UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

CELOVITA OCENA SKLADNOSTI RAČUNALNIŠKIH SISTEMOV V PODJETJU Z VIDIKA INŠPEKCIJE AMERIŠKE AGENCIJE ZA PREHRANO IN ZDRAVILA

Ljubljana, april 2003 Darko Robar

POVZETEK

V pričujočem delu je s pomočjo večparametrskega odločitvenega modela prikazana celovita ocena skladnosti računalniških sistemov v farmacevtskem podjetju z zornega kota inšpekcije ameriške Agencije za prehrano in zdravila.

Ob inšpekciji kot tudi ob oddaji registracijskega dosjeja je ključna pravilnost podatkov in zaupanje ameriške Agencije za prehrano in zdravila v verodostojnost predanih dokazil. Sistem zagotavljanja kakovosti se potrjuje z internimi presojami in ekspertnimi inšpekcijami, npr. ameriške (FDA).

Agencija za prehrano in zdravila je uspela z aktivnim uvajanjem zakona na področju elektronskih zapisov in elektronskih podpisov, t. i. 21 CFR Part 11, postaviti jasne zahteve in smernice za uporabo elektronskih zapisov ter elektronskih podpisov v farmacevtski industriji. S tem pa so dobili tudi pravno veljavo. Informacijska in računalniška tehnologija je torej postala pomemben del v razvoju in izdelavi zdravila.

S pregledno odločitveno analizo, jasnim ozadjem procesov računalniških sistemov na področju elektronskih zapisov in podpisov ter obvladovanjem ostalih v nalogi omenjenih potrebnih znanj, lahko farmacevtsko podjetje bolje zagotavlja kakovost. Vse to omogoča boljšo pripravo na inšpekcijo, manj je stresnih položajev in zato posledično delovanje podjetja uspešnejše.

Ključne besede:

kakovost
elektronski zapisi
elektronski podpisi
inšpekcija ameriške Agencije za prehrano in zdravila
večparametrski odločitveni model

SUMMARY

In this work, a full assessment of the conformity of the computer systems in the pharmaceutical company from the point of view of the American Food and Drug Agency (FDA) inspection authorities by use of a multi-parameter decision-making module is presented.

On the occasion of an inspection visit as well as at the submission of the registration file the correctness of the data and confidence of the FDA inspection authorities in the reliability of the evidences submitted is of key significance. The system of quality assurance shall thus be previously approved by internal audits and expert inspections.

By the introduction of the act on the electronic records and signatures, the so called 21 CFR Part 11, the American Food and Drug Agency has succeeded to establish clear requirements and directions for use of the electronic records and signatures in the pharmaceutical industry which have thus become legally valid. As a result, the information and computer technology has gained even more importance in the development and manufacture of drugs.

By a clear decision-making analysis and clear background of use of computer systems in the field of electronic records and signatures as well as by management of other necessary knowledge mentioned in this work the pharmaceutical company may better assure quality. In addition, it may be better prepared for the inspection visits, which reduces stress situations, and consequentially, the operation of the company may be improved, too.

Key words:

Quality
Electronic records
Electronic signatures
The U.S. FDA inspection authorities
Multi-parameter decision-making model

KAZALO

1. Uvod

1.1. Opredelitev problema

V poslovnem svetu že desetletja veljavno pravilo, da »velike ribe pojedo majhne ribe«, v dobi naprednih tehnologij in globalnega trga izgublja svoj pomen. Vedenjski vzorec se je začel spreminjati: na trgu postajajo uspešna tista podjetja, ki so sposobna informacijsko tehnologijo uspešno uporabiti v svojo korist.

Čas, ki je potreben za zajemanje in obdelavo podatkov, je vse krajši. Velika hitrost procesiranja informacij omogoča podjetju hitrejši odziv na potrebe trga in zveča sposobnost učinkovitega prilagajanja izzivom in spremembam okolja. Sporočilo, ki ga prinaša napredek, lahko strnemo v načelo: »hitre ribe pojedo počasnejše ribe«.

Farmacevtska industrija, ki izdeluje zdravila in medicinske pripomočke, pri tem ni izjema. Tržne zakonitosti veljajo povsod. Čeprav tudi farmacevtska podjetja veliko pozornosti namenjajo merjenju donosnosti, so v zadregi, ko iščejo razumno mero v zagotavljanju regulatorne skladnosti in tveganja pri uvajanju elektronskih tehnologij. Odzivi podjetja so lahko naslednji (PricewatherhouseCoopers, Noferi, B. l., str. 63):

1. *Vzdržujejo »status quo«* in ne naredijo ničesar. Ta podjetja še vedno delajo z ročnimi postopki ali hibridnimi sistemi[1].

2. *Zgrabijo priložnost*. Nadgradijo obstoječe sisteme, vendar le, če je potrebno.

3. *»Potujejo s tokom«*. Ta podjetja opredelijo posamezne obstoječe sisteme kot »zapuščino« in sprejmejo različne samostojne rešitve.

4. *Svetovna klasa.* Ta podjetja ohranjajo vse pomembne vire, da ostanejo v samem vrhu tehnologije in sprejemajo izzive, ki jih prinašajo nenehne spremembe.

Zamenjava običajnih proizvodnih in poslovnih procesov, ki potekajo na osnovi ročnih postopkov ali papirne dokumentacije, z elektronskimi mediji prinaša mnoge pasti.
Pri uvajanju novih tehnologij je nujno, da poleg organizacijske strategije fizičnih sprememb, kot so informacijski sistemi in informacijske tehnologije, obstaja tudi druga vrsta sprememb – to so miselne spremembe, npr. norme, vzorci obnašanja, vrednote; torej vse, kar označujemo z organizacijsko kulturo. (Rozman, Kovač, Koletnik, 1993, str. 169)

Govorimo o dveh razsežnostih. (Rozman, Kovač, Koletnik, 1993, str.169-170) Prvo predstavlja časovni horizont sprememb in lahko traja več let, druga je povezana z vplivno skupino, ki organizacijsko kulturo oblikuje in ima nanjo največji vpliv. V mislih nimamo samo vodstva podjetja z njegovimi pogledi, usmeritvami in strategijo, ampak tudi veljavno regulativo z vsemi njenimi vzvodi v obliki postavljenih smernic, pravil, inšpekcij, sankcioniranja itd.
V farmacevtski industriji ima vlogo regulatorja za ameriški trg ameriška Agencija za prehrano in zdravila (FDA[2]).

---

[1] hibridni sistemi – so delno avtomatizirani sistemi, ki vsebujejo tako elektronske, kot ročne zapise. (Chapman, Winter, 2002, str. 51)

[2] FDA - angl. ***F**ood and **D**rug **A**dministration*

Ta skrbi za zaščito prebivalstva pred škodljivo, oporečno, okuženo ali nekakovostno hrano, zdravili ali kozmetiko in predpisuje potrebne načine označevanja in embaliranja izdelkov. S svojim delovanjem na različnih področjih postavlja temeljna pravila za upravljanje in zagotavljanje sistema kakovosti v podjetjih.

Podjetja, ki želijo prodajati izdelke na zahtevni ameriški trg, morajo pridobiti in ohranjati polno zaupanje agencije, da je njihovo delovanje skladno z regulativo. Sistem zagotavljanja kakovosti se potrjuje z internimi presojami in ekspertnimi inšpekcijami, npr. FDA. Tako ob inšpekciji kot tudi ob oddaji registracijskega dosjeja je ključna pravilnost podatkov in zaupanje FDA v verodostojnost predanih dokazil. Rezultati teh aktivnosti so za farmacevtsko podjetje odločilni in lahko nagradijo ali zapečatijo usodo večletnih razvojnih prizadevanj. FDA je tista, ki izda dovoljenje za promet z zdravilom na ameriškem trgu ali pa ne.

Na pobudo in ob sodelovanju farmacevtske industrije je FDA začela aktivno uvajati smernice na področju elektronskih zapisov in elektronskih podpisov ter s tem farmacevtskim podjetjem omogočila široko uporabo informacijske tehnologije, tako pri pripravi registracijskih dosjejev kot tudi v vseh fazah načrtovanja, razvoja, izdelave in kontrole zdravil. Te smernice so znane pod imenom 21 CFR Part 11[3]. (Code of Federal Regulations, 1997, str. 1)

1.2. Namen in cilj dela

Namen magistrskega dela je predstaviti in zaokrožiti celotno problematiko, s katero se farmacevtsko podjetje srečuje pri doseganju skladnosti računalniških sistemov z regulativo 21 CFR Part 11.

Cilj dela je izdelati večparametrski odločitveni model, s katerim bomo celovito ocenili obvladovanje sistema regulatorne skladnosti farmacevtskega podjetja, ki je predmet inšpekcij FDA.

Prikazati želimo regulativo 21 CFR Part 11, ki opredeljuje elektronske zapise in elektronske podpise kot del modela validacije računalniških sistemov. Z elementi modela bomo določili možne vire odstopov, ki bodisi sami bodisi zaradi medsebojne odvisnosti zvečujejo ali zmanjšujejo varnost in zanesljivost informacijskih sistemov ter posledično verjetnost, da bo inšpekcija potrdila regulatorno skladnost.

Na osnovi odločitvenega drevesa bomo določili profil atributov tveganja za podjetje ob poteku inšpekcije. S pomočjo te ocene želimo opredeliti priložnosti in nevarnosti, ki prežijo na podjetje, ko postavlja sistem zagotavljanja kakovosti in zagotavljanja regulatorne skladnosti informacijskih sistemov s poudarkom na elektronske zapise in podpise. 21 CFR Part 11 obravnavamo tudi kot metodo za migracijo znanja, kajti vizija in cilj sodobnega podjetja je, da združi vse koristne podatke in različne informacije v centralno shrambo znanja (repozitorij[4]), ki bo dostopen vsem upravičenim uporabnikom.

Z odločitvenim modelom bomo postavili jasno platformo, ki bo podjetju omogočala:

---

[3] 21 CFR Part 11- angl. ***21 C**ode of **F**ederal **R**egulations **Part 11***

[4] repozitorij – Opisuje podatke v podatkovni bazi. To so metapodatki ali podatki o podatkih.

- doseganje skladnosti s predpisanimi zahtevami FDA za elektronske zapise in elektronske podpise (21 CFR Part 11) in drugimi zahtevami za elektronsko poslovanje,

- hranjenje elektronskih zapisov v skladu z dobro klinično prakso (*GCP*[5]), dobro laboratorijsko prakso (*GLP*[6]) in dobro proizvodno prakso (*GMP*[7]).

Takšen zaokrožen pristop bo omogočil preglednejše razumevanje celotnega sistema regulatorne skladnosti. Podjetje bo na osnovi novih spoznanj in izvedenih analiz lahko oblikovalo učinkovito strategijo za zagotavljanje kakovosti na področju elektronskih tehnologij. Inšpekcije bodo posledično postale manj stresne, uporabljene rešitve skladnejše, podjetje pa bo naredilo nov korak na poti k odličnosti.

1.3. Metode raziskovanja in vsebina poglavij

Za izdelavo odločitvenega modela je potrebno razumevanje pravil regulatorne skladnosti, celotnega procesa poteka inšpekcije, posameznih elementov sistema podjetja in poznavanje vlog ključnih dejavnikov. Poznati moramo njihovo vplivanje in medsebojne interakcije. Za boljše razumevanje tematike bomo uporabili različno tematsko literaturo, vključili strokovna mnenja in lastna spoznanja, ki jih je avtor magistrskega dela pridobil pri dosedanjem delu.

V magistrskem delu se bomo ukvarjali s pojmom zagotavljanja regulatorne skladnosti informacijskega sistema. Napaka, po terminologiji zagotavljanja kakovosti jo obravnavamo kot odstop, pomeni neskladnost sistema. Kot okvir za določitev možnih virov odstopov, ki bodo pozneje osnovni nosilci raziskave, bomo uporabili metodo DEPOSE[8]. Pri tej metodi za analizo odstopov v kompleksnih sistemih uporabljamo sistemske komponente: načrtovanje, naprave, postopke, operaterje, materiale, okolje. (Perrow, 1984, str. 77)

Z razumevanjem narave napak in pomena tehnologije ter z analizo različnih odstopov želimo pojasniti vlogo posameznih sodelujočih nosilcev ter vpliv ljudi (delež človeškega faktorja) na sistem kakovosti podjetja. Sisteme bomo obravnavali kot niz medsebojno delujočih odvisnih elementov, ki se združujejo z namenom doseganja skupnega cilja, to je doseči regulatorno skladnost in uspešno prestati inšpekcijo.

Delo je razdeljeno na dve tematski področji, ki ju bomo v obravnavi vsebinsko dopolnjevali in nadgrajevali.

V prvem delu bomo predstavili **zahteve regulative** za elektronske zapise in elektronske podpise v okviru validacije računalniških sistemov. Za razumevanje vseh dejavnikov, ki vplivajo na potek inšpekcije, bomo izdelali model (21 CFR Part 11 kot del validacije računalniških sistemov), v katerem bodo prikazani vsi osnovni elementi sistema z medsebojnimi povezavami.

---

5 GCP - angl. ***G**ood **C**linical **P**ractice*

6 GLP - angl. ***G**ood **L**aboratory **P**ractice*

7 GMP - angl. **G**ood **M**anufacturing **P**ractice

8 DEPOSE- angl. ***D**esign, **E**quipment, **P**rocedures, **O**perators, **S**upplies in materials, **E**nvironment*

Uvedli bomo pojem »dobre prakse elektronskega arhiviranja« v podjetju. (Dollar, 2000, str. 25-26) Njen cilj je ohraniti zasebnost, avtentičnost in verodostojnost informacij ter preprečiti zanikanje izvedenih postopkov, ki so bistveni za ohranitev elektronskih zapisov v njihovem življenjskem ciklu.

V drugem delu bomo pojasnili **proces odločanja**. Z uporabo ekspertnega sistema za večparametrsko odločanje bomo izdelali odločitveno drevo za ocenitev ravni kakovosti celovitega obvladovanja informacijskih sistemov.

Z računalniško podporo odločanju v okviru programskega paketa DEXi[9] bomo izdelali kvalitativni hierarhični odločitveni model. (Rajkovič, Bohanc, Zupan, 2000, str. 2) Za identifikacijo kriterijev in definiranje funkcij odvisnosti bomo uporabili spoznanja in zakonitosti izdelanega modela.

Obravnavali bomo pojem inšpekcije, razčlenili različne vzroke zanjo ter pojasnili, kako naj se podjetje pripravi, da bo inšpekcija potekala uspešno.

Prednosti, slabosti, priložnosti in nevarnosti ekspertnega sistema bomo ovrednotili s pomočjo analize SWOT[10].

Uporabili bomo izrazoslovje, ki je značilno za farmacevtsko industrijo. Začetni razlagi izrazoslovja sledi uporaba brez podrobnih obrazložitev.

V uvodu smo podali opredelitev problema, cilje in namen raziskave, odločitvene skupine ter metode raziskovalnega dela za postavitev 21 CFR Part 11 kot dela modela validacije računalniških sistemov preko sistema večkriterijskega odločanja.

V naslednjem poglavju obravnavamo samo naravo napake oziroma odstopa, njeno razumevanje v kontekstu skritih in aktivnih napak ter predstavimo metodo za določitev možnih virov odstopov. Sledi podroben opis standardnih (odprti in zaprti sistemi, zagotavljanje varnosti, zgodovina dogodkov in uporaba elektronskih podpisov) in nestandardnih elementov modela (spremembe in njihov pomen, neskladnost sistemov, tehnologija, procesi, ljudje in računalniški ter informacijski sistemi podjetja).

Predstavimo ohranitev zapisa v smislu priporočil dobre informacijske prakse (GISP[11]) in popišemo osem načel arhiviranja. Poglavje končamo z opisom življenjskega cikla zapisov, ki ga projiciramo na življenjski cikel sistema.

V tretjem poglavju obravnavamo teorijo odločanja. Seznanimo se s procesom odločanja in temeljnim pristopom večparametrskega odločitvenega modela. Razčlenimo posamezne faze odločitvenega modela (identifikacija problema, identifikacija kriterijev, definicija funkcij koristnosti, opis variant, vrednotenje in analiza variant).
V naslednjem poglavju predstavimo računalniški ekspertni sistem za večparametrsko odločanje DEXi in ga uporabimo pri postopku načrtovanja odločitvenega drevesa.

---

9 DEXi - angl. ***De**cision **E**xpert*

10 SWOT - angl. ***S**trenhgts, **W**eaknesses, **O**pportunitties, **T**hreats*

11 GISP - angl. ***G**ood **I**nformation **S**ystem **P**ractice*

V petem poglavju prikažemo motive in cilje inšpekcije ter opredelimo njeno vlogo v okviru zakona 21 CFR Part 11. Predstavimo definicijo uspešne inšpekcije. Preverjamo potrebne aktivnosti za pripravo na inšpekcijo: vodenje, vloga inšpektorja, upravljanje z informacijami oziroma znanjem.

V šestem poglavju postavimo odločitveno drevo z naslednjimi osnovnimi kriteriji: 21 CFR Part 11, skrbnik sistema, upravljanje kakovosti, sistem sprememb, arhiv. V nadaljevanju kriterije razgradimo v vsebinske podskupine, upoštevamo njihove medsebojne odvisnosti ter določimo zaloge vrednosti kriterijev za naš odločitveni problem.

V zaključku prikažemo ovrednotenje ekspertnega sistema s pomočjo analize SWOT ter vzdrževanje in nadgradnjo ekspertnega sistema.

2. Uvajanje novih informacijskih tehnologij v farmacevtski industriji

V nezadržno razvijajočih se družbah se v zadnjih letih vedno bolj izraža težnja po novih načinih delovanja. Farmacevtskega okolja si brez računalniške in informacijske tehnologije praktično ni več mogoče predstavljati. Nove tehnologije se uveljavljajo in vstopajo v vse faze razvoja, proizvodnje in distribucije zdravila.

Razvoj zdravila se začne z odločitvijo raziskovalnega laboratorija, katera bolezen bo predmet raziskave; pravimo, da določijo tarčno bolezen. Raziskovalci morajo na tej stopnji zbrati vse do tedaj znane podatke o obravnavani bolezni in do tedaj znanih načinih zdravljenja. Pri tem ima informatika velik pomen. Informacijska tehnologija v tej stopnji raziskave zelo olajša zbiranje podatkov iz različnih virov (medicinske ustanove, medicinske revije, lastni podatki, sorodne institucije, podjetja …) in področij znanosti v neko pregledno celoto. Pomembno vlogo ima internet, saj omogoča dostop do številnih virov in njihovih baz podatkov. Z združitvijo teh podatkov, ki so danes večinoma že dostopni v elektronski obliki, dobi raziskovalec pregled nad do tedaj znanimi dejstvi. Informacijska tehnologija olajša zbiranje podatkov, njihovo urejanje pa je hitrejše, lažje in preglednejše.

Naslednji korak pri odkrivanju zdravil je oblikovanje molekul, ki bi bile glede na zbrane podatke možne zdravilne učinkovine za obravnavano bolezen. Lastnosti morebitne učinkovine določimo na osnovi zbranih podatkov ali lastnih raziskav. Temu procesu pravimo postavljanje modelov. Za ta postopek imajo nekateri laboratoriji že razvita informacijska orodja, s katerimi na podlagi zbranih podatkov predvidijo oziroma simulirajo učinkovitost predvidene učinkovine. Takim razvojnim sistemom pravimo: oblikovanje zdravila s pomočjo računalnika (*CADD*[12]). Podjetje se tako lahko izogne mnogim do sedaj potrebnim eksperimentom, saj s pomočjo računalnika lahko z veliko verjetnostjo predvidi obliko molekule, njene fizikalne in kemijske lastnosti ter s tem prihrani veliko časa in denarja, kar je v današnji družbi ključni dejavnik.

Tudi v nadaljnjih razvojnih postopkih, pri uvajanju in proizvodnji zdravil farmacevtsko podjetje v polni meri uporablja računalniško in informacijsko tehnologijo, saj spremlja vsak avtomatizirani proces tako pri analizi sestavin, pripravi učinkovin ali pomožnih

---

12 CADD - angl. ***C**omputer-**A**ided **D**rug **D**esign*

materialov kot pri skladiščenju, logistiki in v sklepni fazi pri končni izdelavi farmacevtskih oblik.

