiji ali programskem paketu, marveč ga je potrebno iskati v ustreznih poslovnih procesih. Vloga informacijske tehnologije je le v optimalni izrabi tehnologije za izboljšanje teh procesov. Po standardu odbora za javno nadzorstvo revizijskih družb (PCAOB) so glavna področja odgovornosti informacijske tehnologije v tem procesu sledeča (Štefančič in Štefančič, 2004, str. 6):

- razumevanje postopkov notranjega kontroliranja in poročanja,
- vzpostavitev informacijskega sistema, ki podpira notranje kontroliranje,
- identifikacija tveganj, povezanih z informacijskim sistemom,
- načrt in implementacija kontrol, ki zmanjšujejo tveganja, ter stalno spremljanje njihove učinkovitosti,
- dokumentiranje in preverjanje informacijskih kontrol,
- zagotovitev posodabljanja in spreminjanja nadzora informacijskega sistema, ki odseva spremembe v procesu računovodskega poročanja.

Dejstvo je, da učinkovit informacijski sistem zbiranja, nadzora, upravljanja in dokumentiranja poslovnih procesov daje podjetjem prednost pri vpeljevanju normativov in standardov SOX

zakona. Pri tem pa se mora podjetje odločiti, ali bo uporabilo ta informacijski sistema samo za doseganje SOX standardov ali pa tudi za optimizacijo poslovanja.

3.5 Pregled skladnosti upravljanja incidentov z zahtevami SOX zakona v farmacevtskem podjetju

V farmacevtskem podjetju so morali, če so hoteli s svojimi izdelki prodreti na ameriški trg, začeti izvajati notranjo kontrolo po SOX zakonu,. A kontrole niso mogli izvajati samo nad procesom računovodskega poročanja, temveč tudi nad procesom proizvodnje zdravil. Pod to kontrolo pade tudi informacijski sistem, saj ta kontrolira večino procesov izdelave zdravil in vodenja poslovanja.
Sam nadzor je že dodobra dodelan, vendar so izboljšave še vedno možne in tudi potrebne za izpolnjevanje določil 404. člena SOX zakona, saj ta med drugim določa, da se mora sistem za nadzor na vsake toliko časa spremeniti.

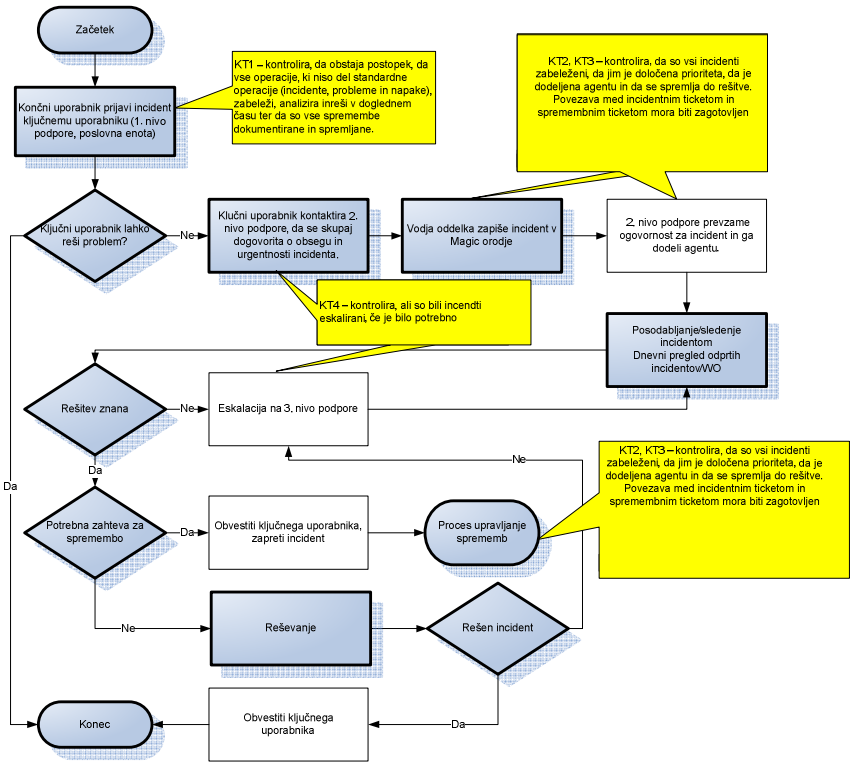
V farmacevtskem podjetju zajemajo vseh pet osnovnih značilnosti notranjega kontroliranja:
1. **kontrolno okolje** – zavedanje odgovornih oseb se je na ravni skupine preko kodeksa ravnanja, pravilnikov, obvestil in drugih metod preneslo na menedžment in zaposlene v podjetju,
2. **ocena tveganja** – mora biti podana za vse ključne procese,
3. izvajajo se **preventivne kontrolne aktivnosti –** odobritve, pregledi poslovanja…
4. **pretok informacij in komunikacija** – zaposleni so primerno obveščeni o svoji vlogi notranjih kontrol,
5. **ugotavljanje slabosti in izboljšava procesa.**

Farmacevtsko podjetje izvaja notranjo SOX kontrolo vsake štiri mesece, čeprav kontrolo sproti izvaja oddelek za kakovost na informacijskem oddelku. Pri SOX kontroli naključno izberejo že vnaprej določeno število vzorcev (ponavadi 20 vzorcev). S takšnimi kontrolami dobijo vzorec, na podlagi katerega vidijo, kje je njihov sistem ranljiv, na podlagi teh rezultatov pa se nato izvede izboljšava procesa nadzora nad posameznimi procesi poslovanja.

Na področju upravljanja incidentov farmacevtsko podjetje preverja štiri kontrolne točke (v nadaljevanju KT):
- KT1 – preverja, če obstaja splošni postopek za upravljanje incidentov,
- KT2 – kontrolira, če so bili incidenti zabeleženi, če jim je bila določena prioriteta in agent, ki jih bo rešil, ter če so bili v resnici incidenti tudi rešeni,
- KT3 – preverja, če je agent spremljal incident in dodajal zapise v polje »action log«,
- KT4 – preverja, če je bil incident eskaliran (če je bilo to potrebno).

Kontrolna točka 1 se preverja enkrat letno, ostale tri pa vsake štiri mesece.