Vsi analitski rezultati, dobljeni v kontrolnih laboratorijih, podatki, zbrani v proizvodnih enotah, ter podatki iz sistemov zagotavljanja kakovosti in kontrole kakovosti se zbirajo pod okriljem določenih informacijskih otokov, ki jih preko notranjega omrežja (intranet) ali preko svetovnega spleta (internet) povežemo z drugimi proizvodnimi in poslovnimi sistemi. Statistične obdelave, analize in sinteze podatkov, odločitveni modeli ter orodja upravljanja so v današnjem času praktično že v domeni računalnikov.

Pri uporabi elektronskih tehnologij želi farmacevtska industrija nesporno večjo učinkovitost dela na mnogih področjih podpreti z zadostno pravno oziroma regulatorno zanesljivostjo. Na ta način lahko že vnaprej omogoči varno in predvidljivo okolje delovanja.

Zadnjih nekaj let postaja vse bolj očitno, da se oblikujeta dve področji elektronskega poslovanja: **zaprto** elektronsko poslovanje in **odprto** elektronsko okolje. Obe imata poleg nekaterih skupnih lastnosti tudi precej različnih tehnoloških in pravnih problemov. Zastavlja se vprašanje, ali lahko vse vrste elektronskega poslovanja obravnavamo z nekimi skupnimi merili in ali lahko postavimo splošna pravila, ki bi veljala za vse možne primere. (Toplišek, 1996, str. 291)

Ugotavljamo, da v svetu na splošno še ne obstaja celovit pristop k **pravnemu** urejanju elektronskega poslovanja, kar velja še zlasti za elektronski podpis. V državah anglosaškega prava, še zlasti v tistih iz ZDA, velja predvsem pragmatičnost, tj. reševanje konkretnih primerov. Pogosto srečujemo merilo »razumnega tveganja«, zato so obravnave včasih nesistematične in zanemarjajo univerzalnost problemov poslovanja. (Toplišek, 1996, str. 291)

Ameriška Agencija za prehrano in zdravila je uspela z aktivnim uvajanjem zakona (nedvoumnih in celovitih pravil) na področju elektronskih zapisov in elektronskih podpisov, t. i. 21 CFR Part 11 postaviti jasne smernice in zahteve za uporabo elektronskih zapisov in elektronskih podpisov v farmacevtski industriji, ki so tako dobili pravno veljavo. Informacijska in računalniška tehnologija je torej postala pomemben del v razvoju in izdelavi zdravila, saj nam olajša delo na praktično vseh ravneh.

Seveda pa je pri tem potrebno opozoriti, da bodo lahko farmacevtska podjetja v »novi ekonomiji« konkurenčne samo takrat, ko (Stemberger, 2003, str. 1):
- se bodo sposobne učiti hitreje od svojih konkurentov,
- se bodo znala bolj kakovostno in hitreje odločati,
- se bodo znala hitreje in bolje prilagoditi spremembam ter
- bodo sposobna razvijati projekte hitreje in učinkoviteje kot pa njihovi konkurenti.

Poudarek pri ključnih elementih konkurenčne prednosti je torej na hitrosti in odločanju. Vendar pa bodo morala biti podjetja pri odločanju pazljiva, saj je odločanje v hitro se spreminjajočem okolju vedno bolj kombinacija pravilnega vira informacij, tipa in ustreznega izbora informacij kot tudi izkušenj in intuicije.

3. "21 CFR Part 11" kot model validacije računalniških sistemov

3.1. Definicije in terminologija

Dobra proizvodna praksa računalniški sistemov (GAMP[13]) je del procesa za obvladovanje kakovosti v farmacevtskem podjetju, ki zagotavlja dosledno izdelavo in kontrolo računalniškega sistema po standardih za kakovost.

Dobra proizvodna praksa (GMP) je del procesa za doseganje kakovosti, ki zagotavlja dosledno izdelavo in kontrolo izdelka po standardih za kakovost ter ustreznost namenu uporabe, kot zahtevata dovoljenje za promet in specifikacija izdelka. (Slovensko farmacevtsko društvo, 1993, 94, str. 17)

Dobre prakse: Sistem »dobrih praks« je razvejana zbirka predpisov in priporočil. Izdajo jih predstavniki izvršnih oblasti. Izvajanje predpisov je naloga industrije in preostalih subjektov na trgu. Nadzor opravljajo inšpekcije, ki so lahko nacionalne (ameriška FDA) ali misije posameznih mednarodnih združenj (npr. PIC). (Slovensko farmacevtsko društvo, 1993, 94, str. 17)

e-CRF[14] je pregleden elektronski zapis, načrtovan za zapis informacij, ki so zahtevane za protokole kliničnih poskusov. Z njimi naročniku poročamo o poteku in izsledkih posameznih poskusov. (Guidance for Industry, 1994, str. 3)

Kvalifikacija načrtovanja (DQ[15]) je dokumentiran dokaz, da je predviden obrat, oprema ali sistem primeren za načrtovan namen.

Kvalifikacija montaže (IQ[16]) je dokumentiran dokaz, da je predviden obrat, oprema ali sistem montiran, instaliran in povezan v skladu s specifikacijami.

Kvalifikacija delovanja (OQ[17]) je dokumentiran dokaz, da obrat, oprema ali sistem, kot je izdelan ali spremenjen, deluje pričakovano ves čas predvidenega obratovanja.

Kvalifikacija delovanja (PQ[18]) je dokumentiran dokaz, da glede na potrjen postopek procesa in specifikacijo produkt, obrat, oprema ali sistem, kot je izdelan ali spremenjen, lahko deluje učinkovito in ponovljivo.

Opozorilno pismo oblike 483 (Form 483) predstavlja pripombe inšpekcije. Inšpektor FDA napiše pripombe o stanju in postopkih, ki so predmet preiskave med inšpekcijo podjetja. (Joseph X. Phillips, 2001, str. 1)

---

13 GAMP - angl. ***G**ood **A**utomated **M**anufacturing **P**ractice*

14 e-CRF - angl. ***E**lectronic **C**ase **R**eport **F**orm*

15 DQ - angl. **D***esign* **Q***ualification*

16 IQ - angl. ***I**nstallation **Q**ualification*

17 OQ - angl. ***O**perational **Q**ualification*

18 OQ - angl. ***P**rocess **Q**ualification*

Prevzemni testi pri proizvajalcu (**FAT**[19]) so postopki, ki jih izvede naročnik pri prevzemu naročenega izdelka s ciljem, da se prepriča, da bo resnično dobil izdelek, ki ga je plačal. (Matthev, 2000, str. 8)

Protokol validacije je dokument, ki definira izvedbo kvalifikacijskih in validacijskih aktivnosti, s katerimi potrjujemo ustreznost opreme, sistemov in postopkov. Definirati mora odgovornosti in časovni potek validacijskih aktivnosti.

Računalniški sistemi so računalniške aparature za sistematičen vnos podatkov, elektronsko obdelavo in izhod informacij za potrebe zapisa, poročanja ali avtomatske kontrole. (Slovensko farmacevtsko društvo, 1993. 94 str. 11)

Retrospektivna validacija je validacija postopka za izdelek (sistem), ki je že v prodaji (uporabi) in ki temelji na zbranih podatkih proizvodnje, preskušanja in nadzora. (Merck, 2001, str. 43)

Standardni operativni postopki (SOPs[20]) so pisni dokumenti, ki predpisujejo natančne postopke in faze delovanja, ki jih je treba upoštevati, da bi dokončali določeno nalogo. Pristojni organi zahtevajo SOP-je za praktično vsak vidik proizvodnje, nadzora in preskušanja farmacevtskih izdelkov. Eden od SOP-jev naj opiše izdajanje in nadzor SOP-jev. (Merck, 2001, str. 48)

Tekoče dobre proizvodne prakse (*cGMPs*[21]) so predpisi, ki so bili uzakonjeni v Zveznem zakonu ZDA (21 CFR 210-211), da opišejo minimalni standard, ki ga je treba izpolniti v proizvodnji zdravil in pripomočkov za ljudi in živali. (Merck, 2001, str. 13)

Validacija je postopek dokazovanja, s katerim v skladu z načeli dobre proizvodne prakse preverjamo katerikoli postopek, proces, opremo, snov, dejavnost in sistem, da bi ugotovili, ali dejansko vodi do pričakovanih rezultatov. (Slovensko farmacevtsko društvo, 1993, 94, str. 13)

Zagotavljanje kakovosti je element v sistemu vodenja kakovosti, ki nadzoruje skladnost z zakonsko predpisanimi uporabami in lokalnimi predpisi, ravnanje v skladu s proizvodnim standardom, uporabo postopkov za nadzor kakovosti ter reševanje pritožb. (Merck, 2001, str. 58)

---

19 FAT - angL. **F**actory **A**cceptance **T**esting

20 SOPs - angl. **S**tandard **O**perating **P**rocedure**s**

21 cGMPs **-** *angl.* ***c****urrent* ***G****ood* ***M****anufacturing* ***P****ractice****s***

3.2. Napake

Napako v kateremkoli delu farmacevtske industrije, ki povzroči neskladnost sistema, obravnavamo kot odstop. V uvodnem delu želimo odgovoriti na vprašanje, zakaj do napak prihaja, razumeti njihovo naravo in njihovo ključno vlogo pri zagotavljanju skladnosti sistema.

3.2.1. Odstop

Ko se odstop pojavi, je skupna začetna reakcija iskanje krivca. Vendar je narava odstopa običajno kompleksnejša in posledica vplivanja mnogih sodelujočih faktorjev. Z obtoževanjem posameznikov teh faktorjev ne spremenimo. Obstaja velika verjetnost, da se bo enak odstop čez čas ponovil. Da bi odpravili odstope in izboljšali varnost sistemov, je nujno vzpostaviti sistemski pristop, ki nam bo omogočil spremembo pogojev, ki povzročajo odstope. Problem ni slabo osebje, ampak sistem, ki ni zanesljiv in preverjen. Primarni poudarek ni na tem, da se »znebimo slabih jabolk« ali posameznikov, ki imajo niz slabih sposobnosti, ampak da s sistemskim pristopom izvedemo najširše izboljšave. Sprejmemo ukrepe, ki onemogočijo pojavitev odstopa tudi v primeru »slabih jabolk«.

3.2.2. Zakaj se dogajajo odstopi?

Posledice odstopov v farmacevtski industriji so na prvi pogled manj vidne, vendar nič manj pomembne kot tiste v drugih industrijah. Odstopi, ki jih obravnavamo, so tudi določena oblika informacij o samih sistemih podjetja (npr. sistemi nadzora, informacijski sistemi, sistemi zagotavljanja kakovosti itd.). Predstavljajo področja, v katerih sistem ne deluje; posledica tega je njegova neskladnost s postavljenimi zahtevami in pričakovanji.

Posamezni elementi se združujejo v manjše sisteme, ti pa pripadajo večjim, sestavljenim sistemom, na primer: procedura je del programa računalniškega sistema, ta je del sistema informacijske tehnologije in skupaj je del večjega sistema zagotavljanja skladnosti z regulativo FDA. Takšne kompleksne sisteme težko analiziramo in razumemo v celoti, predvsem zaradi njihovih spreminjajočih se oblik in obsegov.

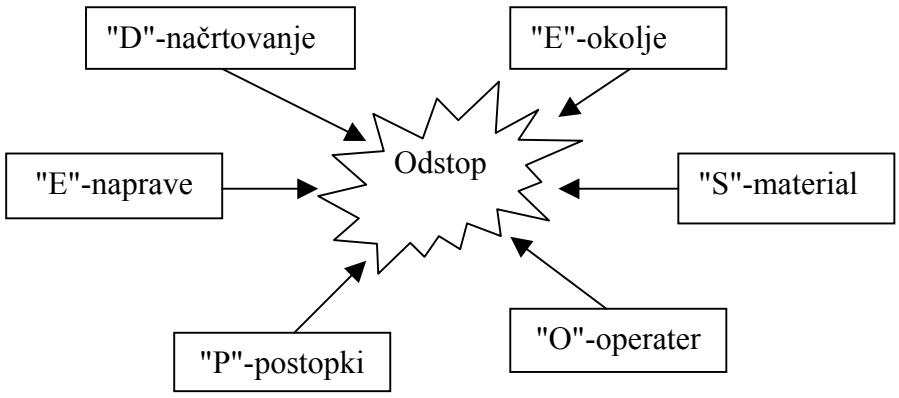
Mnogo manjših odstopov, ki se pojavijo skupaj z nepredvidenimi medsebojnimi vplivi, je posledica verige dogodkov, pri katerih se napake večajo in povzročijo neskladnost sistema. Njihov skupni rezultat je lahko kritični odstop in posledično neustrezen izdelek. Odstop je dogodek, pri katerem se nepravilnost vključi v definiran sistem in zmede potek ter bodoči pričakovani izhod sistema. Posamezni faktorji ne bi povzročili tega dogodka, ko pa se v nekem trenutku pojavijo povezano, lahko pripeljejo do nepopravljive škode.

Perrow uporablja metodo DEPOSE kot okvir za identifikacijo morebitnih virov napak. Napake se pojavljajo pri vseh obravnavanih komponentah sistema: načrtovanju, napravah, postopkih, operaterjih, materialih, okolju in jih uporabimo za analizo nesreč v različnih sistemih. (Perrow, 1984, str. 8)

Z metodo lahko analiziramo in razlagamo napake na teh sistemih z uporabo pojmov, kot so »linearni/kompleksni« sistemi in »ohlapne/tesne« povezave. (Perrow, 1984, str. 100)

Tako se te komponente, na osnovi katerih s pomočjo metode DEPOSE razčlenjujemo in ugotavljamo zakonitosti vzroka odstopov, pojavljajo kot del sistemov, ki jih vključujemo v obravnavani odločitveni model in so posredno ali neposredno vključeni v procese inšpekcije v podjetju. Želimo prikazati in opozoriti na posamezna dejstva in spoznanja o obravnavanih nesrečah oziroma odstopih v kontekstu obravnavane tematike: zagotavljanja skladnosti in uspešne inšpekcije. Naš namen je boljše razumevanje ozadja teh procesov in zakonitosti, ki bi jih drugače težko natančno vgradili v naš odločitveni model, je pa pomembno, da se jih zavedamo.

Slika 1: Sistem DEPOSE



Vir: Wenniger, 1991,S.47 po Perrowu, 1987

Kompleksnost naključij, ki povzročijo odpoved sistema, redkokdaj lahko predvidijo ljudje, ki so del sistema ali z njim delajo. Nepravilnosti običajno spregledajo prepozno. Vendar, poznavanje posledic dogodka lahko vpliva na to, kako te dogodke ocenimo. Kasnejše razumevanje stvari oziroma spregledanje jasnih dejstev, pomenijo tiste stvari, ki jih nismo videli ali razumeli že v času dogajanja odstopa, so pa pozneje očitne in retrospektivne. Nepopolno razumevanje dogajanja in nepoznavanje vseh dejstev lahko prevara ocenjevalca, da poenostavi vzroke odstopa, poudarja le posamezne elemente in pri tem spregleda mnoge druge sodelujoče faktorje.

Napake lahko učinkovito preprečimo ali omejimo s primerno organizacijo, strukturo in sistemom vodenja. V farmacevtskem podjetju je vzpostavljen celovit sistem zagotavljanja kakovosti.

Če dopuščamo, da se informacije o odstopu nenadzorovano širijo, nihče pa nima celovite informacije, se spoznanje lahko pojavi kot enostavna rešitev ali kot obsojanje posameznika, vendar tako s težavo določimo, kaj je resnično bilo narobe.

Značilne odstope, ki se pojavljajo v različnih sistemih, najdemo tudi v farmacevtski industriji, vendar so med njimi pomembne razlike. V mnogih procesih so ob napaki

delavci in podjetje neposredno prizadeti. V farmacevtski industriji ima škodo običajno tretja stranka. Večinoma je torej oškodovan bolnik, redkokdaj pa neposredno osebje ali podjetje. Prizadeti so lahko samo nekateri bolniki in ne cela skupina, kar dela odstop toliko bolj neviden.

Z analizo postopkov so ugotovili, da je človeška napaka vključena v 82 % preprečenih odstopov. Ocenjujejo pa tudi, da približno 60–80 % vseh odstopov povzroči človeška napaka, vzrok preostalih so v glavnem okvare na opremi (Perrow, 1984, str. 9). Ko se pojavi napaka na opremi, jo lahko s človeškim faktorjem celo poslabšamo, na primer človek ob napaki reagira napačno ali ne dojame novo nastalih razmer. Vendar, če rečemo, da je odstop nastal zaradi človeške napake, to ni enako, kot če nekoga obdolžimo.

3.2.3. Razumevanje napak

Napako definiramo kot odstopanje od načrtovanega zaporedja miselnih in fizičnih aktivnosti, da bi dosegli načrtovani rezultat, če teh odstopanj ni mogoče pripisati naključju. (Reason,1990)

Pomembno je opozoriti na upoštevanje »namena«, kajti napaka ni razumljiva brez upoštevanja njenega namena. Ločimo dve vrsti odstopov:
- aktivnosti ne potekajo, kot smo predvidevali;
- nameravana aktivnost ni ustrezna.

V prvem primeru, je želeni cilj lahko dosežen ali ne; v drugem primeru, želenega cilja ne moremo doseči.
Razlikujemo med spodrsljajem, lapsusom in napako. Razlika med **spodrsljajem** in **lapsusom** je, da je prvi opazen, drugi pa ne. Na primer, vrtenje napačnega gumba je lahko spodrsljaj; če nismo sposobni nekaj priklicati iz računalnikovega spomina, je to lapsus. Spodrsljaj ali lapsus se pojavita, ko izvedena aktivnost ni tisto, kar smo nameravali storiti. Posledica je odstop izvedbe. Pri **napaki** so aktivnosti izvedene tako, kot so bile načrtovane, vendar ne dosežemo nameravanega cilja, ker je bila že načrtovana aktivnost napačna. Stanje lahko zaradi pomanjkanja znanja neustrezno ocenimo. Pri napaki je prvotni namen neustrezen in imamo vključen odstop že v postopku načrtovanja.

V farmacevtski industriji spodrsljaji, lapsusi ali napake, ki povzročijo odstope, lahko ogrozijo bolnike. Na primer, v farmaciji je spodrsljaj, če delavec vnese neustrezno vrednost za recepturo: potrdi vrednost 10 mg, čeprav je imel namen dodati recepturo, na kateri piše 1 mg. Izvorni namen je bil pravilen (ustrezna receptura je bila izbrana glede na želeno učinkovino), vendar aktivnost ni sledila načrtovanemu procesu. Pri vnosu nepravilne sestavine pa govorimo o lapsusu, ker je izbrana receptura napačna. V tem primeru je že načrtovana aktivnost napačna.

Če uporabimo termina spodrsljaj in lapsus, je pomembno, da velikosti spodrsljaja ne enačimo z besedo »manjši«. Bolniki lahko dobijo napačno zdravilo tako zaradi spodrsljaja kot tudi zaradi lapsusa.

Napako definiramo kot odstop v načrtovani aktivnosti, kadar le-ta ni celovito izvedena, in jo imenujemo tudi "napaka v izvedbi". Pri uporabi napačnega pristopa za dosego cilja pa jo imenujemo "napaka v načrtovanju".

3.2.4. Skrite in aktivne napake

Ko analiziramo vpletenost ljudi v pojav napake, je pomembno razlikovati med aktivno in skrito napako. Aktivna napaka se pojavi na ravni delovanja in ima takojšen učinek. Pri tovrstnih napakah včasih govorimo o »ostrem koncu«. Skrita napaka ni neposredno povezana z delovanjem, ampak posledica slabega načrtovanja, nepravilne instalacije, napačnega vzdrževanja, slabe vodstvene odločitve in neustrezne organiziranosti. Take napake imenujemo tudi »skrhan konec«. Skrita napaka je posledica neodkrite pomanjkljivosti v načrtovanju.

Skrite napake so v kompleksnih sistemih največja neznanka glede varnosti, ker so pogosto nerazpoznavne in lahko povzročijo različne tipe aktivnih napak. Pri analizi odstopov običajno ugotavljamo, da so se sporni dogodki zgodili že v nekem časovnem obdobju pred pojavom napake. Ljudje, ki delajo na sistemih, napake težko zaznajo, ker so le-te lahko skrite že v načrtovanju rutinskih procesov ali pa so del upravljanja organizacije. Ljudje postanejo do teh odklonov neprevidni, se naučijo z njimi živeti in jih pogosto ne prepoznajo.

Poznamo pojem »normalizacija odklona«, pri katerem majhna sprememba v obnašanju postane normalna in se povečajo dopustne meje, tako da dodatni odstop postane sprejemljiv. Ko postanejo drugačni dogodki sprejemljivi, se zveča verjetnost za nastanek napak, vsi opozorilni signali se spregledajo ali napačno interpretirajo ter kopičijo brez opozorila.