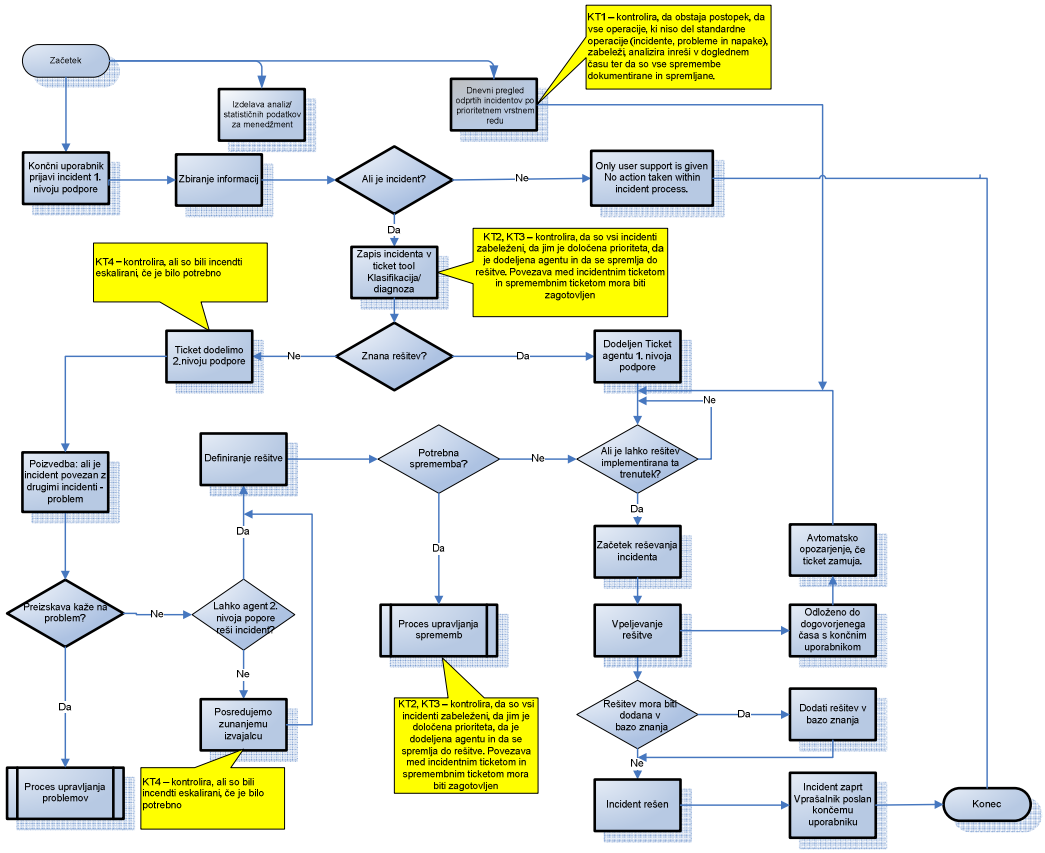
Slika 9: Splošni postopek upravljanja z incidenti v sistemu SAP s SOX kontrolnimi točkami



Vir: Interna dokumentacija podjetja, 2006.

Zgornja slika prikazuje proces upravljanja incidentov v SAP sistemu in iz nje je razvidno, v katerem delu tega procesa se vključuje kontrola SOX. Kot je razvidno iz slike, se kontrolna točka 1 pojavi že na začetku in preverja, ali obstaja splošni postopek za upravljanje z incidenti. Naslednji dve kontrolni točki se pojavita ob zabeleženju incidenta ter na začetku procesa upravljanja s spremembami in preverjata, ali so vsi incidenti zabeleženi, ali so jih agentje prevzeli v za to določenem času, ali se spremlja incident do rešitve in ali obstaja v primeru, da incident preide v proces upravljanja s spremembami, povezava, vnos številke za spremembo na incidentni nalog. Kontrolna točka 4 pa preverja, ali je bil incident, če je bilo to potrebno, ustrezno eskaliran,.

Slika 10: Splošni postopek upravljanja s tehničnimi incidenti s SOX kontrolnimi točkami



Vir: Interna dokumentacija podjetja, 2006.

Zgornja slika prikazuje splošni postopek upravljanja s tehničnimi incidenti v farmacevtskem podjetju z vpeljanimi SOX kontrolnimi točkami. KT1 se tukaj pojavi pri dnevnem pregledu dnevnih incidentov po prioritetnem vrstnem redu in kontrolira, ali obstaja splošni postopek za upravljanje z incidenti. KT2 ter KT3 se tudi tukaj pojavita pri zabeleženju incidenta ter preverjata, ali so bili vsi incidenti zabeleženi, ali sta jim bila določena prioriteta in agent ter ali se je incident spremljal do rešitve. Spremljata pa tudi, ali obstaja v incidentnem nalogu zapis številke zahtevka za spremembo v primeru, da preide proces upravljanja z incidenti v proces upravljanja s spremembami.

3.5.1 Sprotni pregled skladnosti upravljanja incidentov v SAP sistemu s SOX zahtevami

Poleg zgoraj omenjene SOX kontrole se v farmacevtskem podjetju izvaja tudi dnevna kontrola zapisov incidentov, ki jih izvaja “Kontrolor zapisov v programu »Magic«”, saj je zelo pomembno, da je stanje zapisov v program realno, kajti le tako lahko spremljamo, kako učinkoviti smo, in tako pripomoremo h kar največjemu zadovoljstvu strank.

»Magic«

Program »Magic« je IBM-ova programska oprema, narejena po ITIL standardih za spremljanje incidentov, ki ga uporablja farmacevtsko podjetje za beleženje ter spremljanje incidentov. Program je spletna (*angl. WEB*) aplikacija, kar je zelo pomembno zaradi razpršenosti predstavništev po celi Evropi, Ameriki in Aziji ter proizvodnih obratov v Romuniji in na Poljskem. Na ta način lahko vsi beležijo incidente, SAP EE kompetenčni center pa jih dobi v trenutku.

Program »Magic« vsebuje vse bistvene elemente, ki jih priporočajo ITIL standardi, ter je narejen tako, da omogoča spremljanje SOX kontrolnih točk.

Odgovornosti

Vodja SAP kompetenčnega centra EE (oziroma namestnik) je odgovoren, da program »Magic« odraža pravilno, popolno in ažurno stanje vseh nalog s področja incidentov in nadgradenj ter da se incidenti in nadgradnje zaključujejo v dogovorjenih rokih.