Pri aktivnih napakah je odgovorna oseba znana in s kaznovanjem (npr. odstranitvijo), ponovnim šolanjem ali uvedbo drugih ukrepov sistem zaščitimo pred ponavljanjem aktivnih napak. Četudi uporabimo kazensko odgovornost, to ni učinkovita pot za zaščito pred ponovitvami. Večino večjih sistemskih napak zavzemajo skrite napake, njihovo aktiviranje je splet enkratnega naključja in je retrospektivno. Obstaja zelo majhna verjetnost, da bi se enaka kombinacija vplivnih dejavnikov ponovno pojavila; z ukrepi za zaščito specifičnih aktivnih napak še ne zvečamo same varnosti sistema.

Če se osredotočimo samo na aktivne napake, dopuščamo, da skrite napake ostanejo v sistemu in njihovo kopičenje dejansko nagiba sistem k bodočim odstopom. Odkritje in označitev skritih napak ter zmanjševanje njihovega trajanja ima velik učinek na gradnjo varnih sistemov, s katerimi si prizadevamo zmanjšati aktivne napake, ko se pojavijo.

3.3. Osnovna pravila za izgradnjo modela

3.3.1. Dobre prakse

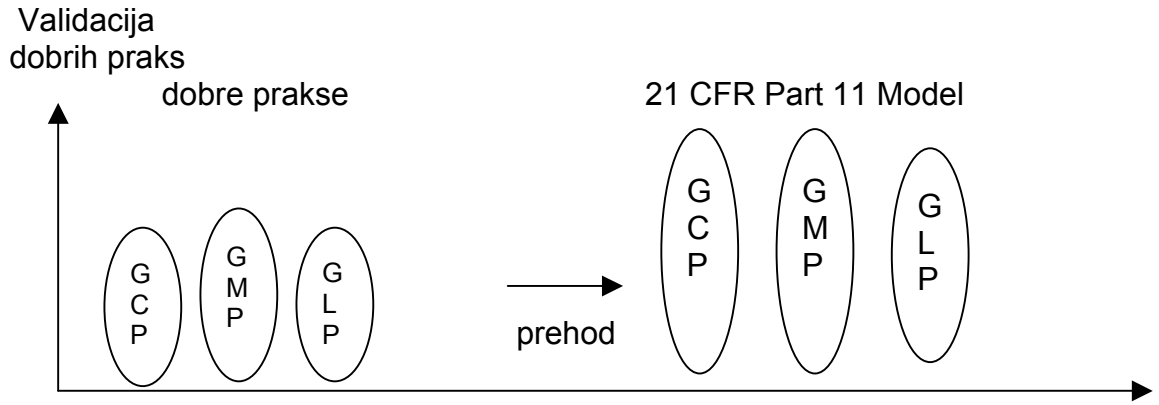
Regulativa na področju računalniških sistemov se nanaša na zapise v elektronski obliki in obsega zahteve dobre klinične prakse (*GCP*), dobre laboratorijske prakse (*GLP*), dobre proizvodne prakse (*GMP*), ki so skupaj znane kot sistem dobrih praks (*GxP*)[22] in se nanašajo na večino računalniških sistemov v okolju farmacevtske industrije; na njih je osnovana validacija računalniških sistemov.

---

[22] GxP - angl. Good Practices

Jasno razumevanje regulatornih zahtev, posebno osnovnih načel zagotavljanja kakovosti, je bistveno pri gradnji skladnosti z regulativo 21 CFR Part 11. Postaviti moramo tak sistem, da bomo zagotovili osnovne pogoje, ki vodijo k vključevanju izvedljivih rešitev.

Slika 2: Prikaz nadgraditve praks GxP v model 21 CFR Part 11



Vir: Lopez, 2001, str. 27

Dobre prakse se vsebinsko razlikujejo glede na okolje, na katerega se nanašajo (npr. okolje proizvodnje zdravil, laboratoriji itd.).

21 CFR Part 11 lahko obravnavamo tudi kot metodo za prenos znanja. Podatki oziroma »viri znanja« na enem mestu omogočajo hitrejše in popolno rudarjenje podatkov, učinkovito zaščito, izdelavo celovitih analiz in podporo sistemu upravljanja podjetja. Enega od izzivov predstavlja združevanje podatkov iz različnih računalniških in formacijskih virov ter konsolidacija kritičnih podatkov v tematske podatkovne vire. Cilj farmacevtskega podjetja je, da združi vse koristne podatke in različne informacije v centralno shrambo znanja.

3.3.2. Validacija računalniških sistemov

Z validacijo računalniških sistemov zagotovimo, da računalniški sistemi ustrezajo predvidenemu namenu. (OECD,1995, str. 12)
Z validacijskim procesom zagotovimo veliko stopnjo verjetnosti, da je računalniški sistem izdelan v skladu s specifikacijo, potrjeno v fazi načrtovanja. Pri tem moramo upoštevati sledeče vidike: (OECD,1995, str. 12-13)

a. Prospektivna validacija

Računalniški sistem načrtujemo tako, da zadostimo osnovnim načelom »dobrih praks« farmacevtske industrije in ga vpeljemo na planiran način. Obstajati mora zadostna dokumentacija, ki dokazuje, da je sistem bil projektno razvit v skladu s priznanimi normami kakovosti in tehničnimi standardi. Preden damo sistem v

uporabo, mora biti razvidno, da le ta ustreza postavljenim prevzemnim kriterijem, kar potrdimo s primernim testiranjem sistema. Formalno testiranje zahteva, da s testi sledimo validacijskemu planu in da ohranimo dokumentirano evidenco vseh testnih postopkov, uporabljenih podatkov, dobljenih rezultatov, povzetek poteka testiranja in zapise formalnih potrditev.

Validacijo izvedemo na osnovi validacijskega plana, v katerega so zajete naslednje osnovne vsebine:

- uveljavitev razvojne metodologije, ki se najbolje sklada z naravo razvijajočih sistemov;
- izbira strojne opreme na osnovi zmožnosti in funkcionalnosti;
- identifikacija in upoštevanje operativnih mej, npr. za določitev razvojnih, analitskih ali proizvodnih postopkov;
- identifikacija in testiranje operativnih funkcij, povezanih z uporabniki, procesom, regulativo, standardi podjetja in varnostnih zahtev;
- identifikacija in testiranje skrajnih mej pogojev proizvodnje;
- ponovljivost testnih rezultatov, osnovana na statistiki;
- dokumentiranje validacijskega procesa;
- veljavnost napisanih procedur za vzdrževanje validiranega stanja računalniških sistemov (navodila za delo, navodila za administracijo, nadzor sprememb).

Sistemska validacija naj bi zajemala dokumentacijo življenjskega cikla sistema, verificiranje in testiranje.

21 CFR Part 11 obravnava validacijo v sekciji §11.10(a*)* takole:
“Sistemi morajo biti validirani tako, da zagotovimo točnost, zanesljivost, doslednost delovanja in zmožnosti razločevanja neveljavnih ali spremenjenih zapisov.“ (Code of Federal Regulations, 1997, str. 11)

Sistem mora biti sposoben zaznavanja nepravilnih in spremenjenih zapisov, računalniško ustvariti zgodovino dogodkov in preverjati polja podatkovnih formatov. Kot del validacijskega procesa ohranitve zapisov je potrebno dokazati, da je sistem sposoben upravljanja z določenim obsegom spominskega prostora, kjer so shranjeni podatki oziroma informacije.

b. Retrospektivna validacija

Obstajajo sistemi, za katere zahteve po skladnosti z načeli »dobrih praks« niso v času uvedbe sistema niso bile predvidene ali določene. Izvedemo retrospektivno vrednotenje za izdelavo ocene primernosti sistema. Retrospektivna validacija se izvede za obstoječe sisteme GxP, za katere osnovna (začetna) validacija ni bila izvedena.

c. Nadzor sprememb

Nadzor sprememb je formalna potrditev in dokumentiranje vsake spremembe na računalniških sistemih skozi življenjski cikel sistema. Potrebna je takrat ko sprememba lahko vpliva na validacijski status računalniškega sistema. Postopki

kontrole sprememb se izvajajo na računalniških sistemih, ko so le-ti enkrat že operativni.

Postopki opisujejo metode vrednotenj, s katerimi določimo dodatna potrebna testiranja, s katerimi vzdržujemo validirani status sistema. V postopkih nadzora sprememb identificiramo osebe za izvedbo in potrditev ter njihovo odgovornosti.

d. Podporne aktivnosti

Da lahko računalniški sistemi ostanejo ustrezni glede na predvideni namen, se uvedejo podporni mehanizmi, s čimer zagotovimo funkcioniranje sistema in njegovo pravilno uporabo. To lahko vključuje sistemsko vodenje, izobraževanje, vzdrževanje, tehnično pomoč, presoje in ponovne kvalifikacije.

3.3.3. Elementi validacije računalniških sistemov

Na osnovi **uporabniških zahtev** in zahtev **dobrih praks** uvedejo farmacevtska podjetja primerne razvojne projekte. **Metodologijo razvojnega cikla sistema** izberejo glede na **vrsto projekta**, ki kasneje opredeli tudi metodologijo **validacije računalniških sistemov** v okviru **aktivnosti za zagotavljanje kakovosti**.

Navedeni osnovni elementi validacije računalniških sistemov temeljijo na regulatornih zahtevah. Osnova za validacijo in tudi za naš model so konstantne regulatorne zahteve ameriške Agencije za prehrano in zdravila, kar je prikazano spodaj.

Opredelitev posameznih elementov:

- Zahteve uporabnika
  - Niso konstantne

Uporabnik določi svoje želje in zahteve v dokumentu »Zahteve uporabnika«. Zahteve uporabnika je dokument, ki opisuje aplikacijo s funkcijskega vidika. Poudarek je na zahtevanih funkcijah in ne na metodah za uporabo teh funkcij. Vsebina in konteksti dokumenta so vezani na vrsto različnih sistemov, ki jih obravnavamo.

- Dobre prakse
  - Niso konstantne

Dobre prakse se v farmacevtski industriji spreminjajo glede na nova spoznanja in razvoj; pomemben del sprememb je povezan z uvajanjem vedno novih tehnologij.

- Vrsta projekta
  - Metodologija razvojnega cikla sistema
    - Aktivnosti zagotavljanja kakovosti (Metodologija validacije rač. sistemov)

- Metodologija razvojnega cikla sistema
  - Ni konstantna

Izbiro metodologije razvojnega cikla sistema določa izbrana razvojna programska oprema.

- Metodologija validacije računalniških sistemov
  - Ni konstantna

Izbiro ustrezne metodologije validacije računalniških sistemov določa vrsta uporabljene programske opreme.

- Regulatorne zahteve
  - **So konstantne** za vse obravnavane sisteme

3.4. Zahteve za validacijo računalniških sistemov

Z analizo 3140 medicinskih naprav, odpoklicanih med letoma 1992 in 1998, je ameriška FDA odkrila, da je bilo med vsemi 242 (7,7 %) takih, ki so bile nagnjene k programskim napakam. Od teh, programsko povezanih odpoklicev je bilo 192 (79 %) povzročenih s programsko napako, uvedeno pri izvedbi sprememb na programih po njihovi začetni izdelavi in poznejši distribuciji. (CDRH, 2002, str. 3)
Naloga validacije računalniških sistemov in drugih povezanih dobrih praks programskega inženiringa je, da že v času razvoja najde odstope in se izogne napakam pri izdelavi ter posledičnim odpoklicem zdravil s trga.

Validacija računalniških sistemov je zahteva regulative sistema kakovosti. Objavljena je bila v zveznem registru (FR)[23] 7. oktobra 1996, veljati pa je začela 1. junija 1997 (gl. *Title 21 Code of Federal Regulations Part 820 in 61 Federal Register*).

Validacijske zahteve se nanašajo na programe, ki so sestavni del naprav, na samostojne programske sisteme ter na programsko opremo, uporabljeno za izdelavo naprav ali sistemov kakovosti v podjetju. Dokler ni posebej izvzeto, je vsak programski izdelek, razvit po 1. juniju 1997, ne glede na vrsto naprave predmet kontrole ustreznega načrtovanja (gl. *21 CFR §820.30*). Ta zahteva se nanaša tako na projekte, ki še potekajo, kot na vse nove razvojne projekte in na vse spremembe na obstoječih napravah. Specifične zahteve za validacijo računalniških sistemov najdemo tudi v 21 CFR §820.30 (g). Dokumentirani rezultati teh aktivnosti so dodatna podpora trditvi, da je računalniški sistem validiran. (CDRH, 2002, str. 3)

Vsak sistem, ki je uporabljen za avtomatizacijo kateregakoli procesa ali dela sistema kakovosti, mora biti validiran glede na namen uporabe, kot je zahtevano z 21 CFR §820.70 (i). Za računalniške sisteme, ki uporabljajo (ustvarjajo, vzdržujejo, spreminjajo, prenašajo) elektronske zapise in uvajajo elektronske podpise, je bila 20. avgusta 1997 objavljena regulativa 21 CFR Part 11, ki opredeljuje zahteve na področju elektronskih zapisov in elektronskih podpisov.

---

[23] FR - angl. ***F**ederal **R**egister*

3.4.1. 21 CFR Part 11

20. avgusta 1997 je ameriška vladna agencija FDA javno objavila regulativo 21 CFR Part 11 (skrajšano Part 11), Electronic Records, Electronic Signatures, Final Rule in z aktivnim pristopom posegla na vsa področja delovanja farmacevtske industrije v elektronskih tehnologijah. Pravila so razdeljena na tri sekcije (Code of Federal Regulations, 1997, str. 8):

- poglavje A, Splošni pogoji
- poglavje B, Elektronski zapisi
- poglavje C, Elektronski podpisi

Z njimi so določeni tehnični in proceduralni standardi za uporabo elektronskih zapisov (e-zapisov) in elektronskih podpisov (e-podpisov).

Podpisi se lahko pojavljajo v ročni, elektronski ali digitalni obliki. 21 CFR Part 11 se nanaša na podatke, ki neposredno vplivajo na kakovost izdelka in njegovo distribucijo. Regulativa določa pravila, po katerih agencija obravnava elektronske zapise in elektronske podpise z vidika zaupanja in zanesljivosti; ti so popolnoma enakovredni papirnim zapisom in ročnim podpisom.

Regulativa o elektronskih zapisih se nanaša na nove in tudi starejše sisteme. Kot nove obravnavamo elektronske zapise, ki so bili ustvarjeni po začetku veljavnosti regulative. 21 CFR Part 11 se nanaša tudi na elektronske zapise, ki so bili ustvarjeni pred omenjenim datumom in so bili pozneje spremenjeni, vzdrževani, arhivirani, obnovljeni ali poslani s pomočjo računalniškega sistema.

Pomembno je poudariti, da ne zadostuje samo, da so starejši sistemi »prevzeti«, ampak da FDA pričakuje, da podjetja izvedejo potrebne korake za njihovo skladnost.

V nasprotju z drugo vladno zakonodajo je 21 CFR Part 11 razvit kot odgovor ameriške vlade na zahteve farmacevtske industrije, ki je želela na področju raziskav, razvoja in proizvodnje zdravil preiti na novejše, napredne računalniške tehnologije. Regulativa je v sodelovanju z industrijo nastajala šest let. Vpeljava novih pravil zagotavlja pogoje, pod katerimi bo FDA imela elektronske zapise za enakovredne papirnim zapisom in elektronske podpise za enakovredne ročnim podpisom. Regulativa 21 CFR Part 11 dopušča najširšo možno uporabo elektronskih tehnologij. Za uporabo elektronskih zapisov se podjetja odločijo prostovoljno, vendar morajo ob njihovem uvajanju upoštevati regulatorne zakonitosti.

Regulativa 21 CFR Part 11 je logično nadaljevanje že uveljavljenih zbirk predpisov dobrih praks in postavljenih pravil ameriške Agencije za prehrano in zdravila. Nova pravila se nanašajo na razvoj, izdelavo in nadzor elektronskih zapisov po smernicah, kot jih določa regulativa FDA. Zajeti so tudi ročni podpisi, izvedeni na elektronskih zapisih, ki so enakovredni ročnim podpisom in papirnim zapisom. (Qineito Trusted Information Managment, 2002, str. 1)

Na kratko, vsak računalniški sistem, ki uporablja zapise in ga obravnavamo po metodologiji FDA za validacije računalniških sistemov, mora biti usklajen z

regulatornimi zahtevami za elektronske zapise in elektronske podpise. (CDRH, 2002, str. 30)

Vendar vsi sistemi, ki uporabljajo elektronske zapise in/ali elektronske podpise in so del informacijske strukture podjetja, ne sodijo pod nadzor FDA in jih ni treba podrediti zahtevam skladnosti s 21 CFR Part 11. Na primer, elektronski podatki o proizvodni seriji in zapisi izobraževanj se obravnavajo v okviru teh pravil, elektronski finančni zapisi pa ne. Kljub temu je pomembno imeti v mislih, da se tudi agencije, kot so SEC[24] in druge, pripravljajo na izdajo podobne regulative in da bodo zahtevale podobno kontrolo elektronskih zapisov ter elektronskih podpisov in bodo splošno prevzete kot dobre prakse informacijske varnosti.

3.5. Regulatorne zahteve in smernice

V okviru regulative validacije računalniških sistemov že nastopajo spodaj navedene zahteve

Regulativa:

- *"21 CFR 211 Code of Federal Regulations, Title 21 - Food and Drugs. Part 211 Current Good Manufacturing Practice For Finished Pharmaceuticals"*

a) 21 CFR §211.2(b): izdano leta 1963
   Obravnava shranjevanje podatkov in validacijsko dokumentacijo, ki obsega glavne formule, specifikacijo, testne zapise, zapise proizvodnih poročil in kontrole, zapise proizvodnih serij in izračune.
b) 21 CFR §211.68: izdano leta 1976
   Obravnava vzdrževanje računalniških sistemov, kontrolo sprememb, validacijo vhodno-izhodnih točk, točnost podatkov in varnost, nadzor elektronskih zapisov (shranjevanje, varnost in ohranitev zapisov).

Tabela 1: Regulativa 21 CFR Part 211, ki se nanaša na računalniško opremo in elektronske zapise

21 CFR	Oprema	21 CFR	Zapisi
§211.22	- odgovornosti upravljanja kakovosti	§211.101(d)	- verifikacija zapisov
§211.25	- kvalifikacija osebja	§211.180(a)	- ohranitev zapisa
§211.63	- (primerna) lokacija naprave	§211.180(c)	- dostop do zapisa
§211.67	- čistilni postopki in vzdrževanje	§211.180(d)	- medij zapisa
§211.100	- napisani postopki in nepravilnosti	§211.180(e)	- pregled zapisa
§211.105(b)	- identifikacija	§211.188(a)	- točnost reprodukcije
§211.180	- zapisi	§211.188(b)(11)	- dokumentiranje
§211.182	- čistilni postopki	§211.192	- pregled zapisa s strani kontrole kakovosti

Vir: Lopez, 2001, str. 17-18

[24] SEC - angl. ***S**ecurities and **E**xchange **C**ommision*

Druga ključna regulativa in smernice:

- "*European Union E-commerce Legislation and Regulations*"
- *"Pharmaceutical Inspection Convention, Best Practices for Computerized System in Regulated 'GxP' Environments, Draft Version 3.01, Jan 2000"*
- "*EC Directive 1999/93/EC, A Community Framework for Electric Signature, Published on the Official Journal of the European Communities, 19. 1. 2000*"

"Direktiva št.1999/93/EC Evropskega parlamenta in Sveta EU z dne 19. januarja. 2000 o Skupnosti za elektronske podpise. "

- *"The rules governing medicinal products in the European Union (EU), Volume 4, Good Manufacturing practice, 1997 Edition, Annex 11 - Computerized Systems*"
- *"Guidance for industry; Part 11, Electronic Records; Electronic Signatures – Scope and Application, Feb 2003"*
- *"Good Practice and Compliance for Electronic Records and Signatures: Good Electronic Records Managment (GERM):Part 1, Version 1, July 2002 "*
- *"GAMP Special Interest Group, "Good Practice and Compliance for Electronic Records and Signatures, Part 2, Complying with 21 CFR Part 11, Electronic Records and Electronic Signature"*
- *"GAMP 4, Guide For Validation of Automated Systems in Pharmaceutical Manufacture, Volume 1: User guide, December 2001"*

Tabela 2: Prikaz ključnih sekcij regulative GAMP-a in Aneks-a 11, ki vsebinsko ustrezajo sekcijam 21 CFR Part 11- Elektronski zapisi v zaprtih sistemih

GAMP dodatek 4 priročnik	EU Aneks 11 Računalniški sistemi	21 CFR Part 11 Elektronski zapisi- zaprti sistemi	
2, 2.1, 4	11.2, 11.7, 11.19	*§ 11.10(a)*	Validacija
5	11.12, 11.13	*§ 11.10(b)*	Kopije zapisov
5, 2 ,2.1 ,6	11.13, 11.14, 11.15, 11.16	*§ 11.10(c)*	Zaščita zapisov
3, 4	11.8, 11.19	*§ 11.10(d)*	Sistemski dostop
4	11.10, 11.19	*§ 11.10(e)*	Zgodovina dogodkov
4	11.16, 11.19	*§ 11.10(f)*	Zaporedje
3, 4	11.8, 11.9, 11.10	*§ 11.10(g)*	Preverjanje pooblastil
2.1, 4	11.6, 11.9	*§ 11.10(h)*	Preverjanje naprav
1.3	11.1	*§ 11.10(i)*	Izobraževanje
4	11.19	*§ 11.10(j)*	Politike
2, 2.1, 6	11.16, 11.17	*§ 11.10(k)(1)*	Kontrola dokumentacije
2, 2.1, 6	11.11, 11.17	*§ 11.10(a)(2)*	Kontrola sprememb

Vir: Electronic records and electronic signatures An Insight, Tescom,15.1.2003

3.6. Modeli razvojnega cikla sistema

Razvojni cikel sistema: opisuje faze razvoja računalniškega sistema. Te faze so običajno: zasnova, definiranje zahtev, načrtovanje, izgradnja, izvedba, delovanje, vzdrževanje, sistem sprememb in iztek življenjskega cikla sistema. (National Archives and Record Administration, 2000, str. 5)

Nekatere oblike razvojnih ciklov sistema: (Webster's, 1997, str. 23)

3.6.1. Kaskadni model

Model razvoja programa, pri katerem so posamezne faze: zasnova, definiranje zahtev, načrtovanje, uporaba, testiranje, instalacija in preverjanje, delovanje in vzdrževanje dosledno izvedene po vrsti; možno je prekrivanje, vendar brez medsebojnega vpliva. Dokumentacija si sledi od validacijskega plana do končnega validacijskega poročila.

3.6.2. Inkrementalni model razvoja

Model razvoja programa, pri katerem se definiranje zahtev, načrtovanje, uporaba in izvedba testiranja pojavljajo v prekrivajočih, vzajemnih aktivnosti ter se kažejo v postopnem, naraščajočem dokončanju celotnega programskega izdelka.

3.6.3. Spiralni model

Model razvoja programa, pri katerem se zahteve analize, začasna in natančna načrtovanja, programiranje, integracije in testiranje izvajajo vzajemno, dokler program ni končan.

3.6.4. Objektno orientiran model

Model razvoja programa, pri katerem so sistem ali sestavni deli izraženi v odnosu do objektov in povezav med temi objekti.

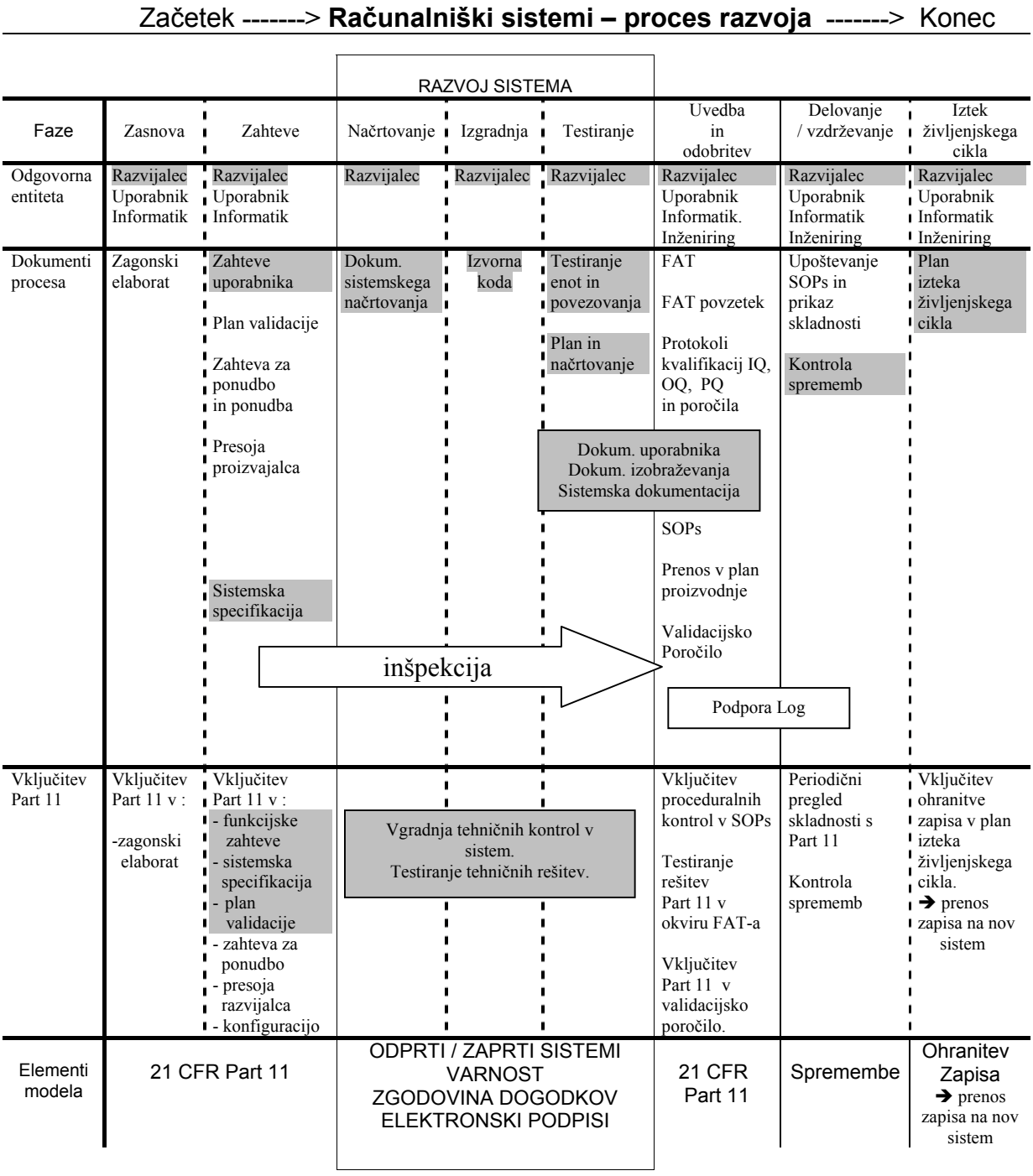
Razvojni cikel sistema definira aktivnosti, ki so primerne za validacijo računalniških sistemov**.**

3.7. Prikaz faze razvojnega cikla računalniškega sistema

Prikazane so osnovne razvojne faze, odgovorni nosilci aktivnosti in vsi bistveni postopki oziroma dokumentacija v procesu razvoja računalniškega sistema. (glej slika 3)

Pri načrtovanju skladnosti z 21 CFR Part 11 dodamo še polja, ki dodatno vključujejo zahteve za aktivnosti, potrebne za 21 CFR Part 11. Spremna dokumentacija in postopki so prikazani tako z zornega kota uporabnika kot razvijalca sistema (obarvano temneje).

Slika 3: Prikaz faze razvojnega cikla računalniškega sistema in vključitev zahtev regulative 21 CFR Part 11

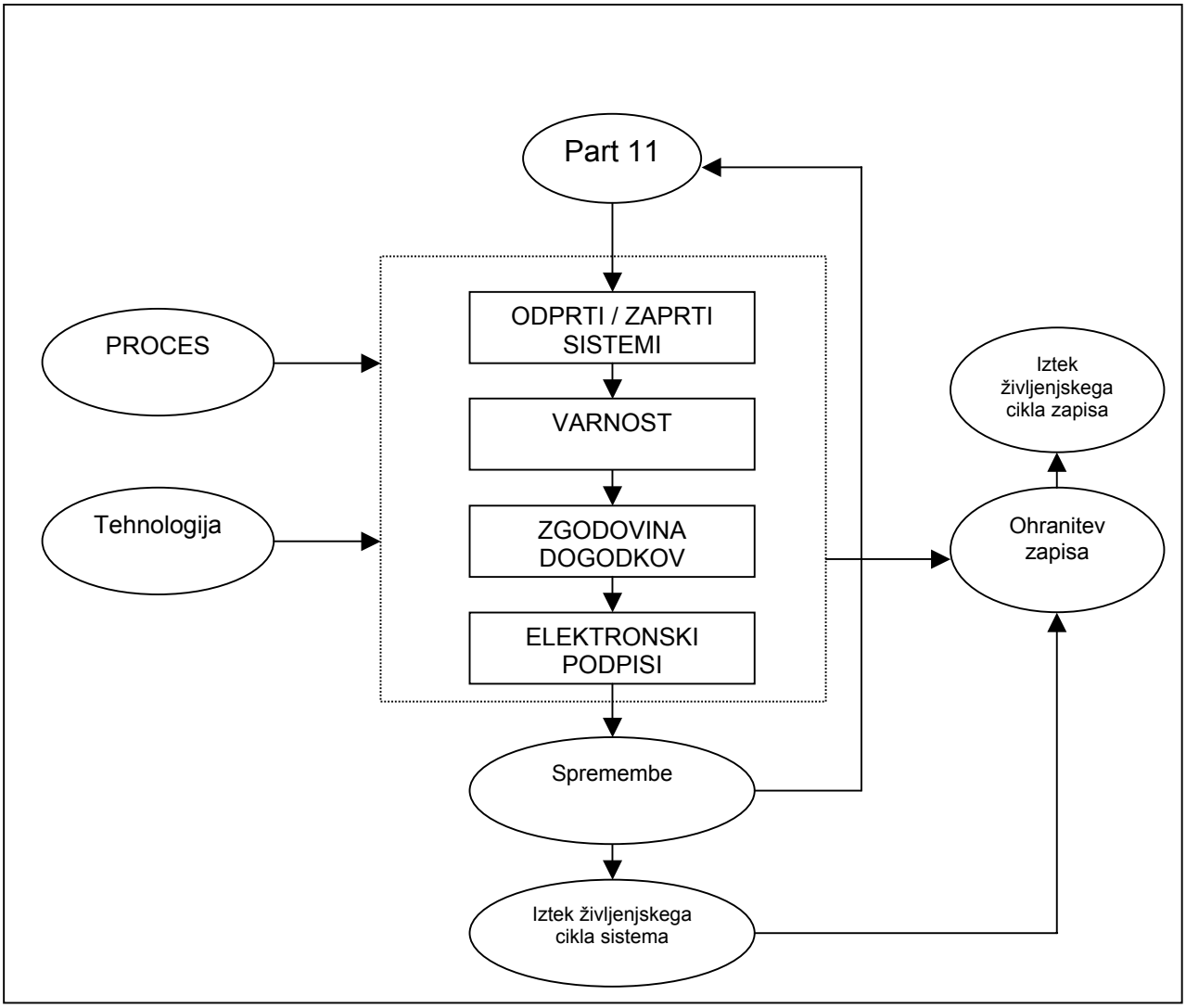


Vir: Lopez,2000, str. 23

Zadnja vrstica na sliki prikazuje osnovne elemente 21 CFR Part 11 kot del modela validacije računalniških sistemov.

3.8. Model

Slika 4: 21 CFR Part 11 kot del modela validacije računalniških sistemov



3.8.1. Elementi modela

3.8.1.1. Odprti/zaprti sistemi

Raven zahtevanih kontrol je odvisna od tega, ali sistem obravnavamo kot odprt ali zaprt. Qineito Trusted Information Managment, 2002, str. 3) FDA definira odprte sisteme kot »okolje, v katerem sistemskega dostopa ne kontrolira osebje, odgovorno za vsebino elektronskih zapisov, ki so na sistemu«. (Code of Federal Regulations, 1997, str. 10) Večina internetnih in ekstranetnih sistemov se uvršča v odprte sisteme. Nasprotno so zaprti sistemi »okolje, v katerem sistemski dostop kontrolira osebje, odgovorno za vsebino elektronskih zapisov, ki so na sistemu«. (Code of Federal Regulations, 1997, str. 10) Primer zaprtega sistema je lokalna mreža, ki ni povezana z drugimi poslovnimi mrežami ali internetom.

Vsi odprti sistemi, skladni z 21 CFR Part 11, vključujejo šifriranje dokumentov, digitalne podpise ali podobno tehnologijo za zaščito zaupnosti, celovitosti in avtentičnosti elektronskih zapisov na sistemih.

Zaprti sistemi: Procedure in kontrole

Arhitektura zaprtih sistemov mora temeljiti na politiki, procedurah in kontroli, s katerimi zagotovimo avtentične, celovite in, kjer je potrebno, zaupanje vredne elektronske zapise. Zagotoviti moramo mehanizme, pri katerih podpisnik ne more spodbijati pristnosti podpisanega zapisa.
Sekcija §11.10 21 CFR Part 11 podaja tehnične in proceduralne zahteve za zaprte sisteme. V nadaljevanju podajamo pregled zahtev za zaprte sisteme: (Qineito Trusted Information Managment, 2002. str. 4)

§11.10(a): Sistemi morajo biti validirani tako, da zagotovimo točnost, zanesljivost, doslednost delovanja in zmožnosti razločevanja neveljavnih ali spremenjenih zapisov.

§11.10(b): Organizacije morajo zagotoviti proizvajanje točnih in popolnih kopij zapisov v človeku čitljivi in elektronski obliki, primerni za inšpekcije, preglede in kopiranje, ki jih bo izvajala FDA.

§11.10(c): Organizacije morajo zaščititi zapise, da ohranijo njihovo točnost in sposobnost ponovne vzpostavitve v celotnem obdobju hranjenja zapisov.

§11.10(d): Organizacije morajo omejevati informacije in omogočiti dostop do sistemov samo pooblaščenim posameznikom.

§11.10(e): Organizacije morajo zagotoviti varno, računalniško proizvedeno zgodovino dogodkov s časovnim žigom ter neodvisno zapisovanje podatkov, časov operaterjevih vnosov in vrste izvedenih aktivnosti. Sistemske aktivnosti ne smejo okrniti podatkov, npr. prepisati predhodnih s sedanjimi.

§11.10(f): Organizacije morajo uporabljati procedure, ki omogočajo ustrezno zaporedno delovanje sistema. Če imamo zaporedne operacije, zaporedje dogodkov ali zaporedno vnašanje podatkov je pomembno, da sistem zagotovi, da si ta zaporedja sledijo.

§11.10(g): Organizacije morajo uporabljati politiko in procedure za zagotovitev preverjanja pooblastil uporabnikov informacijskega sistema, s čimer samo pooblaščenim posameznikom zagotovijo uporabo sistema za elektronsko podpisovanje zapisov, dostop do operacij oziroma računalniških vhodnih/izhodnih naprav, spremembo zapisov in ročne izvedbe operacij.

§11.10(h): Organizacije morajo oceniti tveganje in uvesti periodično kontrolo naprav (npr. terminalov), preverjanje vhodnih podatkov in operativnih navodil.

§11.10(i): Organizacije morajo definirati metode, s katerimi preverjajo izobraževanje, urjenje in pridobivanje izkušenj za izvedbo dela, za katerega so odgovorni, pri sistemskih uporabnikih, raziskovalcih in izobraževalnem ter vzdrževalnem osebju.

§11.10(j): Organizacije morajo definirati in slediti napisani politiki, ki določa popolno odgovornost za vse aktivnosti, ki se pojavijo v sklopu elektronskih podpisov in s katerimi pomagamo zaščititi zapise in podpise proti ponarejanju.

§11.10(k): Organizacije morajo kontrolirati dostop do sistemske in vzdrževalne dokumentacije. Takšne kontrole naj bi vpeljale postopke nadzora sprememb za vzdrževanje zgodovine dogodkov in nadzora za spremembe na sistemski ali vzdrževalni dokumentaciji.

Splošne zakonske določbe s področja elektronskega poslovanja ne veljajo v zaprtih sistemih, kjer se medsebojni odnosi in pravila poslovanja urejajo s sporazumi, ki veljajo le za člane teh zaprtih sistemov. (Pavliha, Bogataj, et al., 2002, str. 23)

Odprti sistemi: Dodatne zahteve

Zaradi narave arhitekture odprtih sistemov in možnih tveganj moramo uporabiti dodatne kontrole, da zadostimo zahtevam skladnosti. Poleg kontrol, ki so del zaprtih sistemov, dodamo zgoščevalne algoritme, tajnopise, digitalne podpise ali podobne tehnologije, da zagotovimo avtentičnost, celovitost in zaupnost elektronskih zapisov.

Te zahteve so določene v sekcijah §11.30 in §11.50 regulative 21 CFR Part 11. Sekcija §11.70 zahteva, da mora biti elektronski podpis, kadar je izveden na elektronskih zapisih, tehnološko povezan s tem elektronskim zapisom. Za zaščito elektronskih zapisov, ko so ti enkrat podpisani, pred morebitnimi spremembami je treba uporabiti varnostno tehnologijo. Pri spremembi elektronskega zapisa se mora sprememba vpisati v zgodovino dogodkov skupaj s podpisom pooblaščene osebe. Regulativa 21 CFR Part 11 omenja pojem »digitalni« podpis kot obliko elektronskega podpisa, uporabljenega v odprtih sistemih.

FDA definira digitalni podpis kot:
"… zasnovan na kriptografskih metodah overitve podpisnika, računalniško obdelan z uporabo vrste pravil ter vrste parametrov, ki so takšni, da se lahko preveri identiteta podpisnika in nedotakljivost podatkov". (Code of Federal Regulations, 1997, str. 10)

Šifriranje je proces transformacije besedila (čistopis) v obliko, ki onemogoča njegovo razumevanje (tajnopis). Obraten proces je dešifriranje. S šifriranjem zaščitimo ***zasebnost*** zapisa (zahteva 21 CFR Part11-§11.10(d)) in omogočimo njegovo **zaščito**. (zahteva 21 CFR Part11-§11.10(c)).

Za popolno razumevanje digitalnih podpisov (American Bar Association, 1996, 125 str.) moramo razumeti infrastrukturo javnega ključa *(*PKI[25]), ki je lahko uporabljena za odprte sisteme znotraj farmacevtske industrije. Infrastruktura javnega ključa je najboljša izbira za zagotovitev skladnosti z 21 CFR Part 11 glede varnostnih zahtev; s tem posledično zagotavljamo zasebnost zapisov. Omenjena infrastruktura temelji na različnih standardih za kriptografijo javnih ključev. FDA najpogosteje omenja standard za šifriranje javnih ključev (PKCS[26]), razvit v laboratorijih RSA[27], vendar za farmacevtsko podjetje ni obvezno, da ga uporabi.

---

25 PKI - angl. ***P**ublic **K**ey **I**nfrastructure*

26 PKCS - angl. ***P**ublic **K**ey **C**ryptography **S**tandards*

27 RSA - angl. **R**ivest-**S**hamir-**A**dleman

Infrastruktura javnega ključa je kombinacija programske opreme, tehnologije dešifriranja, platforme na osnovi strežnikov in delovnih postaj, politik za upravljanje digitalnih certifikatov in parov javnega ter zasebnega ključa, ki omogoča uporabnikom varno in zasebno izmenjavo podatkov v nezavarovanem javnem omrežju, kot je internet.

Digitalni certifikat ali potrdilo je dokument v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto. (Pavliha, et al., 2002, str. 39) Digitalni certifikati so digitalno podpisane podatkovne strukture, ki vsebujejo informacije, kot so ime entitete, javni ključ, algoritem podpisa in razširitev. Najbolj razširjena uporabljena specifikacija digitalnega certifikata je standard ITU X.509. Tehnika na osnovi digitalnega certifikata zagotavlja ***avtentičnost*** sporočil. (zahteva 21 CFR Part 11-§11.10(d))

Kot sredstvo za oblikovanje elektronskega podpisa se uporablja nastavljen program (na primer program za varno elektronsko pošto) ali spletni strežnik ali strojna oprema (na primer pametne kartice z izvedbo algoritmov za podpisovanje ali kriptografski modul). (zahteva 21 CFR Part 11 - §11.10 (h), gl. preverjanje)

Prikazanih je nekaj elementov, ki so bistveni za razumevanje infrastrukture javnega ključa z zornega kota osnovnih zahtev 21 CFR Part 11:
Overitelj je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. (Pavliha, Bogataj, et al., 2002, str. 40)

Overitelj, ki izdaja potrdila (CA[28])
To je center »zaupanja« v infrastrukturi javnega ključa, v katerem se upravlja s certifikati javnega ključa v njihovem življenjskem ciklu. (McDowall, 2001, str. 1) Overitelj izdaja certifikate javnega ključa (potrdila), ki povezujejo identiteto uporabnika ali sistema z njegovim javnim ključem. Vsi certifikati imajo rok uporabe, vendar se lahko prekličejo in se objavijo v listi razveljavljenih (preklicanih) certifikatov, t. i CRL[29].