Kontrolor zapisov v programu »Magic« je odgovoren za dnevno izvajanje kontrole ter za ustrezno opominjanje informatikov o morebitnih nepravilnostih, zamujenih incidentih ter nadgradnjah ter o incidentih in nadgradnjah, ki se približujejo roku izvedbe in še niso zaprti. Odgovoren je tudi za obveščanje vodje SAP kompetenčnega centra o svojih ugotovitvah.

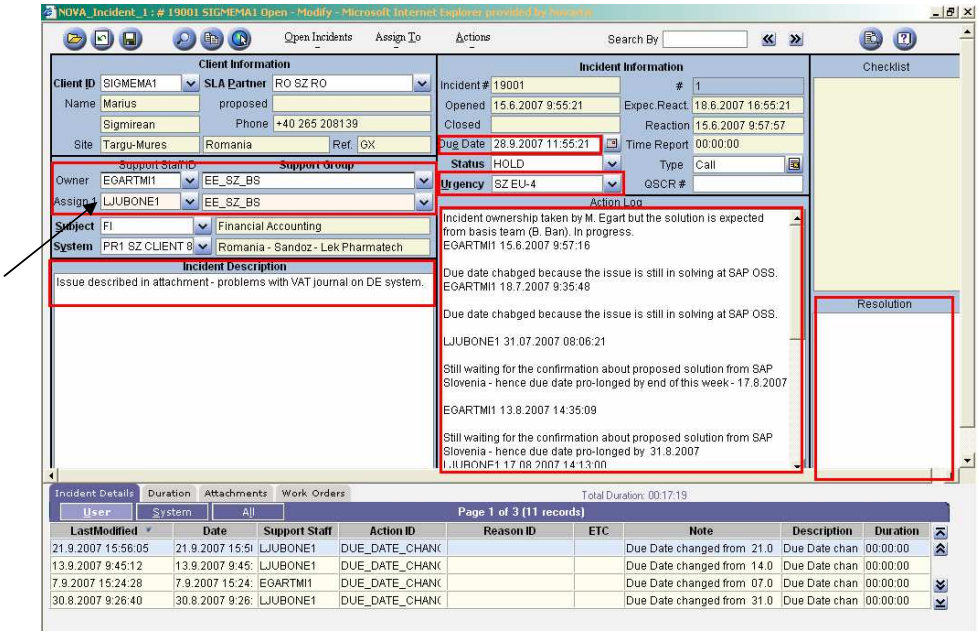
Kontrolne točke

Kontrolne točke, ki jih kontrolor zapisov v programu »Magic« kontrolira, so naslednje:

- ali obstaja vnos v polju »Assign ID«, ki je obvezen, saj nam pove, kdo rešuje incident,
- ali obstaja vnos v polju »Owner ID«, ki je obvezen, saj nam pove, kdo je lastnik incidenta,
- smiseln opis incidentov,
- ustrezen zapis urgentnosti (po določenih standardih),
- preverja zapise v polju »Action log« – vsaka akcija, ki jo kdo naredi glede incidenta, mora biti vpisana v polje »Action log« (še posebej v primerih prioritetne stopnje1 ali 2, v primeru statusa HOLD ter v primeru spreminjanja roka izvedbe),
- rok izvedbe – da se le-ta ne prekorači ali pa da se zaradi določenih vzrokov prestavi s soglasjem stranke,
- eskalacija incidentov z nivojem nujnosti 1 ali 2 (ustrezen zapis v polju »Action log«),
- vpis v polje »Resolution« - ko se incident zapre, se mora v polje vpisati rešitev.

Polja so prikazana na spodnji sliki.

Slika 11: Magic in SOX kontrolne točke



Vir: Interna dokumentacija podjetja, 2007.

V programu »Magic« se kontrolirajo samo tri KT, saj KT1 kontrolira, če obstaja splošni postopek za upravljanje sprememb. Kot sem omenil že zgoraj, KT2 ter KT3 kontrolirata polja, označena z rdečo barvo, in sicer kontrolirata, ali so bili vneseni vsi pomembni podatki ter ali so bili vneseni pravilno. V primeru, da preide proces upravljanja z incidenti v proces upravljanja s spremembami, se mora vnesti tudi polje QSCR#. Medtem ko KT 4 preverja, ali je bil incident eskaliran, kar prikazuje puščica.

3.5.2 Sprotni pregled skladnosti upravljanja tehničnih incidentov s SOX zahtevami

Tudi v primeru tehničnih incidentov se v farmacevtski družbi izvaja sprotna kontrola reševanja incidentov, zato da so skladni s SOX zahtevami. Sam postopek kontrole je nekoliko drugačen kot pri SAP sistemu, vendar je namen isti, to je zagotavljanje čim večje sledljivosti reševanja incidentov in s tem tudi večje hitrosti reševanja ter zagotavljanje čim večjega zadovoljstva uporabnikov.