Izjava o uporabi certifikata *(CPS[30])*
Predstavlja opis postopkov delovanja overitelja. Sistemi infrastrukture javnega ključa (PKI), ki uporabljajo overitelja za izdajo potrdil (CA), zahtevajo izjavo o uporabi certifikata (CPS). Ta izjava razčlenjuje operativne procedure o uporabi varnostne politike in podpore v praksi. Definira sestavo overitelja, njegovo delovanje, način izdaje certifikata, sprejetje in preklic potrdil, generiranje ključev, registracije in overitve, kje in kako jih hranimo ter kako jih prilagodimo uporabniku.

Urad za registracijo *(RA[31])*
Zagotavlja povezavo med uporabnikom in overiteljem (CA). Preveri identiteto uporabnika in njegovo zahtevo po certifikatu, ki ga izda overitelj (CA). Kakovost tega procesa overitve določa raven zaupanja, ki ga lahko vgradimo v certifikat. (McDowall, 2001, str. 1)

---

28 CA - angl. **C**ertificate **A**uthority

29 CRL - angl. ***C**ertificate **R**evocation **L**ists*

30 CPS - angl. ***C**ertificate **P**ractice **S**tatement*

31 RA - angl. **R***egistration **A**uthority*

Ključno je, da uporabniki infrastrukture javnega ključa (PKI) zaupajo v overitelja (CA) in urad za registracijo (RA) tako, da posameznikom ni potrebno ustvariti medsebojnega zaupanja. Infrastruktura omogoča ***preprečevanja zanikanja*** pošiljanja ali podpisovanje sporočila.

Seznam za nadzor dostopa (*ACL*[32])
Spisek varnostnih zaščit, ki se nanaša za objekt. Objekti so lahko datoteke, procesi, dogodki …, skratka vse, kar ima varnostni opis. (21 CFR Part 11 - §11.10 (d), gl. sistemski dostop)

Sistem distribucije certifikatov
Certifikati se lahko razpošljejo po nekaj različnih poteh, odvisno od strukture okolja infrastrukture javnega ključa (PKI). Strežnik s tem imenikom lahko že obstaja znotraj organizacije ali pa je lahko sestavni del izvedbe certifikatnega overjanja.

Politika certificiranja
Ko podjetje želi uporabiti infrastrukturo javnega ključa (PKI), mora imeti varnostno politiko z ustreznimi postopki znotraj nje.

Ti postopki so zahtevani tudi v skladu z 21 CFR *Part 11* regulativo in podjetje mora imeti resnično celovit vpogled o možnosti njene uporabe. (McDowall, 2001, str. 2) Politika definira najvišjo raven zahtev za informacijsko ***varnost***, vključno s tajnopisom in postopki ravnanja z javnim in zasebnim ključem, ter tudi njihovo intelektualno lastnino, izobraževanja.

Varnost overitelja *(CA)/* ***Urada za registracijo*** *(RA)*
Urada za registracijo in overitelj so srce infrastrukture javnega ključa. Varnost teh sistemov je primarnega pomena. Če je ta kompromisna, je celotna infrastruktura javnega ključa brez pomena.

Digitalni podpis je oblika elektronskega podpisa. Njegova uporaba zagotavlja mehanizem za preverjanje celovitosti podpisa kot povezave zapisa z identiteto podpisnika, kar je osnovna zahteva sekcije §11.70 v 21 CFR Part 11.

Digitalni podpis vsebuje najmanj dva ključa: (McDowall, 2001, str. 2)

– javni ključ, ki je na voljo vsem uporabnikom,
– zasebni ključ, ki mora ostati tajen.

V digitalnih podpisih zasebni ključ označuje, javni ključ pa preverja avtentičnost podpisov, s čimer se preverjata osebna identiteta in celovitost podatkov. Javni ključ šifrira sporočila, zasebni ključ jih dešifrira tako, da dosežemo določeno raven zaupnosti. Šifriranje ščiti ***zasebnost*** zapisov.

Podpisnik uporabi za oblikovanje elektronskega podpisa edinstvene podatke, kot so šifre in zasebni ključ v asimetrični (javni) kriptografiji. Za preverjanje elektronskega podpisa prav tako nastopajo edinstveni podatki, npr. javni ključ v asimetrični kriptografiji.

---
[32] ACL - angl. ***A**ccess **C**ontrol **L**ist*

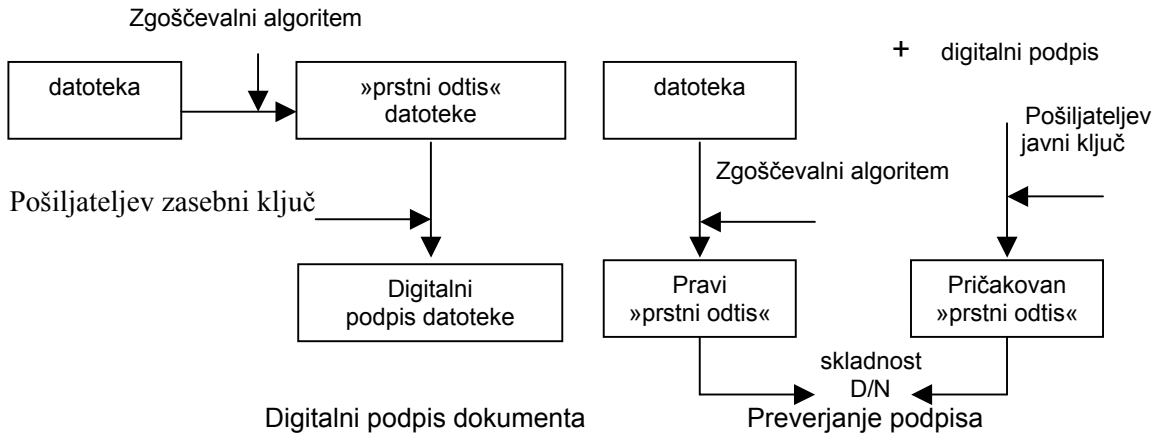
Nekaj znanih standardov digitalnega podpisa: (Lopez, February 2002, str. 46)
- RSA definiran v ANSI X9.31 Part 1 (ISO 9796) ali PKCS 1,
- DSS definiran v ANSI X9.30 Part 1 in NIST FIPS PUB 186-2,
- eliptična krivulja DSA (ECDSA) definiran v ANSI X9.62.

Preverjanje avtentičnosti
Preverjanje avtentičnosti zagotavlja pravica pristopa k zapisom in drugim virom ter jo določa nadzor dostopa, ki je kombinacija identifikacije s potrdili in seznam za nadzor dostopa (ACL).

Preverjanje enot
21 CFR Part 11 definira preverjanje enot v smislu ugotavljanja avtentičnosti strežnika, preverjanje vira podatkov ali operativnih navodil. Za izvedbo kateregakoli od teh preverjanj se lahko uporabi digitalni certifikat. Za preverjanje enot, vključenih v infrastrukturo javnega ključa (PKI), se lahko uporabi zapis in podpis e-CRFs v obliki uporabe inteligentnih kartic ali žetonov.

Povezovanje podpis-zapis
Elektronske podpise varujemo z varnostnim šifriranjem, ki onemogoča kopiranje, rezanje in lepljenje podpisov ali zgodovine dogodkov za že potrjene zapise. Ta zahteva pomaga izpolniti ***celovitost*** (zahteva 21 CFR Part 11 - §11.70, gl. povezava podpis-zapis) digitalno podpisanih zapisov. Upoštevati je treba, da sta celovitost in varnost glavni značilnosti digitalnih podpisov. Zaupanje uporabnika do povezave javnega ključa in njegovega lastnika je močno odvisno od tega, kakšno je uporabnikovo zaupanje v sistem, ki izdaja te certifikate. Poleg certifikatov, tehnologije kontrole dostopa in postopkov za povezave podpis-zapis imamo podporna orodja za preverjanje celovitosti teh povezav. Infrastruktura javnega ključa (PKI) uporablja zgoščevalni algoritem in ključe, ki demonstrirajo celovitost podpisanih zapisov. Povezava podpis-zapis je hranjena tako dolgo kot zapis, s tem zagotovimo verodostojnost elektronsko podpisanih zapisov za to časovno obdobje. (Lopez, March 2002, str. 56)

Slika 5: Prikaz izvedbe digitalnega podpisa dokumenta in preverjanje podpisa



Vir: R. D. McDowall, 2001, str. 2

Za tiste sisteme, ki vsebujejo uporabniško identifikacijsko kodo (ID[33]) in gesla kot elektronske podpise, trenutna raven tehnologije ne omogoča enostavne uporabe povezave podpis-zapis glede na sekcijo §11.70 v 21 CFR Part 11 in je posledično verodostojnost takšnih podpisanih zapisov lahko ogrožena. Skladnosti z zahtevami sekcije 11.200(a)(2), 11.200(a)(3) in 11.300(d) v 21 CFR Part 11 ne moremo zagotoviti v dikciji: (Lopez, marec 2002, str. 56)
»Kombinacija avtentičnih shem, kot so gesla, biometrične metode, avtentičnost na osnovi fizikalnih lastnostih, postopki obnašanja in žetoni morajo skupaj s kriptografskimi tehnikami zagotoviti avtentičnost povezave podpis-zapis.«

Originalnost elektronskih podpisov
Glavni element podpisanega zapisa in sporočila v digitalnem podpisu je zasebni ključ. V infrastrukturi javnega ključa (PKI) sta para ključev izvedena z izvirnimi števili, ki se ustvarijo iz naključnih številk. Tehniko generatorja ključa definira standard ANSI X9.17. (ANSI X9.17, 2002, 5 str.) Zasebni ključ je enkratno povezan z entiteto in ni narejen javno.

Zaščita elektronskih podpisov
Pri izvedbi digitalnih podpisov nekdo skrbi za celovitost in varnost komponent infrastrukture javnega ključa (PKI). Javni ključ je zaščiten pred nepooblaščenimi spremembami in zamenjavami znotraj kriptografskega modula, ki je del sistema ali programa, ki zagotavlja kriptografski servis, kot so šifriranje, overjanje, generiranje elektronskega podpisa in verifikacije. Zasebni ključ in izjava o uporabi certifikata sta prav tako zaščitena pred nepooblaščenim razkritjem, spreminjanjem ali zamenjavo.

Zasebni ključ je lahko shranjen v uporabnikovem lokalnem disku v šifrirnem formatu ali je del žetona, ki je povezan z računalnikom. Kot zahteva 21 CFR Part 11, se morajo žetoni testirati periodično, da zagotovimo njihovo ustrezno delovanje in potrdimo, da niso bili spremenjeni na neavtoriziran način. (zahteva 21 CFR Part 11 - §11.300 (e), gl. testiranje naprav)

Kvalifikacija
Funkcionalnost kriptografskih modulov lahko preverjamo s testi, ki jih izvajajo v neodvisnih in akreditiranih testnih laboratorijih.

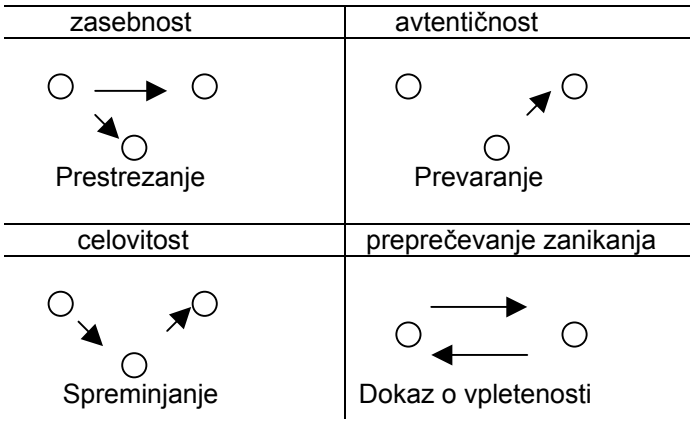
Zgodovina dogodkov
Zgodovina dogodkov je prav tako računalniško generirana in je lahko del zapisa ali zapis sam. Kombinacija avtentičnosti, potrdila, tajnopisa in seznama kontrole dostopa zagotavlja mehanizme za kontrolo dostopa do datotek zgodovine dogodkov. Sledilni mehanizem vsebuje računalniško generirano časovno žigosanje; datum in čas sta sinhronizirana z zaupanja vrednim servisom (npr. http://www.datum.com/tt). Nadzor zgodovine dogodkov vsebuje povezavo zapis-pregled, dostop je omejen samo na funkcijo branja ali izpisa. (Part 11-§11.10 (e), gl. zgodovina dogodkov)

3.8.1.2. Varnost

Ključni namen 21 CFR Part 11 je ustvariti verodostojne, zaupanja vredne elektronske zapise.

---
33 ID - angl. ***Id****entification Code*

Slika 6: Različne varnostne razmere, ki se pojavijo v digitalnem svetu



Lastnosti teh zapisov so:
zasebnost ali zaupnost (varnostne informacije)

avtentičnost ali pristnost (potrjena identiteta)

celovitost ali neokrnjenost (informacijska celovitost)

preprečevanje zanikanja (dokaz o vpletenosti)

Vir: Lopez, February 2002, str. 40.

Varnostne zahteve za posamezne atribute: (McDowall, 2001, str. 1)

1. *Zasebnost* - Določene informacije ne smejo biti razkrite nepooblaščenim subjektom.

2. *Avtentičnost* - Vsak mora imeti možnost preveriti identiteto subjektov, katerimi komunicira in izvor podatkov.

3. *Celovitost* - Podatki morajo biti zaščiteni pred nepooblaščenim spreminjanjem.

4. *Preprečevanje zanikanja*
   - Z gotovostjo vemo, da pošiljatelj ali podpisnik sporočila pozneje ne more zanikati pošiljanja ali podpisovanja dokumenta in prejemnik ne more zanikati prejetja sporočila. (National Archives and Record Administration, 2000, str. 15)

Tabela 3: Prikaz rešitve zahtev posameznih varnostnih atributov za papirni in elektronski zapis

Pogoj	Rešitev za papirni zapis	Rešitev za elektronski zapis
Zasebnost	pisemska ovojnica	podatkovni tajnopis
Avtentičnost	notarstvo, močan ID, fizična prisotnost	digitalni podpisi, digitalni certifikati
Verodostojnost	podpisi, vodni znaki, bar kode	zgoščevalni algoritmi, sporočila s »prstnim odtisom«, digitalni podpisi
Nezatajljivost	podpisi, prejemnice, potrditve	digitalni podpisi, zgodovina dogodkov

Vir: Lopez, February 2002, str. 40

Pri prehajanju podjetja na e-poslovanje je uvajanje rešitev z uporabo elektronskih tehnologij vitalnega pomena za zanesljivo in učinkovito doseganje varnostnih lastnosti zapisa.

Tabela 4: Priporočila GAMP *, ki se nanašajo na varnost računalniških virov

Varnostna priporočila in kontrole, ki so ključni element 21 CFR Part 11		
Part 11	*Opis*	*tehnološka kontrola v skladu z GAMP**
§11.10 c	zaščita zapisov	Sistem naj bi bil sposoben vzdrževati elektronske podatke za obdobje več let, ne glede na nadgradnjo programskega ali operacijskega sistema.
§11.10(d) §11.10(d)	kontrola dostopa avtentičnost	Sistem naj bi omejeval dostop in deloval v skladu z redno vzdrževanimi predpisanimi pravili. Vsaka sprememba pravil mora biti zapisana.
§11.10(e)	kontrola zgodovine dogodkov	Sistem naj bi bil sposoben zapisati vsako ustvarjanje elektronskih zapisov, dodajanje ali brisanje. Zapis naj bi bil varen pred morebitnimi nepooblaščenimi spremembami.
§11.10(e)	kontrola računalniškega sistemskega časa	/
§11.10(g)	kontrola odobritve	Sistem naj bi omejeval uporabo sistemskih funkcij in deloval v skladu s predpisanimi pravili vzdrževanja. Vsaka sprememba pravil mora biti zapisana.
§11.10(h)	preverjanje naprav	Ko farmacevtske organizacije zahtevajo, da določene naprave delujejo kot viri podatkov ali ukazov, mora sistem to funkcionalnost uveljaviti.
§11.30	tehnični nadzor odprtih sistemov	Ni del GAMP.
§11.70	povezava podpis-zapis	Sistem mora zagotoviti metodo, ki poveže uporabljeni podpis z ustreznim zapisom tako, da prepreči namero za ponareditev zapisov z odstranitvijo, kopiranjem ali spremembo podpisa.
§11.100(a)	edinstvenost elektr varnost e-podpisa podpisa	Sistem mora uveljaviti edinstvenost, zaščititi prestavitev e-podpisa ter preprečiti brisanje informacij, ki se nanašajo na elektronski podpis, ko je bil ta enkrat že uporabljen.
§11.300	varnost e-podpisa	Sistem naj bi bil sposoben identificirati spremembe na e-zapisih, zaznati neveljavne in spremenjene zapise.

*GAMP Special Interest Group, "Good Practice and Compliance for Electronic Records and Signatures, Part 2, Complying with 21 CFR Part 11, Electronic Records and Electronic Signature"

Vir: Lopez, marec 2002, str. 50

FDA govori o varnosti računalniških zapisov v svoji regulativi tekoče dobre proizvodne prakse (cGMP) s pridruženo politiko smernic, podrobno v sekciji 21 CFR §211.68(b) (FDA 21, 1996, str 15) in v novejših navodilih za industrijo (Guidance for Industry, 1999, str. 9), v katerih zahtevajo ustrezen nadzor računalniških virov, s katerimi zagotovimo, da samo pooblaščeno osebje izvaja glavne spremembe v proizvodnji, kontroli in upravljanju z zapisi.

3.8.1.3. Zgodovina dogodkov

Zgodovina dogodkov je varnostni, računalniško proizveden in časovno zapisan elektronski zapis, pri katerem lahko rekonstruiramo vzrok nastanka elektronskih zapisov glede na, njihovo spreminjanje ali brisanje. Zgodovino dogodkov obravnavamo kot meta podatek.

a. Pri spremembi podatkov, ki so hranjeni na elektronskem mediju, je zgodovino dogodkov vedno treba ustvariti v skladu z 21 CFR 11.10(e). Zgodovina dogodkov je eden od postopkov za zaščito verodostojnosti, celovitosti in, kadar je potrebno, zaupnosti elektronskih zapisov. (Guidance for Industry, 1999, str. 6-7)

   - Uporabljati moramo varno, računalniško proizvedeno, časovno žigosano zgodovino dogodkov s samodejnim zapisom datuma in ure nastanka, spreminjanja ali brisanja elektronskega zapisa. Zapis v zgodovino dogodkov je narejen, ko se shrani na trajen medij.
   - Zgodovino dogodkov moramo ohraniti za tako dolgo obdobje, kot je zahtevano za elektronske zapise. FDA mora biti zgodovina dogodkov dostopna za pregled in kopiranje.

b. Osebju, ki ustvarja, spreminja ali briše elektronske zapise, mora biti onemogočeno spreminjati zgodovino dogodkov.
c. Inšpektorji lahko zadržijo originalno ali overjeno kopijo zgodovine dogodkov.
d. Osebju FDA mora biti omogočeno branje zgodovine dogodkov na mestu nastanka zapisov ali na katerikoli drugi lokaciji, kjer pripadajoče elektronske zapise hranijo.
e. Zgodovina dogodkov mora biti ustvarjena v časovnem zaporedju, kronološko in na način, ki ne dovoli, da bi se nova informacija prepisala preko obstoječih podatkov.

S pomočjo časovnega žiga lahko označimo ali preverimo obstoj podatkov v elektronski obliki v določenem času. (Pavliha, Bogataj, et al., 2002, str. 33) Jasno je definirana vsebina zgodovine dogodkov, npr.: datum, čas, tiskano ime posameznika, ki je izvedel spremembo, staro stanje in novo stanje.