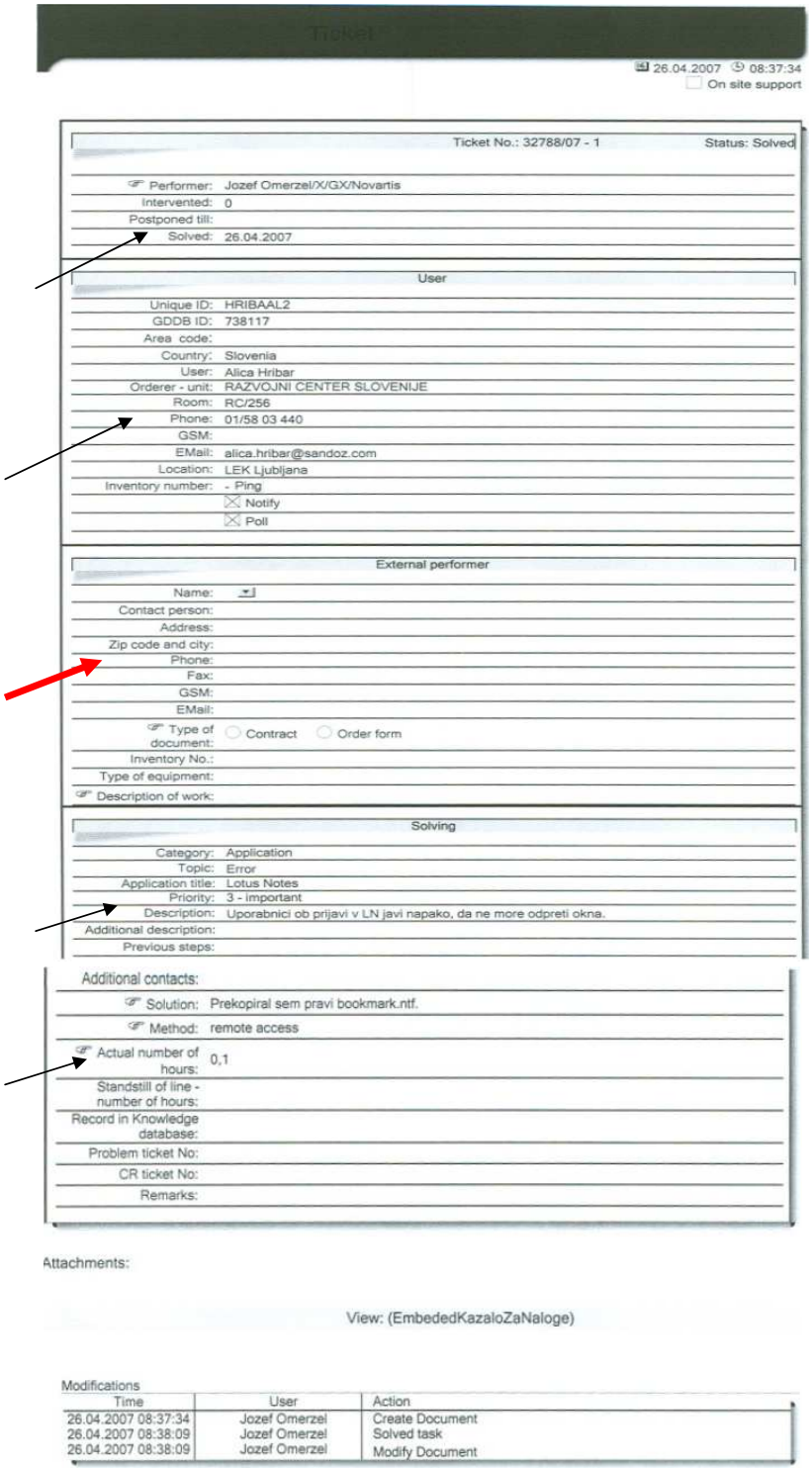
Kontrola na dnevni bazi se izvaja po naslednjem vrstnem redu:

- **pregled pravilnosti vpisov v »Help Desk« aplikacijo** – tu se kontrolira, ali sta uporabnik in lastnik/agent, ki je prevzel incident, pravilno izpolnila vsa potrebna polja. Pregleda se naslednja polja:

- »User« – ali je uporabnik pravilno izpolnil vse svoje podatke oziroma ali je agent, ki je sprejel prijavo incidenta, pravilno izpolnil vse podatke o uporabniku,
- »Performer« – ali je vpisano ime agenta, ki rešuje incident,
- »Solved« – vpisan mora biti datum rešitve incidenta,
- »External performer« – ali je agent v primer, da je bil za rešitev incidenta potreben zunanji izvajalec, pravilno izpolnil vsa potrebna polja,
- »Solving« – ali je incident smiselno opisan, ali je pravilno določena prioriteta ter z njo povezana odzivnost agenta in ali so navedene vse akcije, ki so bile potrebne za razrešitev incidenta.

- **izvedba eskalacije** – tu se preverja, ali je bila eskalacija v primeru, da je bila potrebna, pravilno izvedena.
- **poizvedba lastnika incidenta** – lastnik incidenta se osebno prepriča, ali je bil incident tudi dejansko razrešen. Šele po tej poizvedbi dobi incident status »Zaključen«.

Slika 12: Help Desk aplikacija in SOX kontrolne točke



Ticket

26.04.2007 08:37:34
On site support

Ticket No.: 32788/07 - 1 Status: Solved

Performer:	Jozef Omerzel/X/GX/Novartis
Intervented:	0
Postponed till:	
Solved:	26.04.2007

User

Unique ID:	HRIBAAL2
GDDB ID:	738117
Area code:	
Country:	Slovenia
User:	Alica Hribar
Orderer - unit:	RAZVOJNI CENTER SLOVENIJE
Room:	RC/256
Phone:	01/58 03 440
GSM:	
EMail:	alica.hribar@sandoz.com
Location:	LEK Ljubljana
Inventory number:	- Ping
	☒ Notify
	☒ Poll

External performer

Name:	
Contact person:	
Address:	
Zip code and city:	
Phone:	
Fax:	
GSM:	
EMail:	
Type of document:	○ Contract ○ Order form
Inventory No.:	
Type of equipment:	
Description of work:	

Solving

Category:	Application
Topic:	Error
Application title:	Lotus Notes
Priority:	3 - important
Description:	Uporabnici ob prijavi v LN javi napako, da ne more odpreti okna.
Additional description:	
Previous steps:	

Additional contacts:	
Solution:	Prekopiral sem pravi bookmark.ntf.
Method:	remote access
Actual number of hours:	0,1
Standstill of line - number of hours:	
Record in Knowledge database:	
Problem ticket No:	
CR ticket No:	
Remarks:	

Attachments:

View: (EmbededKazaloZaNaloge)

Modifications

Time	User	Action
26.04.2007 08:37:34	Jozef Omerzel	Create Document
26.04.2007 08:38:09	Jozef Omerzel	Solved task
26.04.2007 08:38:09	Jozef Omerzel	Modify Document

Vir: Interna dokumentacija podjetja, 2007.

Zgornja slika prikazuje izpis iz »Help Desk« aplikacije. Ta izpis se uporablja pri SOX ocenjevanju in na njem se lepo vidi, kateri podatki iz izpisa se preverjajo. Tudi tukaj se izvaja kontrola treh kontrolnih točk. KT1 preverja, ali obstaja splošni postopek za upravljanje z incidenti. KT2 ter KT3 preverjata, ali so bili vneseni vsi podatki ter ali so bili vneseni pravilno. Vsi podatki, ki jih preverjamo, so označeni s črnimi puščicami. V primeru, da proces upravljanja z incidenti preide v upravljanje s spremembami, moramo vnesti številko zahtevka za spremembo v polje »CR ticket No.«. KT4 preverja, ali je bila potrebna eskalacija incidenta. V tem primeru to ni bilo potrebno, polje, kjer bi moral biti zapis, pa označuje rdeča puščica.