3.8.1.4. Elektronski podpisi

Zahteve 21 CFR Part 11 natančno določajo uporabo, upravljanje in sestavo elektronskih podpisov.
»Elektronski podpis predstavljajo računalniški podatki, sestavljeni iz poljubnih simbolov ali niza simbolov, ki je izveden, prevzet, overjen in zakonsko vezan na posameznika ter kot takšen enakovreden ročnemu podpisu«. (Code of Federal Regulations, 1997, str. 10)

Obstajati mora napisana politika, ki zagotavlja, da se bo posameznik zavedal in bil odgovoren za aktivnosti, povezane z elektronskimi podpisi. Elektronski podpisi morajo biti edinstveni, ne smejo biti ponovno dodeljeni ali ponovno uporabljeni. Identiteta posameznika, ki prejme elektronski podpis, mora biti nedvoumno preverjena. Če je bil sistem v uporabi pred vpeljavo skladnosti z 21 CFR Part 11, se morajo vse identifikacijske kode uporabnika in gesla ponovno dodeliti v skladu z zahtevami 21 CFR Part 11. Podpisani elektronski zapisi morajo poleg imena, datuma in časa podpisa vsebovati tudi opis namena. Datumsko in časovno značko mora sistem dodati avtomatsko.

a) Elektronski podpis z nebiometrično metodo

Nebiometrični elektronski podpisi so definirani kot metoda za identifikacijo posameznikove identitete in so osnovani na najmanj dveh različnih identifikacijskih sestavnih delih, kot sta identifikacijska koda (t. i.uporabniško ime) in geslo.

Uporabniško ime je lahko znano. Kombinacija uporabnikove identifikacijske kode in gesla je lahko znana edino lastniku in mora biti edinstvena. Izvedene morajo biti proceduralne kontrole, s katerimi zagotovimo, da elektronske podpise uporabljajo samo pristni lastniki in jih ne delijo, posojajo ali prenašajo. Pri izvedbi nebiometričnega elektronska podpisa sodeluje le uporabnik sam.

Uporabniške identifikacijske kode in statično geslo

Statična gesla so še vedno najcenejši in najširše uporabljani mehanizmi overjanja. Danes večina sistemov ponuja najmanj osnovni sistem za upravljanje z gesli z naslednjimi značilnostmi: (Lopez, marec 2002, str. 52)

- staranje gesel in zapadlost: dovoljuje geslom življenjski cikel, po izteku mora biti geslo spremenjeno;
- zgodovina gesel: preverjanje novega gesla, da to ni ponovno uporabljeno, definirano je tudi število sprememb gesel;
- blokiranje dostopa: po določenem številu neuspešnih poskusov vnosa gesla sistem avtomatsko blokira uporabniku dostop do sistema: časovno ali dokler administrator uporabniškega računa ne sprosti;
- preverjanje zapletenosti gesel: s tem zagotovimo sprejemljivo zaščito proti vsiljivcem, ki želijo vdreti v sistem z ugibanjem gesel.

Uporabniške identifikacijske kode in dinamično geslo

Gesla in osebne identifikacijske številke se uporabljajo za potrjevanje avtentičnosti. Kadar so združeni še z drugimi metodami, z njimi zagotovimo večji pomen overjanja. Kombinacija vsebuje nekaj, kar oseba pozna (gesla, osebna identifikacijska številka), in nekaj, kar oseba poseduje (žetone). Obstajajo programski in strojni mehanizmi, ki zagotavljajo povezavo z drugim delom informacije.

b) Elektronski podpis z biometrično metodo

Biometrični elektronski podpisi so definirani kot "metoda ali identifikacija osebe na podlagi meritve posameznikovih bioloških značilnosti ali ponavljajočih se akcij. Te značilnosti in/ali akcije so svojstvene posamezniku in so merljive". (Code of Federal Regulations, 1997, str. 10) Biometrični elektronski podpisi morajo biti načrtovani tako, da jih lahko uporablja samo pravi lastnik.

c) Kontrole podpisa

Kontrole za identifikacijo kod in gesel za sisteme z elektronskim podpisom so definirane v sekciji §11.300. Uporabimo takšne tehnične ukrepe, da zagotovimo, da niti dva posameznika nikoli ne bosta uporabljala enake kombinacije uporabniške identifikacijske kode in gesla. Postavimo kontrole za periodično preverjanje, odpoklice ali pregled izdajanja identifikacijske kode uporabnika in gesla. Uporabnikov dostop oziroma kode uporabnika in/ali gesla morajo biti onemogočeni takoj, ko jih ne potrebujemo več. Zahtevano trajanje oziroma frekvenca spremembe gesel mora biti določena z dokumentirano politiko in postopki, zlasti če se to na sistemu ne izvaja samodejno. Postopki ukrepanja v primeru zlorab gesel morajo biti jasno dokumentirani in se ob dogodku takoj aktivirati. Kontrole morajo imeti vlogo zaščite,

zaznave in poročanja o poskusih nepooblaščene uporabe gesel in identifikacijskih kod uporabnikov. Obstajati morajo tehnična in proceduralna jamstva za zaščito uporabniških identifikacijskih kod in gesel pred nepooblaščeno uporabo. Nepooblaščeni poskusi morajo biti zaznani takoj (v realnem času). Pomen vdora mora biti opredeljen z analizo tveganja. Od pomena je odvisno, ali je treba vodstvo obvestiti o vdoru.

Naprave, ki omogočajo funkcionalnost elektronskega podpisa, moramo periodično pregledovati, da zagotovimo ustrezne lastnosti in jih zaščitimo pred nepooblaščenimi spremembami in izrabo (dotrajanost).

Dodatne kontrole niso nič manj pomembne kot tiste, ki so dokumentirane v sekciji §11.10 in določajo trdno osnovo za varnost sistemov, ki vključujejo elektronske podpise.

d) Proglasitev elektronskega podpisa

V sekciji §11.100(c) 21 CFR Part 11 je zahtevano, da morajo organizacije, ki uporabljajo elektronske podpise, skladne z zahtevami FDA, v primeru uporabe le-teh o tem obvestiti FDA. S tem obvestijo agencijo, da je zanje elektronski podpis enakovreden ročnemu podpisu.

3.8.2. Nestandardni elementi modela

3.8.2.1. Spremembe

Zanimajo nas spremembe računalniških sistemov v njihovem celotnem življenjskem ciklu in spremembe na elektronskih zapisih.

Vse spremembe v zapisih morajo biti izvedene tako, da ne spremenijo originalne informacije. Na spremenjenem zapisu mora biti jasno razvidno, da je bila sprememba narejena; zagotoviti moramo popolno dosegljivost predhodne informacije. Postopki za vnos spremembe se prav tako obravnavajo in vodijo po splošnih postopkih za zagotavljanje kakovosti. Programske posodobitve, zamenjave naprav ali sestavnih delov nove programske opreme uvajamo v skladu z napisanimi protokoli, tako da vzdržujemo celovitost podatkov in postopkov.

Spremembe v fazi delovanja in vzdrževanja računalniškega sistema so legitimne in so v modelu predvidene. Dopuščajo, da sistem v okviru standardnih elementov modela nenehno sledi zahtevam okolja oziroma odpravlja njegova neskladja z ugotovljenimi dejstvi oziroma odstopi.

Vsako spremembo v sistemu je treba pretehtati. Z revalidacijo sistema pa ponovimo tisti segment validacije, pri katerem se sprememba uvaja. Slednjo izvedemo pri spremembah, ki presegajo operativne meje ali limite v specifikaciji načrtovanja, pri čemer je treba vse na sistemu izvedene aktivnosti celovito dokumentirati.

Revalidacija, ki se nanaša na programske spremembe, pomeni validacijo spremembe same. Vrednotimo naravo spremembe in definiramo morebitni učinek »valovanja« (odziv sistema na motnjo oziroma na izvedeno spremembo) ter izvedbo

potrebnih obnovitvenih testov (t. i. regresijskih), s katerimi potrdimo nespremenjene in nove funkcionalnosti sistema. (Webster's, 1997, str. 53)

3.8.2.2. Procesi

Teorija zanesljivosti pravi, da se pred napakami oziroma odstopi v kompleksnih, visoko tehnoloških procesih lahko zaščitimo z dobro organiziranim načrtovanjem in vodenjem. Takšni sistemi morajo zagotavljati skupno predanost sistemu varnosti, zadostno število osebja, nadzor varnosti, strogo organizacijsko strukturo in ljudi, ki sproti osvajajo novo znanje in so pripravljeni na spremembe.

Čeprav se odstopi dogajajo, so sistemi načrtovani z namenom, da postanejo vse bolj zanesljivi in da postanejo napake z leti prej izjema kot pravilo.

Varnost oziroma zanesljivost ni odvisna samo od oseb, naprav ali oddelkov, temveč se pojavi z interakcijo sestavnih delov sistema. Varnost je relativna, saj se neprestano dopolnjuje; ko tveganja postanejo znana, postanejo del varnostnih zahtev.

Zanesljivost je več kot le odsotnost napak. Ima večkratno dimenzijo in zajema:

- kompleksen pogled, prepoznaven kot skrb za skladnost, zaznavanje tveganj in iskanje rešitev v širokem sistemskem kontekstu;
- predstavlja niz postopkov, s katerimi določimo nepravilnosti in zmanjšujemo možnost naključij; postopke nenehno dopolnjujemo in izboljšujemo;
- analiziranje odstopov in zmanjševanje njihova tveganja.

V varnen, stabilnem in predvidljivem okolju procesov se zmanjša tveganje za nastanek napak oziroma odstopov.

3.8.2.2.1. Neskladnost sistemov

Odstopi, ki pomenijo določeno stopnjo neskladnosti, se največkrat zgodijo v določenih delih sistema. Ko se pojavijo, so znak napake v načrtovanju sistema. Ravno s sistemskim načrtovanjem bi morali primarno preprečevati pojav napak in, če se že pojavijo, poskrbeti, da je nastala škoda minimalna.

Sisteme označujemo z dvema pomembnima lastnostma (Perrow, 1984, str. 100): kompleksnostjo in povezanostjo. Sistemi, ki so bolj kompleksni in tesno povezani, so bolj nagnjeni k napakam in morajo biti narejeni bolj zanesljivo. Taki sistemi imajo mnogo sestavnih delov, ki so med seboj povezani. Težava nastane, kadar en del opravlja različne funkcije. Če ta izpade, po sistemu domin prav tako izpadejo vse odvisne funkcije .

Kompleksni sistemi so označeni kot specializirani, medsebojno povezani in imajo težnjo za večkratnimi povratnimi zankami. Informacije sprejemajo posredno, tako je zaradi velike specializiranosti majhna možnost hitrih zamenjav, preimenovanja osebja ali drugih virov.

V nasprotju s kompleksnimi sistemi linearni sistemi s pričakovanim medsebojnim delovanjem delujejo v običajnih in znanih zaporedjih. Linearni sistemi težijo k ločevanju v podsisteme, manjše povratne zanke in enostavne zamenjave. Napaka na enem delu sistema lahko nepričakovano prekine drugi del in vsi povezani procesi, na katere lahko vpliva dogodek, niso več obvladljivi. Kompleksnost je torej prav tako vzrok, da morajo biti morebitne spremembe na teh sistemih potrjene in premišljene.

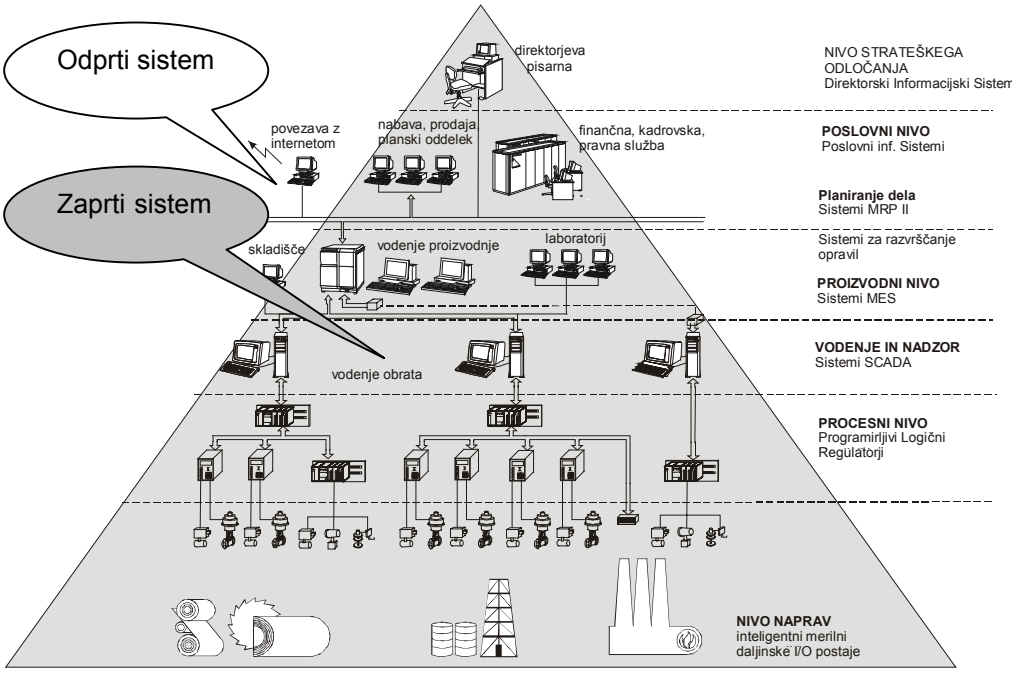
Pri presojah ali inšpekcijah so naloge porazdeljene, zato mnogo soodvisnih in vplivnih povezav, ki so kritične za proces presoje, ne bomo prepoznali, dokler se ne pojavi sprememba ali odstop.

Povezava je mehanski pojem; med entitetama je povezava lahko tesna, šibka ali pa nevtralna. Veliki sistemi, ki so tesno povezani, imajo več med sabo časovno odvisnih podsistemov in določena zaporedja. pri njih vedno obstaja samo ena pot za dosego cilja. Nasprotno pa šibko povezan sistem lahko dopušča procesno zakasnitev, tako lahko ponovno zahteva določena zaporedja ter lahko uporabi alternativne metode in vire.

Kompleksna interakcija povzroča napake, kar zmede skrbnike sistemov. Pri veliki kompleksnosti in povezanosti lahko majhne napake prerastejo v velike odstope. Sistemi, ki so bolj kompleksni in tesneje povezani, so bolj nagnjeni k napakam. Vendar pri njih lahko zmanjšamo verjetnost odstopov in jih naredimo zanesljivejše, in sicer s poenostavitvijo in standardizacijo procesov (npr. enoten, pregleden model), zagotovitvijo prekrivanja znanja zaposlenih (npr. osebje, ki se lahko nadomešča v zagovorih) in razvojem podpornih sistemov (npr. »problemska matrika« inšpekcije).

3.8.2.2.2. Računalniški in informacijski sistemi

Slika 7: Arhitektura informacijskega sistema v farmacevtskem podjetju



Vir: Informacijski sistemi v proizvodnih podjetjih, 2000, str. 2

Farmacevtsko podjetje mora imeti pravočasen dostop do ažurnih in zanesljivih informacij, saj je to eden od ključnih pogojev za celovito obvladovanje fizičnih, proizvodnih in poslovnih procesov ter odločanje na osnovi dejanskih podatkov o stanju v procesih podjetja. Integrirani računalniški in informacijski sistemi odražajo vso specifičnost tehnologije in organizacije dela posameznega podjetja. Ključno vlogo pri vsebinskem razvoju sistemov mora imeti uporabnik sam.

Tabela 5: Osnovna računalniška orodja na posameznih ravneh podjetja

Poslovna raven	Informacijski sistemi za načrtovanje virov podjetja (ERP[34]) informacije procesirajo v daljšem časovnem obdobju (v dnevih, tednih ali mesecih).
	Informacijski sistemi za načrtovanje proizvodnih virov (MRPII[35]).
Proizvodna raven	Računalniški sistemi za podporo razporejanja opravil.
	Računalniški sistemi za upravljanje proizvodnje (MES[36]) omogočajo dostop do informacij o proizvodnih operacijah in virih ter odločanje na osnovi le-teh.
Nadzorna raven	Računalniški sistemi za nadzor in vodenje (SCADA[37])so bili prvotno zasnovani za razvoj programov za spremljanje in vizualizacijo procesa; v novejšem času se nadgrajujejo s proizvodnimi funkcijami.
Procesna raven	Računalniške enote za avtomatsko vodenje (PLC,MLC,RTU[38]).

Vir: Informacijski sistemi v proizvodnih podjetjih, 2000, str. 2

Razvoj poslovnih informacijskih sistemov je potekal neodvisno od razvoja sistemov na nadzorni in procesni ravni, zato še danes ni dosežena popolna integracija obeh v skladno celoto. Vrzel v komunikaciji med transakcijsko orientiranimi sistemi za načrtovanje in sistemi za vodenje v realnem času povzroča probleme predvsem v primeru odstopanj med dejanskim in načrtovanim potekom dela. Računalniški sistemi za upravljanje proizvodnje, ki delujejo kot vmesnik med sistemi načrtovanja in vodenja proizvodnje, so se pojavili kot rezultat potrebe po koordinaciji proizvodnih in poslovnih funkcij podjetja.

V sklopu validacije računalniških sistemov obravnavamo računalniške in informacijske sisteme na poslovni, proizvodni, nadzorni in procesni ravni, kjer so močno prisotne tudi regulatorne zahteve 21 CFR Part 11. Z integracijo poslovnih procesov, informacijskih sistemov in sistemov vodenja znotraj podjetij se pojem varnega elektronskega poslovanja vse bolj vpeljuje tudi na poslovni ravni v okviru nacionalne zakonodaje.
Posamezni računalniški ali informacijski sistem se v izdelanem odločitvenem modelu uvede kot varianta odločitvene analize.

34 ERP - angl. ***E**nterprise **R**esource **P**lanning*

35 MRPII - angl. ***M**anufacturing **R**esource **P**lanning*

36 MES - angl. ***M**anufacturing **E**xecution **S**ystems*

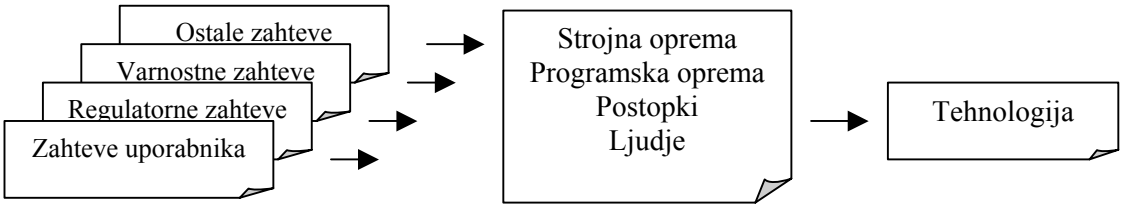
37 SCADA - angl. ***S**upervisory **C**ontrol **a**nd Data Acquisition*

38 PLC,MLC,RTU - angl. *Programmable Logic Controllers, Multi-Loop Controllers, Remote Terminal Units*

3.8.2.3. Tehnologija

Tehnologijo sestavljajo načini in sredstva, ki jih uporablja človeštvo, da preživi v svojem okolju in to okolje nadzira ter spreminja.

Slika 8: Elementi, ki določijo izbiro ustrezne tehnologije



Vir: Lopez, 2001, str. 23

3.8.2.3.1. Napake v tehnologiji

Tehnologija si zasluži vso pozornost. Napake, ki se lahko pojavijo med načrtovanjem skladnosti sistemov, se pozneje pokažejo kot odstop v samem procesu. Kljub dobrim odločitvam za varno in učinkovito zagotavljanje kakovosti to ni dovolj. Treba je imeti pravo opremo, dobro in zanesljivo vzdrževanje, strokovno in izobraženo osebje, odgovoren delovni načrt, optimalno načrtovana delovna mesta in jasna navodila. Ti dejavniki so znanilci ali temeljni pogoj za učinkovito zagotavljanje skladnosti računalniških sistemov.

Pomanjkanje temeljnih pogojev lahko prispeva k večjemu številu neustreznih izdelkov in celo odpoklicu zdravil s trga. Nezadostno izobraževanje, velika delovna obremenitev in časovni pritisk povzročijo neprimerno zaznavanje nepravilnih situacij ter težave z motiviranostjo. Pri načrtovanju varnega sistema moramo upoštevati človekove psihološke meje in iskati poti za omilitev njihovega vpliva. Okolje, oprema, njena uporaba, operativni postopki in delovna razporeditev so dejavniki v proizvodnem procesu, ki jih moramo upoštevati pri načrtovanju doseganja zanesljivosti sistema.