3.6 Ocena vpeljave ter izvajanje procesa upravljanja z incidenti

Oceno bom speljal glede na kritične kazalnike učinkovitosti procesov, saj vsak kazalnik vsebuje določena merila, ki jih merimo in na osnovi katerih lahko rečemo, da se je proces izboljšal (Planning to implement service Management, 2002, str. 92).

Kritični kazalniki za upravljanje z incidenti:

- hitro reševanje incidentov:
  - znižanje odzivnega časa prvega nivoja podpore,
  - zvišanje števila incidentov, ki so bili rešeni v 1. nivoju podpore,
  - zvišanje števila rešenih incidentov ob prvem kontaktu,
  - znižanje števila napačno dodeljenih incidentov,
  - zmanjšanje števila napačno kategoriziranih incidentov.

Farmacevtsko podjetje je bilo najuspešnejše ravno pri hitrosti reševanja incidentov, saj so informatizirali komuniciranje med končnim uporabnikom ter 1. nivojem podpore. Agent je bil tako takoj, ko mu je končni uporabnik dodelil incident, o tem seznanjen preko e-pošte. Poleg tega so za reševanje SAP incidentov določili za 1. nivo ključne uporabnike (vodje oddelkov), tako da do 2. nivoja podpore (programerjev) pridejo samo incidenti, povezani z napakami v sistemu SAP, ne pa tudi vsebinske napake ali pa incidenti, ki se zgodijo zaradi neznanja uporabnikov. Sistem bi lahko še dodatno izboljšali tako, da bi na vidno mesto na intranetu dali tabelo s ključnimi uporabniki in njihovimi namestniki, zato da bi uporabniki lažje prišli do informacije, na koga se morajo obrniti, ko naletijo na incident. Za pospešitev reševanja tehničnih incidentov pa so v podjetju vzpostavili enotno telefonsko številko, ki so jo napisali na vsa vidna mesta v podjetju (na hodnike so postavili plakate in na vsak telefon nalepili nalepko s telefonsko številko centra za pomoč uporabnikom (angl. help desk)), tako da uporabnik, ko naleti na incident, ve, kam se mora obrnit po pomoč. Poleg tega so vzpostavili tudi informacijski sistem, da lahko agent v primeru, da se je uporabnik z incidentom obrnil na napačno mesto, incident hitro in enostavno dodeli pravemu agentu. Zapleta pa se zaradi birokracije, saj rešitev incidenta ni vpeljana na produkcijski sistem, dokler testiranje ni dokumentirano in ga uporabniki, ki so izvajali testiranje, niso podpisali, ter dokler pri večjih incidentih ni dokumentirana rešitev ter spremembe, ki so nastale pri reševanju incidenta.

- vzdrževanje kvalitete informacijskih storitev:
  - zmanjšanje prekinitev storitev, povzročenih zaradi incidentov,
  - znižanje povprečnega reakcijskega časa 2. nivoja podpore,
  - zmanjšanje števila zaostalih incidentov,
  - zvišanje števila rešenih incidentov, preden jih opazijo uporabniki,
  - zmanjšanje števila ponovno odprtih incidentov,
  - znižanje povprečnega časa reševanja incidentov.

Farmacevtsko podjetje je zelo veliko pridobilo tudi na kvaliteti informacijskih storitvah, saj vse spremembe dokumentirajo ter testirajo uporabniki. Poleg tega se je zmanjšal tudi povprečni rekreacijski čas ter čas, potreben za rešitev incidenta, saj celoten proces dnevno kontrolira kontrolor zapisov v programu »Magic«, ki agente opozarja na naloge 48 ur pred pretekom dogovorjenega časa za rešitev incidenta, pa tudi pred prekoračitvijo reakcijskega časa za prevzem incidenta. Zaradi birokracije, ki je potrebna zaradi SOX zakona (dokumentiranje testiranja rešitve, morebitnih sprememb zaradi incidenta ter uporabnikov s svojim delom), se prekorači čas reševanj pri manj pomembnih incidentih, ki se zaključijo šele, ko jih uporabniki nujno potrebujejo, saj šele takrat izpolnijo vso potrebno dokumentacijo, da se lahko rešitev prenese iz testnega okolja na produkcijsko okolje. Za ta problem bi lahko farmacevtsko podjetje naredilo prijaznejši obrazec za dokumentacijo, čeprav so postopek že nekoliko poenostavili. Prej se je moral namreč uporabnik, ki je pripravljal dokumentacijo ali izvajal testiranje, podpisati na vsako stran (kar predstavlja precejšen problem, ko dokumentacija obsega 100 strani ali več), sedaj pa le na prvo stran, vendar mora še vedno vso dokumentacijo speti.

- zvišanje celotne produktivnosti:
  - znižanje povprečnih stroškov reševanja incidentov,
  - zvišanje povprečnega števila obdelanih incidentov v prvem nivoju podpore,
  - pravočasna izdelava poročil.

Celotna produktivnost se je povečala glede na sorazmernost med zgoraj navedenimi dobrimi ter slabimi stranmi procesa za upravljanje incidentov.

- zadovoljstvo uporabnikov:
  - izboljšani rezultati anket o zadovoljstvu uporabnikov,
  - izboljšani odzivni čas centra za izvajanje storitev,
  - zmanjšanje števila uporabljanih navodil.

Uporabniki so dokaj zadovoljni s hitrostjo reševanja incidentov, saj v primeru, ko pride do več incidentov, agenti najprej rešijo incident z najvišjo prioriteto, šele nato pa tiste z manjšo prioriteto. Za uporabnika je sicer vedno najpomembnejši njegov incident, zato jih vsakršno čakanje na njegovo rešitev moti. Poleg tega jih moti tudi birokracija, ki so jo uvedli za

sledenje incidentom ter zaradi SOX zakona, saj imajo dovolj dela že z lastnimi zadolžitvami v podjetju, zdaj pa morajo dokumentirati še vse spremembe ter testiranja.
Pri dosedanjem delu sem se spoznal tudi s podjetjem, ki izdeluje gospodinjske aparate in se lahko po velikosti, organizaciji poslovanja ter poslovnem sistemu SAP primerja s farmacevtskim podjetjem. Največja razlika med njima je samo dobičkonosnost gospodarske panoge, v kateri poslujeta obe podjetji. Vendar sem kljub nizki dobičkonosnosti panoge za izdelovanje gospodinjskih aparatov pričakoval večjo organiziranost informacijskega oddelka v podjetju. Rešeno imajo samo reševanje tehničnih incidentov, medtem ko proces reševanja incidentov v sistemu SAP še ni določen, tako da ko uporabnik naleti na incident, pokliče v informacijsko službo naključnega informatika, ki prevzame incident v reševanje ali pa klic preveže do informatika, ki je odgovoren za modul poslovanja, v katerem se je zgodil incident.

Če bi ocenjecal obe podjetji z oceno od 1 do 10 glede uvedenega procesa upravljanja z incidenti, bi farmacevtsko podjetje ocenil z 8, medtem ko bi podjetje, ki se ukvarja z izdelavo gospodinjskih aparatov, ocenil s 3.

Sklep

Ob vse hitrejšem napredku je potrebna velika prilagodljivost, da lahko posameznik ali podjetje sledi potrebam na trgu. To pa je mogoče doseči, če imaš na razpolago pravo informacijo. Ta je danes najdražja dobrina na svetu, saj je zaradi poplave informacij težko izbrati pravo informacijo v pravem trenutku. Pri izbiri informacij nam pomaga, če imam na razpolago pravo informacijsko-komunikacijsko tehnologijo, informacijski sistem ter dobro organizirano informatiko. Upravljanje teh področij zaenkrat, vsaj po mnenju večine strokovnjakov, najbolj celovito pokrivajo ITIL standardi.

Sam proces upravljanja z incidenti, ki ga je uvedlo farmacevtsko podjetje in je opisan v diplomski nalogi, načeloma deluje odlično, vendar ga bo potrebno še prilagoditi, tako da bodo hitrost rešitve incidenta ter sledljivost incidentov, varnost in nemoteno delovanje sistema IT bolj uravnoteženi.

Po moji oceni je proces v farmacevtskem podjetju v teoriji dobro zastavljen ter dobro deluje tudi v praksi, a kljub temu sem opazil nekaj pomanjkljivosti, ki bi jih bilo potrebno odpraviti. Še najbolj moteče je dogajanje pri incidentih v sistemu SAP, kjer končni uporabnik v primeru, da naleti na incident, ne ve, na koga se lahko obrne, težava pa je tudi v tem, da ta podatek ni objavljen na intranetu, kjer bi lahko uporabnik pogledal, kdo je ključni uporabnik za posamezni modul v podjetju. Druga težava je ta, da za ključnega uporabnika niso določeni namestniki in da v primeru, ko je ključni uporabnik odsoten, končni uporabnik ne ve, na koga se lahko obrne. To težavo so delno rešili, ampak samo za incidente, ki jih je potrebno nujno rešiti, ker bi v nasprotnem primeru naredile veliko gospodarsko škodo. V tem primeru se podpis vseh sodelujočih v reševanju incidenta pridobi naknadno. Zaenkrat je sistem

birokratsko preveč zapleten in uporabnik porabi preveč časa s tem, da pridobi vse potrebne podpise in da gre lahko incident naprej v reševanje. Ker imajo v podjetju že uveden sistem elektronskega podpisovanja, bi lahko ta del procesa informatizirali in s tem končnim uporabnikom prihranil precej časa.

V sklepu svoje diplomske naloge bi dodal še to, da so slovenska podjetja v preteklosti namenjala premalo pozornosti informacijski tehnologiji in njeni organizaciji, vendar se stanje izboljšuje, saj vse več podjetij pridobiva ISO certifikate na teh področjih. Kljub vsemu bodo morala vložiti še veliko v sam razvoj in upravljanje z informacijsko tehnologijo, če bodo hotela konkurirati podjetjem v zahodni Evropi, saj so bili sami standardi ITIL razviti že v 80-ih letih, slovenska podjetja pa jih spoznavajo ter uvajajo šele v zadnjih desetih letih.

Literatura in viri

1. A Conceptual Approach to Safeguarding Integrity (2003). Objectivity and Independence throughout the Financial Reporting Chain. FEE, FEE Paper. najdeno avgusta 2006 na spletni strani www.fee.be.
2. A definition of service level management (2000). Najdeno junija 2006 na http://www.ics.de/lounge/infopack/white_paper/A_definition_of_Service_Level_Management.pdf.
3. Benedek D. (2002). Kako globoka je greznica? Delo, Sobotna priloga, Ljubljana, 16.11.2002
4. DiPiazza A. S. & Eccles G. R.(2002). Buildin Public Trust – The Future of Corporate Reporting. New York: John Wiley & Sons Inc.
5. Executive guide to IT Service Management (2000). Najdeno junija 2006 na http://www.ics.de/lounge/infopack/white_paper/Executive_Guide_to_IT_Service_Management.pdf.
6. Fox L. (2003). Enron – The rise and Fall. Hoboken, New Jersy: John Wilkey & Sons, Inc.
7. Fusaro Peter C. & Miller Ross M. (2003). What went wrong at Enron? Hoboken, New Jersy: John Wilkey & Sons, Inc.
8. Horvat T. (2002). Nova odkritja v WorldComu. Revizor, (9), 112-113.
9. Inciden Management (2007). Open Guide. Najdeno avgusta 2006 na spletni strani http://www.itlibrary.org/index.php?page=Incident_Management.
10. IT Infrastructure Library practices in small IT units. London: the Stationery Office Book (1998).
11. ITIL – The Key to Managing IT Services – Best Practises for Service Delivery (2003). version 2.0, OGC.
12. ITIL – The Key to Managing IT Services – Best Practises for Service Support (2003). version 2.0, OGC
13. Kim G. (2003). Sarbanes-Oxley, Fraud Prevention, and IMCA. Computer Fraud & Security, (9), 12-16.
14. Knez R.(1999). Osma direktiva Sveta EU. Podjetje in delo, revizija za gospodarsko, delovno in socialno, (3-4), 585-592.
15. Kranjc T. (2005). ITIL – upravljanje IT storitev, Organizacija, 38, (6), 302-308.
16. Mehle U. (2005). Sarbanes-Oxleyev zakon: vsebina in posledice v svetu in Evropski Uniji. Diplomsko delo. Ljubljana: Ekonomska fakulteta.
17. Miha E. (2007). Interna dokumentacija podjetja.
18. MOF Service Management Function Incident Management (2002). Najdeno junija 2006 na http://www.microsoft.com/technet/itsolutions/techguide/msm/smf/smfincmg.mspx.
19. Odar M. (2006). Metodika revizijskega previrjanja notranjih kontrol. Gradivo za izobraževanje. Ljubljana: Slovenski inštitut za revizijo.
20. Operations of IT systems (2006). Interna dokumentacija podjetja.