Pojav človeških napak ustvarja dojemanje, da je človek nezanesljiv in neučinkovit. Če nezanesljiva oseba naredi napako, se sistem običajno osredotoči na to osebo, da se napaka ne bi ponovila. Vendar je pravi odgovor pravilna uporaba določenih tehnologij, saj s tem odstranimo priložnost, da bi ljudje napake naredili. Z naraščanjem razvoja tehnologije so tudi sistemi postali kompleksnejši. Zaradi tehnologije se spreminja narava dela, ljudem se spreminjajo delovne obremenitve, zmanjšuje se neposredna vloga človeških odločitev. Proces, ki je avtomatiziran, je za neposrednega uporabnika manj pregleden, kajti posrednik med osebjem in okoljem so stroji. Neposredne informacije so filtrirane (računalniški algoritmi), zato je tveganje, da je osebje zasuto z goro informacij ali da sploh ne dobi prave informacije, veliko.

Razdelitev, pri kateri so posamezna dela razdeljena med nekaj ljudi, lahko vpliva na sposobnost odkrivanja in odpravljanja napak.

3.8.2.3.2. Ljudje in človeški faktor

Raziskave o vplivu človeškega faktorja izhajajo s področja industrijskega inženiringa in psihologije človeka. Človeški faktor je obravnavan v okviru medsebojnih povezav med ljudmi, orodji, ki jih uporabljajo, in okolja, v katerem ljudje živijo in delajo. (Weinger, Pantiskas, et al., 1998)

Pristop želimo uporabiti za razumevanje, kje in zakaj sistem ali proces odpove in kaj povzroči odstop. Raziskujemo nastanek napak, analiziramo njihove vzroke, okoliščine, pogoje za nastanek, postopke, naprave in druge dejavnike, povezane z tem dogodkom.

Poznavanje človeških lastnosti lahko vodi v ustvarjanje učinkovitih varnostnih sistemov. S tem preprečimo pogoje oziroma se izogibamo okoliščinam, ki vodijo v napake. Vsi odstopi niso povezani s človeškim faktorjem.V primeru napak na napravi ali materialu le-ta nima neposrednega vpliva.

Pri obravnavanju človeškega faktorja je večina dela in naporov vloženih v izboljšanje komunikacijskega vmesnika »človek-sistem«, in sicer z načrtovanjem boljših sistemov in procesov.
V analizi človeških faktorjev uporabljajo dva pristopa:

1. Prvi je kritična analiza odstopov. Raziskovalci proučujejo značilne in osrednje dogodke, da bi lažje razumeli, kje je sistem popustil, zakaj se je odstop zgodil in kakšne so bile okoliščine. Kritična analiza odstopov tako v primeru, ko dogodek vodi k slabemu izidu kot kadar ne, zagotavlja razumevanje pogojev, ki so povzročili napako ali tveganje za njen nastanek.

2. Drugi analitični pristop je prikazan kot "*naravne odločitve*". (Klein, 1998, str. 4) Raziskovalci preiskujejo človeške odločitve pri naravnih delovnih zadolžitvah. Pri tem upoštevajo vse tipične dejavnike, kot so časovne omejitve, psihični pritisk, nezadostne informacije, nasprotujoči si cilji, hrup ali druge motnje, in jih znanstveno kontrolirajo. Pri tej metodi gredo ljudje, npr. skrbniki sistemov, skozi mnoge namišljene situacije. Z analizo odkrijejo pomembna dejstva in nepravilnosti. Izsledke uporabijo v procesu odločanja, vodenja ali upravljanja s sistemi in pri ravnanju ob soočanju z dvoumnimi informacijami pod časovnim pritiskom.

S poročanjem o napakah ali drugimi oblikami določanja napak ugotavljajo, kje se napake pojavijo in kje je mogoče narediti spremembe oziroma izboljšave. Načrtovanje varnih in skladnih sistemov zagotavlja priložnost za inovacije in testiranje novih pristopov. Nenazadnje, širjenje inovacij in novih tehnologij po sistemu sprememb je osnovna smer bodočega razvoja.

3.8.2.3.3. Standardni postopki delovanja

Za obvladovanje posameznih področij mora imeti podjetje izdelane standardne postopke delovanja (*SOPs*), ki so prav tako sestavni del poznejše podrobne analize skladnosti.

Omenimo nekaj najpogostejših (Stotz, 2002, str. 14):
– postopki za delovanje računalniškega sistema in za odgovornost osebja;
– postopki za zagotavljanje varnosti, zaznavanje in preprečitev nepooblaščenih vstopov in sprememb programov;
– postopki in pooblastila za programske spremembe in zapise sprememb;
– postopki in pooblastila za menjavo opreme ter tudi testiranje njene primernosti;
– postopki za vzdrževanje računalniških sistemov in naprav;
– postopki za periodično testiranje ustreznega delovanja celotnega sistema in njegovih posameznih sestavin ter za zapisovanje teh testov;
– postopki za razvoj programske opreme, testov ustreznosti in njihov zapis;
– postopki za arhiviranje in načrtne aktivnosti ob dogodkih, ki porušijo podatkovno celovitost;
– postopki za opazovanje in pregled računalniških sistemov;
– postopki za upravljanje s konfiguracijami (nadzor sprememb, upravljanje z verzijami, nove izdaje in gradnja sistemov);
– postopki dela z izvornimi kodami;
– postopki sistema revalidacije,
– postopki v izobraževalnem procesu.

Pravila za vzdrževanje podatkovne celovitosti, dodeljevanje in uporabo elektronskih podpisov ter vzdrževanje zgodovine dogodkov morajo biti prav tako zapisana v standardnih postopkih delovanja (SOPs) podjetja.

3.8.2.4. Zahteve elektronskega arhiviranja – ohranitev zapisa

Farmacevtska industrija, ki je že davno spoznala prednosti ohranjanja razvojnih in proizvodnih podatkov, uporablja za dolgoročni zajem in hranjenje takšnih informacij posebne sisteme. S stalnim razvojem strojne opreme, programskih rešitev, sistemov za arhiviranje elektronskih podatkov in uvajanjem nove regulative postaja v prihodnosti zelo pomembno zagotoviti normalizacijo podatkov, uvesti enotne podatkovne formate, sisteme upravljanja znanja, razvijati standarde arhiviranja in sistem rudarjenja podatkov. (Smith, 2002,str. 48) Danes je znano, da se vsebina digitalnih nosilcev zgubi prej kot tisto na papirju.

Na začetku jasno definirajmo, kaj pojem elektronsko arhiviranje pomeni za 21 CFR Part 11. Pojma, kot sta “elektronsko arhiviranje” ali “zahteve dolgoročnega hranjenja”, v 21 CFR Part 11 nista uporabljena. Vendar je v odstavku A sekcije §11.3 elektronski zapis definiran kot:
»katerakoli kombinacija besedila, grafike, podatkov, zvočnih, slikovnih prikazov ali predstavitve drugih podatkov v digitalni obliki, ki nastane, se spreminja, ohranja, arhivira, prikliče ali razpošilja prek računalniškega sistema«. (Code of Federal Regulations,1997, str. 10)

V odstavku B sekcije §11.10 je zahtevana uporaba “postopkov in kontrol, načrtovanih za zagotovitev avtentičnosti in celovitosti … elektronskih zapisov“.

Definicije elektronskih zapisov in kontrolnih postopkov so lahko podane in razčlenjene v okviru različnih zahtev za elektronsko arhiviranje, ki opisujejo npr.:
- hranjenje elektronskih zapisov;

- hranjenje združenih meta podatkov, kot so integracijski parametri ali informacije zgodovine dogodkov, skupaj z elektronskimi zapisi;
- zaščito celovitosti elektronskih podpisov v celotnem obdobju hranjenje zapisov z ustrezno politiko in postopki;
- zaznavanje sprememb ali brisanje elektronskih zapisov ter dokumentiranje le-teh v zgodovini dogodkov;
- točnost in časovno obnovljivost zapisov ves čas trajanja predpisanega obdobja;
- izvedbo točnih, popolnih kopij elektronskih podpisov v človeško berljivi in elektronski obliki.

V regulativi 36 CFR 1234 (U.S. National, 2001, 11 str.) so zbrana natančnejša navodila glede zahtev pri elektronskem arhiviranju, in sicer:

- Predvideti moramo primerno raven varnosti, da zagotovimo celovitost dokumentov (*36 CFR 1234.22(a)(2)*).
- Elektronske zapise moramo hraniti v uporabnem formatu do preteka predpisanega datuma (*36 CFR 1234.30)(a)(3)*).
- Določiti je treba standardno izmenljiv format, ki je potreben, da zagotovimo izmenjavo dokumentov na elektronskem mediju med posameznimi računalniki, ki uporabljajo različne programske/operacijske sisteme, ter pretvorbe ali migracije dokumentov na elektronskem mediju z enega sistema na drugega (*36 CFR 1234.22(3)*).
- Osnovati moramo postopke pravilnega kopiranja, ponovnega oblikovanja ter druge potrebne vzdrževalne postopke, da zagotovimo ohranitev in uporabnost elektronskih zapisov v predpisanem življenjskem ciklu (*36 CFR 1234.32 (c)*).
- Zagotoviti moramo, da se pri spremembi tehnologije, zamenjavi spominskega medija in zagotavljanju skladnosti z obstoječo strojno in programsko opremo v podjetju informacije ne izgubijo ali poslabšajo.

Najbolj natančna navodila za elektronsko shranjevanje so podana v ameriškem obrambnem ministrstvu (Department of Defense 5015.2, 1997, str. 11):
Sprejeta načela elektronskega arhiviranja so:
- Elektronskih zapisov ni dovoljeno spreminjati, njihov format in vsebino je treba ohraniti v taki obliki, kot je bila shranjena.

- Za zanesljivost in avtentičnost elektronskih zapisov pri zajemanju in ponovnih vzpostavitvah moramo zagotoviti zapise v obliki poročil ali zgodovine dogodkov.

- Arhivske kopije elektronskih zapisov morajo biti vzdrževane in shranjene na ločenih lokacijah.

- Zagotoviti moramo, da so elektronski zapisi na ogled in da se lahko kopirajo in, če je potrebno, procesirajo tako dolgo, kot je zahtevana življenjska doba hranjenja zapisov. Tej zahtevi lahko ustreženo z vzdrževanjem strojne in programske opreme, uporabljene za ustvarjanje ali zajemanje elektronskih zapisov, z vzdrževanjem strojne in/ali programske sposobnosti za obdelavo zapisov v njihovem naravnem okolju, z ohranjanjem združljivosti, ko je strojna in/ali programska oprema nadgrajena, s selitvijo elektronskih zapisov v novi format, preden postane stari zastarel. Da zagotovimo zanesljivost elektronskih zapisov, mora biti vsaka migracija nadzirana.

3.8.2.5. Načela elektronskega arhiviranja

Pri elektronskem arhiviranju poznamo osem osnovnih načel, ki jih predstavljamo v nadaljevanju. (Dollar, 2000, str. 11)

3.8.2.5.1. Elektronski zapis z možnostjo procesiranja

S prvim načelom elektronskega arhiviranja vzdržujemo možnost obdelave elektronskih zapisov tako dolgo, kot je to potrebno. Te zapise lahko beremo, točno interpretiramo in upravljamo s trenutno strojno in programsko opremo. Z uporabo uvozno/izvozne funkcionalnosti jih lahko enostavno prestavimo na novo tehnološko platformo.

Pri elektronskih zapisih, ki jih lahko samo vidimo ali tiskamo, ne obstaja možnost procesiranja, kajti originalne programske funkcionalnosti, povezane z zapisi, ne moremo izvršiti. Ta možnost procesiranja je podobna zahtevi FDA o sposobnosti »play back« elektronskih zapisov za ponovitev analiz. Ti zapisi imajo sposobnost njihove enostavne pretvorbe na novo tehnološko platformo.

Običajno sta za dosego omenjenega cilja na voljo dve poti. Prva je ohranjanje združljivosti z obstoječimi programi, ki jih je izdelovalec vgradil v izdelek. Druga je uporaba javne, tako imenovane tehnologije nevtralne izmenjave podatkov. Ohranjanje združljivosti je učinkovita kratkoročna rešitev, vendar postane problematična, če se proizvajalec odloči, da ne bo podpiral nadaljnjega razvoj izdelka, in ustavi podporo uporabniku oziroma se želi prestaviti na popolnoma drugačno tehnološko platformo. Uporaba javne tehnologije nevtralne izmenjave podatkov je kritična, ko se vpeljuje nova tehnološka platforma.

3.8.2.5.2. Jasen elektronski zapis

Drugo načelo elektronskih zapisov z možnostjo procesiranja je, da morajo biti elektronski zapisi jasni za računalnik. Vsak današnji računalnik lahko prepozna dvojiški tok števil ("1" in "0"), proizveden z drugim računalnikom. Informacija iz niza binarnega toka nima pripadajoče vsebine, da bi jo računalnik lahko prepoznal in interpretiral z namenom procesiranja. Sama bitna mapa kot takšna ni razumljiva. Meta podatki, ki jih najdemo v glavah datotek, lahko vsebujejo informacije, kot so ureditev "bytov", uporabljeni algoritmi za združevanje, ki so bistveni za računalnikovo sposobnost interpretacije bitnega toka in njegov prikaz. Vsak namenski računalnik lahko prepozna dvojiški bitni tok izvornih podatkov, če je uporabljen format laboratorijskega podatkovnega sistema. Seveda je ta dvojiški bitni tok jasen samo programski opremi, ki zna interpretira ta uporabljeni format in ga lahko pripravi za pregledovanje, tiskanje, analizo in ponovno procesiranje.

3.8.2.5.3. Obnovljiv elektronski zapis

Obnovljivi elektronski zapisi so shranjeni za določeno časovno obdobje z namenom, da bomo imeli za poznejše konzultacije jasen informacijski vir, ki bo na voljo v čitljivi obliki v celotnem obdobju hranjenja. Tekstovne elektronske zapise rajši shranimo v datoteko, medtem ko številčne podatke raje shranimo v podatkovno bazo.

Elektronski zapis, shranjen v podatkovno bazo, je relativno lahko obnovljiv, ker je vanj avtomatsko vključena funkcionalnost indeksiranja pri ustvarjanju tabel.

3.8.2.5.4. Rekonstruiran elektronski zapis

Rekonstruiran elektronski zapis prikazuje enake fizikalne in logične lastnosti kot v času, ko je bil elektronski zapis shranjen na trajen spominski medij. Z drugimi besedami, rekonstruirani elektronski zapisi so popolnoma enaki tistim, ki so jih naredili njihovi tvorci. Poleg tega morajo rekonstruirani elektronski zapisi ohraniti vsako notranjo ali zunanjo lastnost, ki je bila zahtevana za celovitost in učinkovitost v času njihovega nastajanja ali začetne uporabe. To pomeni, na primer, da je, kadar je bilo zahtevano, da overita laboratorijsko analizo analitik in vodja preiskovalcev ter da se pridobi soglasje druge strani, ohranjena celovitost preverjanja overitve. Pri rekonstruiranih elektronskih zapisih mora obstajati sposobnost rekonstruiranja digitalnih podpisov za namen overitve tako dolgo, kot je zahtevana življenjska doba zapisa.

3.8.2.5.5. Razumljiv elektronski zapis

Razumljivi elektronski zapisi vključujejo okoliščine ali dejstva, ki soustvarjajo nastajanje, uporabo in vzdrževanje elektronskih zapisov z namenom omogočiti uporabnikom izluščiti njihov pomen. Pomen ali razumljivost zapisa ni determinirana izključno z njihovim tekstom ali številkami, temveč tudi v kontekstu nastajanja in uporabe. Ključni element za razumljive elektronske zapise je njihova relacija z drugimi elektronskimi zapisi v času ustvarjanja, uporabe in ohranitve. Tipične so referenčne kode, nazivi map, ki lahko identificirajo ta razmerja. V vsakem primeru je informacija, ki definira medsebojno zvezo, meta podatek, za katerega moramo skrbeti in ga ščititi enako kot sam elektronski zapis.

3.8.2.5.6. Nespremenjen elektronski zapis

Pojem nespremenjen elektronski zapis označuje zapise, ki niso namerno ali naključno izpostavljeni spremembam, predelavi, izgubi ali popačenosti po njihovem zapisu na trajen medij. Nespremenjeni elektronski zapisi so zanesljivi in zaupanja vredni; sporočajo nam dejstva, ideje, dogodke. Zaščita elektronskih zapisov pred spremembami je velik izziv, ker jih je sorazmerno lahko spreminjati, ne da bi puščali vidne sledi. Tako načrtovani kot naključni prenos elektronskega zapisa na nov spominski medij ali pretvorba na novo tehnološko platformo predstavljata tveganje, da se bodo podatki popačili in izgubili.
Za obrambo pred spremembami in brisanjem elektronskih zapisov moramo najprej poskrbeti ob njihovem prenosu z mesta, kjer so pod skrbništvom in nadzorom nastali, se uporabljali in bili vzdrževani, v spominsko enciklopedijo. Tam zanje skrbi zaupanja vredna tretja stran, ki uporablja najboljšo arhivsko prakso in zaščito zapisov pred spremembami, brisanjem in popačenjem. Spominska enciklopedija potem, ko je elektronski zapis enkrat shranjen na trajnem mediju, zagotavlja samo »bralni dostop«. Če s poznejšo analizo odkrijemo napako ali če uporabimo novo tehniko, je treba narediti kopijo zapisa in jo ustrezno nadgraditi. Ta nadgrajeni zapis je shranjen na trajnem mediju kot nova verzija.

Drugi način zaščite pred spremembo vsebine elektronskega zapisa je uporaba digitalne tehnike, ki lahko zazna izvedeno spremembo. Tehniki se imenujeta CRC[39] in enosmerna zgoščevalna funkcija.

3.8.2.5.7. Elektronski zapis, sposoben revidiranja

Če je elektronski zapis sposoben revidiranja to pomeni, da je iz ustvarjene in shranjene zgodovine dogodkov, mogoče razbrati kdo, kaj, kdaj, zakaj ter kako je nekaj storil. Iz informacij v teh dokumentih je mogoče ugotoviti tok njihovega zajemanje, uporabe, vzdrževanja in ohranjanja.
Zgodovina dogodkov je izjemno pomembna za dokumentiranje osnovnega nastanka elektronskega zapisa, tudi digitalnih časovnih označitev, in uvedenih dodatnih ukrepov za razširitev uporabnosti elektronskih zapisov v smislu obnove, pretvorbe ali migracij. Informacija zgodovine dogodkov je meta podatek in je shranjena kot zapis, največkrat kot del meta podatka, ki je zaprt skupaj s sorodnim elektronskim zapisom.

3.8.2.5.8. Zaprt elektronski zapis

V zaprtih elektronskih zapisih vse informacije, ki so povezane s specifičnim zapisom ali zapisi, ki obsegajo elektronske podatkovne mape, kot so meta podatki, njihove vsebine, obstajajo kot enojna logična ali fizična entiteta. (Rothenberg, 1996, 15 str.)

3.8.2.6. Strategija elektronskega arhiviranja

Podjetja morajo imeti izdelano dolgoročno strategijo, ki bo vključevala vsa načela elektronskega arhiviranja. Ta strategija naj bi temeljila na sistematični analizi in poznavanju sposobnosti obstoječe digitalne tehnologije za podporo načelom elektronskega arhiviranja. Strategija mora vključevati pričakovano omejeno življenjsko dobo, ranljivost spominskega medija, uporabo tehnologije nevtralnega prenosa podatkov ali izmenjavo formata, prenosljivost programov na raznovrstne tehnološke platforme in v tehnološko zastarele sisteme.

3.8.2.6.1. Pričakovana življenjska doba in ranljivost spominskega medija

Kljub ocenjeni napovedani pričakovani življenjski dobi – od dvajset do sto let – so digitalna spominska sredstva v sovražnem spominskem okolju ranljiva in podvržena tehnološki zastarelosti.Pogosta trditev o tri- ali petletnem tehnološkem ciklu zastarelosti ima na praktični operativni ravni manjši pomen. Uporabnost elektronskih zapisov lahko pomembno razširimo z obnovitvijo spominskega medija, izvedeno s kopiranjem ali obnovo.

S kopiranjem naredimo zrcalno kopijo slike osnovnega bitnega toka elektronskega zapisa z enega spominskega medija na novem, z enako specifikacijo formata.