21. Pultorak D. (2002). An Introduction to IT Service Management: ITIL and MOF. DCM Magazin, (5), 14-17

22. Samec N. (2003). Sarbanes Oxley Act – Nova pravila Corporate Governance v ZDA. Pravna praksa, 22, (36/37), 14.
23. Section 404, Practical Guidence for Management , B.k. (2004), PricewaterhouseCoopers.
24. Service Support. London: The Stationery Office Books, 2001.
25. Schultz E. E. (2004). Sarbanes-Oxley – A Huge Boon to Information Security in the US. Computers & Security, (23), 353-354
26. Štefanič Pičman P. & Štefančič M. (2004). Sarbanes-Oxley Act – Vpliv zakonodaje na IT. Ljubljana: Genis d.o.o.
27. Uvodna predstavitev ITIL (2004). itSMF, različica 2.0. qSTC d.o.o. najdeno julija 2006 na spletni strani http://www.itsmf.si/Shared%20Documents/ITIL_pregled2.pdf .
28. Tartell J. (2001). Key ingridients of the IT Service Desk. Najdeno junija 2006 ma http://www.alternetics.com/articles/Key%20Ingredients%20of%20the%20IT%20Service%20Desk%20-%20Gartner.pdf.
29. The benefits of ITIL White Paper. Najdeno julija 2006 na http://www.pinkelephant.com/pdf/Benefits_of_ITIL.pdf
30. The ITIL Story. (2003). Najdeno julija 2007 na http://www.pinkelephant.com/pdf/The_ITIL_Story.pdf.
31. The Sarbanes-Oxley Act of 2002, Regulatory Compliance Series 1 of 6. B.k. (2005).

PRILOGE:

Priloga 1

Odkritje incidenta in 1. nivo podpore (koraki 1-3)

1: Analiza incidenta na 1. nivoju	Ko ključni uporabnik prejme klic od končnega uporabnika, ki je naletel ali odkril incident, poskuša od njega pridobiti čimveč informacij, da vidi, ali lahko on reši incident.
2: Rešitev incidenta na 1. nivoju in obveščanje o rešitvi	Če je mogoče, ključni uporabnik reši incident in o tem obvesti končnega uporabnika. V primeru, da ključni uporabnik rešuje incident več kot pol ure, mora zavesti nalog v Magic orodje, v nasprotnem primeru naloga ni potrebo zavesti.
3: Posredovanje incidenta	Če ključni uporabnik ne more rešiti incidenta, potem zbere vse potrebne informacije o incidentu in posreduje incident 2. nivoju podpore.

Klasifikacija incidenta, začetna podpora in dodelitev incidenta agentu (koraki 4-8)

4: Isti incident je že bil prijavljen in je v reševanju - obvestilo ključnemu uporabniku	V primeru, da je bil isti incident že prijavljen in je v reševanju, je ključni uporabnik ustrezno obveščen. Ali ustvarimo nov nalog in ga povežemo z že obstoječim incidentnim nalogom ali pa v obstoječi incidentni nalog napišemo, da mora biti nov ključni uporabnik ročno obveščen o napredku pri reševanju. V obeh primerih je ključni uporabnik obveščen. Ključni uporabnik dobi tudi kontaktne podatke za lastnika naloga in za ključnega uporabnika, ki je prvi prijavil incident.
5: Hitra ocena incidenta	Osebje SAP EE kompetenčnega centra na hitro oceni incident, če je potrebno, zbere še dodatne informacije, in če je mogoče, reši incident preko telefona. Oceniti mora tudi, ali gre dejansko za incident, in ne za nadgradnjo. Če gre za nadgradnjo, mora obvestiti ključnega uporabnika in začeti s procesom reševanja nadgradnje. V nasprotnem primeru odpre osebje SAP EE kompetenčnega centra nalog v orodju Magic in vpiše vse razpoložljive podatke.
6: Definiranje stopnje nujnosti oz. okvirnega datuma za rešitev incidenta	Ključni uporabnik in 2. nivo podpore skupaj določita stopnjo nujnosti in okvirni datum za rešitev incidenta. V primeru 1. in 2. stopnje urgentnosti morata biti obveščena tudi vodja SAP kompetenčnega centra EE, vodja oddelka za kakovost (ITQM). V primeru, da se ključni uporabnik in agent 2. nivoja ne moreta dogovoriti o stopnji nujnosti, mora posredovati vodja SAP kompetenčnega centra EE.

7: Zapis naloga	Osebje SAP EE kompetenčnega centra identificira določeno skupino na 2. nivoju podpore, ji dodeli lastništvo nad incidentom in shrani nalog. Nato začne teči reakcijski čas in incident postavi v status OPEN. Nalog je avtomatično posredovan skupini, poleg tega se posreduje tudi obvestilo ključnemu uporabniku. V primeru incidentov 1. in 2. stopnje urgentnosti mora ključni uporabnik obvestiti skupino preko telefona, da se zagotovi kratek reakcijski čas.
8: Dodelitev naloga	Član določene skupine dodeli nalog samemu sebi in s tem postane tako lastnik naloga kot tudi prvi pooblaščenec naloga, zažene čas za rešitev in spremeni status v WIP (delo v teku). Obvestilo o vseh spremembah se avtomatsko pošlje ključnemu uporabniku. Lastnik naloga lahko dodeli nalog tudi drugim članom skupine, vendar še vedno ostane lastnik naloga.

Diagnoza incidenta in definiranje rešitve (koraki 9-12)

9: Diagnoza incidenta	Trenutni pooblaščenec naloga naredi diagnozo incidenta.
10: Definiranje rešitve	Trenutni pooblaščenec naloga definira rešitev za osnovni problem incidenta.
11: Notranja premestitev incidenta	Če trenutni pooblaščenec naloga ne more identificirati osnovnega problema ali najti rešitve zanj (recimo zato, ker je problem del drugega modula), a je prepričan da lahko interni know-how reši ta incident, potem incident dodeli drugemu agentu znotraj podjetja v 2. ali 3. nivoju podpore.
12: Dodelitev incidenta zunanjemu izvajalcu	V primeru, da je bil incident v reševanje že dodeljen 3. nivoju podpore in trenutni pooblaščenec misli, da interni know-how ne more rešiti incidenta, ga posreduje primernemu zunanjemu izvajalcu. Kljub temu se vloga lastnika in pooblaščenca naloga ohrani.

Rešitev in zaprtje incidenta (koraki 13-18)

Zahteva za spremembo ni potrebna

13: Rešitev	Trenutni pooblaščenec reši in dokumentira rešitev v nalogu. Po realizaciji rešitve obvesti uporabnika.
14: Obvestilo o rešitvi incidenta in zaprtje naloga	Lastnik spremeni status naloga na CLOSED (zaprto). Ključni uporabnik je avtomatično obveščen o zaprtju naloga in od lastnika dobi vse potrebne informacije in pojasnila.

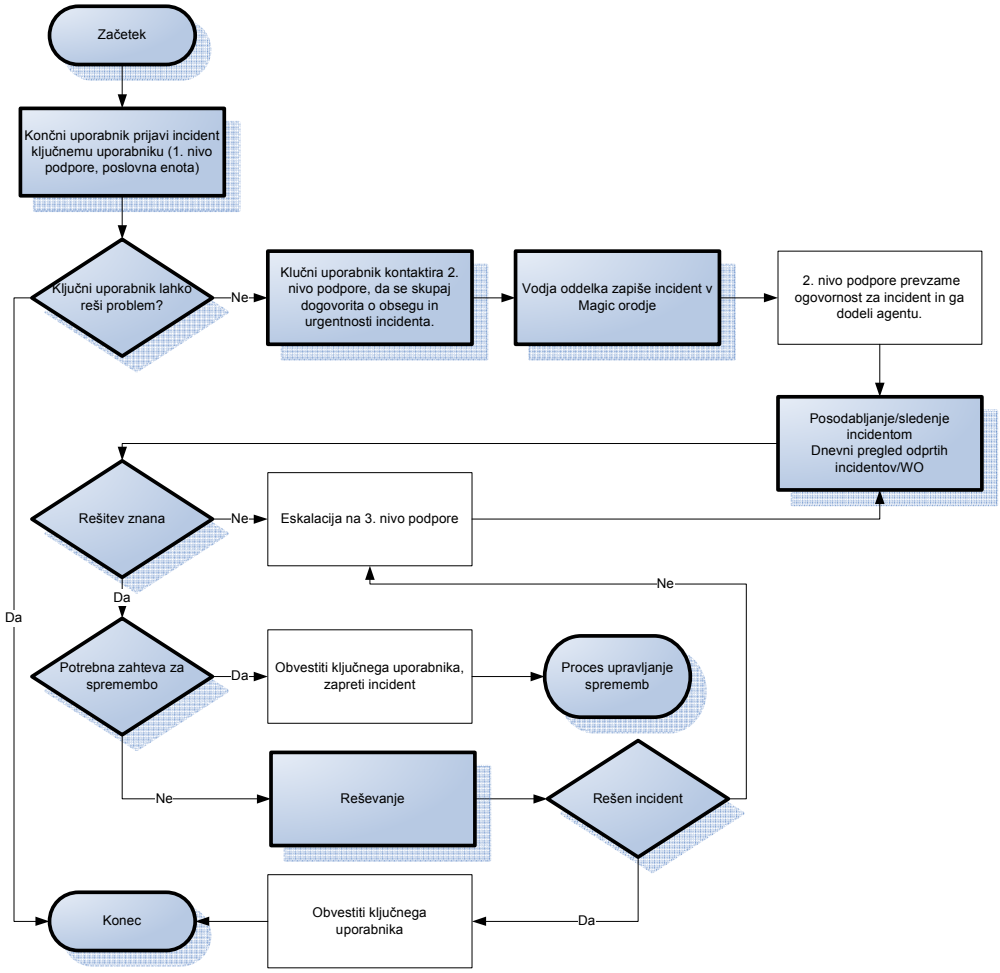
	V primeru incidenta, ki ima stopnjo urgentnosti 1 ali 2, mora lastnik naloga obvestiti tudi vodjo SAP kompetenčnega centra EE.
15: Potrditev ključnega uporabnika	Ključni uporabnik potrdi rešitev incidenta.
16: Ponovno odprtje naloga	Če ključni uporabnik ni zadovoljen z rešitvijo, je potrebno nalog ponovno odpreti. Potrebna je nadaljnja komunikacija med lastnikom in ključnim uporabnikom, da ugotovita razlog za ponovno odprtje. Za ponoven zagon procesa je odgovoren lastnik naloga.

Zahteva za spremembo je potrebna

17: Proces upravljanja sprememb	Če je zahteva za spremembo potrebna, potem moramo začeti proces upravljanja sprememb, kot nam narekuje lokalni splošni postopek. Proces upravljanja sprememb je povezan z incidentom preko vpisane številke zahteve za spremembo v naloga. Pooblaščenec naloga je zadolžen za posodabljanje naloga in obveščanje ključnega uporabnika o napredku. Če čas reševanja preseže dogovorjeni čas za rešitev incidenta, lahko lastnik naloga spremeni status naloga v HOLD in/ali se z uporabnikom dogovori za novi čas razrešitve s ključnim uporabnikom ter ga nato spremeni v nalogu.
18: Zaprtje naloga	Lastnik spremeni status naloga na CLOSED (zaprto). Ključni uporabnik je avtomatično obveščen o zaprtju naloga. Lastnik ga oskrbi z vsemi potrebnimi informacijami in pojasnili. V primeru incidenta, ki ima stopnjo urgentnosti 1 ali 2, mora lastnik naloga obvestiti tudi vodjo SAP kompetenčnega centra EE.

Priloga 2

Prikazuje proces upravljanja z incidenti v sistemu SAP v farmacevtskem podjetju.



Priloga 3

Prikazuje proces upravljanja s tehničnimi incidenti v farmacevtskem podjetju.