Obnovljen elektronski zapis vsebuje transformacijo osnovnega bitnega toka elektronskega zapisa iz enega spominskega medija na drug spominski medij.

---

[39] CRC - angl. *Cyclical Redundancy Checksum* (Vir: URLS, ”How the CRC algorithm works”)

3.8.2.6.2. Tehnološko nevtralni formati za izmenjavo podatkov

Kopiranje in obnova elektronskih zapisov z namenom povečanja njihove uporabnosti ne zagotavljata njihove operativnosti, kajti izdelovalci razvijajo svojstvene formate za povečanje učinkovitosti notranje obdelave in razvoj analitične tehnike. Ti svojstveni formati so zaprti (lastniški), zahtevajo uporabo aplikacijskega programa in po potrebi posebno tehnološko platformo v času zajemanja in uporabe elektronskega zapisa. Odprti (javni) ali tehnološko nevtralni formati za izmenjavo podatkov, ki so lahko uporabljeni na poljubni tehnološki platformi ali s katerimkoli aplikacijskim programom, so bistveni za vzdrževanje ali procesiranje elektronskih zapisov.
Poznamo dva tehnološko nevtralna formata za izmenjavo podatkov na mestu, ki podpirata prenosnost elektronskih zapisov na raznovrstne tehnološke platforme.

Prvi je XPORT[40] to je prenosni, odprti format, ki ga podpira inštitut SAS; njegove specifikacije so v javni domeni. Načrtovan je za zapise kliničnih testov. XPORT je dobro vpeljan in zanesljiv format za izmenjavo podatkov, zato ga je FDA sprejela kot format za izmenjavo elektronskih kliničnih testnih podatkov.
Druga tehnologija nevtralnega prenosa podatkov je ANDI[41] To je protokol, ki se uporablja za laboratorijske podatkovne sisteme v farmacevtskih laboratorijskih analizah. Namen protokola ANDI, ki ga sponzorira Ameriška družba za preskušanje in materiale (ASTM[42]), je zagotoviti »ustaljen, od proizvajalcev neodvisen podatkovni format«, ki med drugim pospešuje prenos laboratorijskih podatkov med različne programe CDS[43] in arhiviranje analitičnih podatkov. Protokol ANDI uporabljajo številni proizvajalci in tudi Ameriška družba za preskušanje in materiale aktivno pospešuje večjo uporabo tega protokola.

3.8.2.6.3. Vsesplošna uporabnost aplikacij

V zadnjih petnajstih letih so se pojavili odprti sistemi (ki niso v nasprotju z definicijo »odprtih sistemov« v Part 11) s sestavnimi deli, ki imajo prilagojene vmesnike, s čimer se je zvečala vsesplošna uporabnost sistemov. To pomeni, da funkcije, ki jih neka aplikacija podpira v specifičnem okolju, z natančno enakimi rezultati lahko ponovimo v popolnoma drugem okolju, pri čemer se to sklada z bistveno zahtevo »play back« lastnosti v 21 CFR Part 11. FDA imenuje to »neprekinjenost znanja«.

Vsesplošna uporabnost aplikacij je za laboratorijske podatkovne sisteme posebej pomembna zaradi dveh razlogov.
Prvič, standardne procedure delovanja dopuščajo uporabniku precejšnjo samostojnost glede interpretacije, analize podatkov ali pregleda analitičnih parametrov.
Drugič, izdelovalci programske opreme poskušajo doseči izboljšanje in s tem vzdrževati konkurenčno prednost z dopolnjevanjem ponudbe z uporabniku bolj prijaznimi in učinkovitimi analitičnimi orodji. Značilen primer je vgraditev algoritmov, ki uporabljajo različne atribute za pretvorbo dvojiških izvornih podatkov v značilne procesirane podatke. Malo verjetno je, da bi ob uporabi dveh različnih algoritmov, četudi sta si sorazmerno podobna, dobili absolutno enako procesirane podatke.

---

40 XPORT- angl. *Transport Format* (Vir: XPORT Transport Format)
41 ANDI - angl. ***An**alytical **D**ata **I**nterchange*
42 ASTM - angl. ***A**merican **S**ociety for **T**esting and **M**aterials*
43 CDS - angl. ***C**hemical **D**atabase **S**ervice*

Seveda je vsesplošna uporabnost aplikacij znotraj določene družine izdelkov mogoča. Proizvajalec ohrani združljivost z obstoječimi sistemi, kar običajno pomeni, da so vse funkcionalnosti aplikacije skupaj z razširjeno novo funkcionalnostjo zajete v novi verziji.

3.8.2.6.4. Tehnološko zastareli aplikacijski sistemi

Po FDA so starejši aplikacijski sistemi tisti, ki so jih začeli uporabljati pred 20. avgustom 1997. Starejši sistem ustreza opisu aplikacije, ki ji manjkajo izvozno/uvozne funkcionalnosti za prenašanje elektronskih zapisov in programske funkcionalnosti za prehod na novo tehnološko platformo brez izgube vsebine, konteksta ali funkcionalnosti. To imenujemo migracija zapisov. Edina sedaj znana pot za migracijo elektronskih zapisov skupaj z nujno programsko funkcionalnostjo za odprte sisteme je pisanje posebne namenske kode ali programa.

Poznamo deset »migracijskih korakov« (Brodle, Stonebraker, 1995, str. 30), ki naj bi jim sledila organizacija, ko seli starejši operativni informacijski sistem na novo platformo. To so:

1. analiza starejšega informacijskega sistema
2. razčlenitev strukture starejšega informacijskega sistema
3. načrtovanje ciljnih vmesnikov
4. načrtovanje ciljnih aplikacij
5. načrtovanje ciljnih podatkovnih baz
6. instalacija ciljnega okolja
7. instalacija in ustvarjanje potrebnega portala
8. migracija tehnološko zastarele podatkovne baze
9. migracija tehnološko zastarelih aplikacij
10. migracija tehnološko zastarelih vmesnikov

Ni nujno, da vedno izvedemo vseh deset korakov, ker se okoliščine pri posamezni migraciji lahko močno razlikujejo, kar je odvisno od starejšega in ciljnega aplikacijskega sistema. Zadnji trije koraki so zelo pomembni, ker vplivajo na celovitost zapisov in funkcionalnost aplikacije.

Pred izvedbo popolne migracije je priporočeno, da predlagani pristop testiramo z vzorčnim elektronskim zapisom. Tako preverimo, da ni prišlo do pomembne degradacije v programski funkcionalnosti ali celovitosti zapisa. Selitveni vzorec elektronskih zapisov primerjamo z originalnim zapisom v stari aplikaciji in tako preverimo celovitosti prenesenega vzorca. Za novo programsko aplikacijo se bo preverjala funkcionalnost v smislu potrjevanja dobljenih analitičnih rezultatov, ki morajo biti znotraj določenih, še sprejemljivih mej.

Strategija elektronskega arhiviranja, ki podpira načela elektronskega arhiviranja in upošteva omejitve današnje digitalne tehnologije, je zajeta v naslednjih točkah: (Dollar, 2000, str. 25)

- Uporabnost elektronskih zapisov podaljšujemo s periodično obnovo spominskega medija z metodo kopiranja in/ali obnovitvijo zapisov na nov spominski medij.

- Uvesti moramo standarde tehnološko nevtralnih formatov za izmenjavo podatkov, kot sta prenosni format XPORT in protokol ANDI.

- Izkoristimo skladnost programskih verzij za zagotovitev aplikacijske operativne prenosljivosti.

- Elektronske zapise iz starih aplikacijskih sistemov prenesemo na odprte tehnološke platforme.

3.8.2.7. Življenjski cikel zapisov

Življenjski cikel zapisov je življenjska doba zapisa od njegovega nastanka ali prejetja do njegovega uničenja oziroma deaktiviranja. Običajno ga sestavljajo tale stanja: nastanek, vzdrževanje, uporaba in končno uničenje. (National Archives and Record Administration, 2000, str. 5)

Elektronsko podpisani zapis je ustvarjen v prvi fazi življenjskega cikla zapisa. V drugi fazi ga, če je v aktivni uporabi, vzdržujemo in uporabljamo, lahko pa tudi samo vzdržujemo. Končna faza življenjskega cikla zapisov je odstranitev, to je brezpogojno uničenje.

Zapisi so kategorizirani tako, da je njihova odstranitev »začasna« ali »trajna«. Začasni zapisi se ohranijo za določeno časovno obdobje, šele nato se uničijo ali zbrišejo. Trajne zapise shranimo v trajne arhive.

Življenjski cikel zapisov pogosto preseže razvojni cikel sistema. Kadar je potrebno, se zapis ohrani za daljše časovno obdobje, ki presega trajanje elektronskega informacijskega sistema, v katerem je bil elektronski zapis ustvarjen. To predstavlja poseben izziv, zagotoviti je potrebno verodostojnost zapisa, ko le-ta migrira iz enega sistema v drugega.

4. Teorija odločanja

Verjetno ni človeške umske dejavnosti, ki bi nas bolj zaznamovala, kot nas odločanje. Težavnost odločitvenih problemov je zelo raznolika. Sega od enostavnih osebnih odločitev, ki so večinoma rutinske in se jih večinoma niti ne zavedamo, do težkih problemov pri skupinskem odločanju.
Sposobnost sprejemanja dobrih odločitev je veščina, potrebna tako v zasebnem kot strokovnem in poslovnem življenju.

Odločanje je težavno predvsem zaradi (Jurančič, Rajkovič, B.I., str. 2):
- velikega števila dejavnikov, ki vplivajo na odločanje,
- nezadostnega opredeljevanja ciljev,
- zahtevnosti definiranja odločitvenega problema,
- omejenega časa in drugi virov za izvedbo odločanja,
- zahtevnosti definiranja odločitvenega problema in ciljev odločitve,
- izbora možnosti, ki so skladne z našimi cilji.

Mnogo računalniških rešitev se večinoma posveča le vrednotenju različnih možnosti. Proces odločanja je veliko več. V ta namen je bilo razvitih mnogo metod in računalniških programov za podporo odločanju (*DSS*[44]), vendar bom v analizi uporabil metodo večparametrskega odločanja (*MADM*[45]) s programskim orodjem DEXi[46].

4.1. Proces odločanja

Odločanje je proces, pri katerem izmed več možnosti izberemo tisto, ki nas v danem trenutku pripelje do zastavljenega cilja.

Obravnavamo elemente odločitvenega procesa (Rogelj, Rajkovič, Bohanec, 2001) in predpostavimo, da imamo množico variant:

$$\boldsymbol{A} = \{a_1, a_2, a_3, \ldots, a_n\}.$$

Odvisno od problema je ***A*** lahko končna ali pa tudi neskončna množica. Preferenčna relacija

$$\boldsymbol{P} \in \boldsymbol{A} \times \boldsymbol{A},$$

a ***P*** *b* pomeni, da imamo varianto *a* rajši kot varianto *b*.

Relacija ***P*** uredi množico ***A*** po zaželenosti, ustreznosti oziroma koristnosti. Racionalna odločitev pomeni izbiro tiste variante $a \in \boldsymbol{A}$, ki je najbolj zaželena. Navadno je takih variant lahko več. V primeru neskončne množice ***A*** se v praksi omejimo na neko končno podmnožico.

V odločitveni praksi običajno skušamo preferenčno relacijo nadomestiti s funkcijo koristnosti oziroma zaželenosti. Funkcija v(a) izmeri stopnjo zaželenosti variante a, tako da za vsak par $a,b \in \mathbf{A}$ velja:

$$a \; P \; b \Leftrightarrow v(a) > v(b).$$

---

44 DSS - angl. ***D****ecision* ***S****upport* ***S****ystem*

45 MADM - angl. ***M****ulti-****A****ttribute* ***D****ecision* ***M****aking*

46 DEXi - angl. ***De****cision* ***E****xpert* (*Windows)*

Racionalna odločitev je potem izbira variante a*, tako da je

$$v(a^*) = \max_{a \in \mathbf{A}} v(a)$$

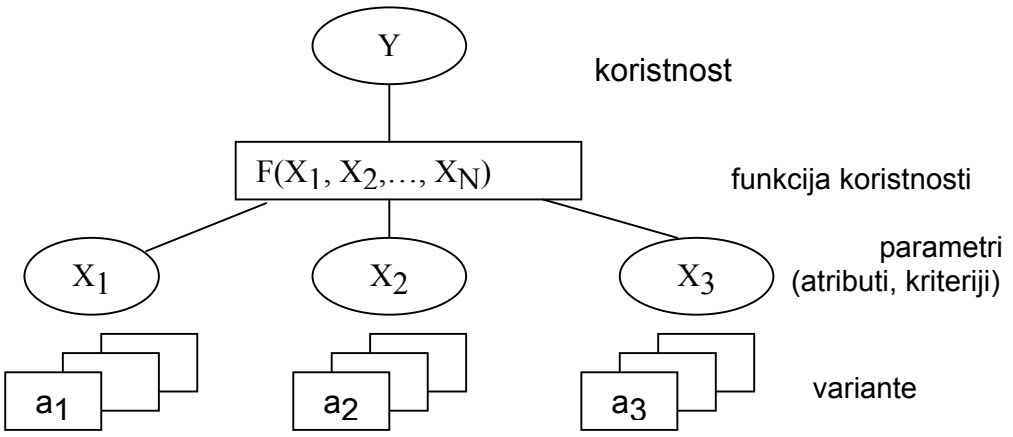
Relacija P predstavlja preferenčno znanje. Preferenca ni aditivna.

Funkcija koristnosti je kriterijska funkcija, s katero določamo koristnost variant na osnovi posameznih parametrov. Pri večparametrskem odločanju predpostavljamo opisljivost variant in obstoj ustrezne funkcije koristnosti. Funkcijo koristnosti v praksi postavi človek, ki se odloči na podlagi izkustev in znanja.

4.2. Večparametrsko odločanje

Večparametrsko odločanje temelji na razgradnji odločitvenega problema na manjše podprobleme. Variante razgradimo na posamezne parametre (kriterije, atribute) in jih ločeno ocenimo glede na vsak parameter. Končno oceno variante dobimo z nekim postopkom združevanja. Tako izpeljana vrednost je osnova za izbor najustreznejše variante.

Slika 9: Prikaz večparametrskega odločitvenega modela



Vir: Rajkovič V., 2001

Vrednotenje variant pri večparametrskem odločanju poteka na osnovi večparametrskega odločitvenega modela, ki je na splošno sestavljen iz štirih sestavnih delov:

V… koristnost,
F… funkcija,
X… parametri, atributi,
a… variante.

Funkcije koristnosti opredeljujejo vpliv posameznih kriterijev na celotno odločitev in izražajo odločitveno moč posameznega kriterija. Variante opišemo z vrednostmi po osnovnih kriterijih v listih drevesa. Končno oceno variant dobimo po njihovem vrednotenju.

Množica parametrov $\boldsymbol{X}$: $x_1, x_2, x_3, \ldots x_n$. $x_i : \boldsymbol{A} \rightarrow \boldsymbol{D}_i$,

kjer so $\boldsymbol{D}_i$ zaloge vrednosti posameznih parametrov.
Vsako varianto a iz množice $\boldsymbol{A}$ opišemo z vektorjem vrednosti parametrov:

$$\overset{\circ}{a} = x_1(a), x_2(a), x_3(a), \ldots x_n(a).$$

Preferenčna relacija P, ki uredi množico $\boldsymbol{A}$ po zaželenosti oziroma koristnosti, sedaj deluje med temi vektorji.

Funkcijo koristnosti v: $\boldsymbol{A} \rightarrow \boldsymbol{D}$ nadomestimo s funkcijo, kjer je $\boldsymbol{D}$

$$v_x: \boldsymbol{D}_1 \times \boldsymbol{D}_2 \times \boldsymbol{D}_3 \times \ldots \times \boldsymbol{D}_n \rightarrow \boldsymbol{D}.$$

Vhod v model predstavljajo parametri (atributi, kriteriji) X_i. To so spremenljivke, ki ponazarjajo podprobleme odločitvenega problema, to je tiste dejavnike, ki opredeljujejo kakovost variant. Funkcija koristnosti F je predpis, po katerem se vrednosti posameznih parametrov združujejo v spremenljivko Y, ki ponazarja končno oceno ali koristnost variante. (Bohanec, Rajkovič, 1995, str. 428)

Variante opišemo po osnovnih parametrih z vrednostmi a_i. Na osnovi teh vrednosti funkcija koristnosti določi končno oceno vsake variante. Varianta, ki dobi najvišjo oceno, je praviloma najboljša.

4.3. Faze odločitvenega procesa

Odločitveni proces je proces sistematičnega zbiranja in urejanja odločitvenega znanja. Poteka po fazah, ki se lahko tudi prepletajo ali ponavljajo. (Bohanec, Rajkovič, 1995, str. 429-430)

4.3.1. Identifikacija problema

V tej fazi definiramo problem ter opredelimo cilje in zahteve. Način, kako opredelimo problem, že oblikuje našo odločitev. Predvsem je potrebno podati problem v jeziku potreb in ne težavnosti situacije.

Oblikujemo odločitveno skupino. Pri zahtevnejših problemih vključimo v delovno skupino tudi: eksperte, odločitvenega analitika - metodologa in predstavnike tistih področij, na katere vpliva odločitev.

4.3.2. Identifikacija kriterijev

Zasnujemo strukturo odločitvenega modela in določimo kriterije, na osnovi katerih bomo ocenjevali variante.
Naredimo nestrukturiran seznam kriterijev v obliki spiska kriterijev. V strukturiranju kriterijev le-te hierarhično uredimo. Pri tem upoštevamo medsebojne odvisnosti in povezave. Rezultat je drevo kriterijev. Vsem kriterijem v odločitvenem drevesu določimo mersko lestvico, ki predstavlja zalogo vrednosti, ki jih zavzamejo pri vrednotenju.

4.3.3. Definicija funkcij koristnosti

Temelji na razgradnji odločitvenega problema na manjše podprobleme. Možnosti razgradimo na posamezne parametre in jih ločeno ocenjujemo. Končno oceno, ki je osnova za izbiro najustreznejše možnosti, dobimo s postopkom združevanja, npr. utežne vsote, povprečja, odločitvenega pravila, mehkih množic ali funkcij zvezne logike. (Bohanec, Rajkovič, 1995, str. 430)

4.3.4. Opis variant

Vsako varianto opišemo z vrednostmi osnovnih kriterijev, ki ležijo na listih odločitvenega drevesa.

4.3.5. Vrednotenje in analiza variant

Vrednotenje variant je postopek določanja končne ocene variant na osnovi opisa po osnovnih kriterijih. Poteka od spodaj navzgor v skladu s strukturo kriterijev in funkcijami koristnosti. Najboljša varianta običajno dobi najvišjo končno oceno.

Na končno oceno vpliva mnogo dejavnikov in pri vsakem od njih se lahko pojavi napaka. Dobljena ocena včasih ne poda celovite slike variante.

4.4. Računalniška podpora

Računalniška podpora odločanju nam prikazuje ustrezne postopke v procesu odločanja in z večkriterijskim in neostrim odločanjem širi naše miselne zmogljivosti. Omogoča večplastno analizo in upošteva različne variante pri ocenjevanju in izbiri optimalnih rešitev; tega samo z miselno aktivnostjo ne bi uspeli doseči. Usmerja nas v sistematično zbiranje in urejanje znanja, zagotavlja informacije za primerno odločitev in zvečuje verjetnost, da bomo upoštevali vse dejavnike, ki bistveno vplivajo na odločitev.

Uporaba računalniške podpore v procesu odločanja ne more zagotoviti, da bodo naše odločitve boljše in pravilnejše, omogoči pa nam ustrezno tehnologijo izvedbe. Še tako dobra računalniška rešitev ne more nadomestiti naših vrednot in uskladiti ciljev. Verjetno bo ta del odločanja k sreči vedno ostal v človeški domeni.

4.4.1. Programsko orodje DEXi

DEXi je lupina ekspertnega sistema za večparametrsko odločanje.(Bohanc, Rajkovič, 1999, str.1) DEXi tesno sledi konceptu večparametrskega odločanja, ki je osnovan na razčlembi odločitvenega problema v manjše manj kompleksne probleme.

V DEXiju je pristop sestavljen z nekaterimi elementi ekspertnega sistema in strojnega učenja. Atributi in združevalne procedure so obravnavani kot nedvoumne baze, sestavljene iz (1) drevesa kriterijev, (2) združevalne procedure, izražene z odločitvenimi pravili, in (3) opisa opcij.

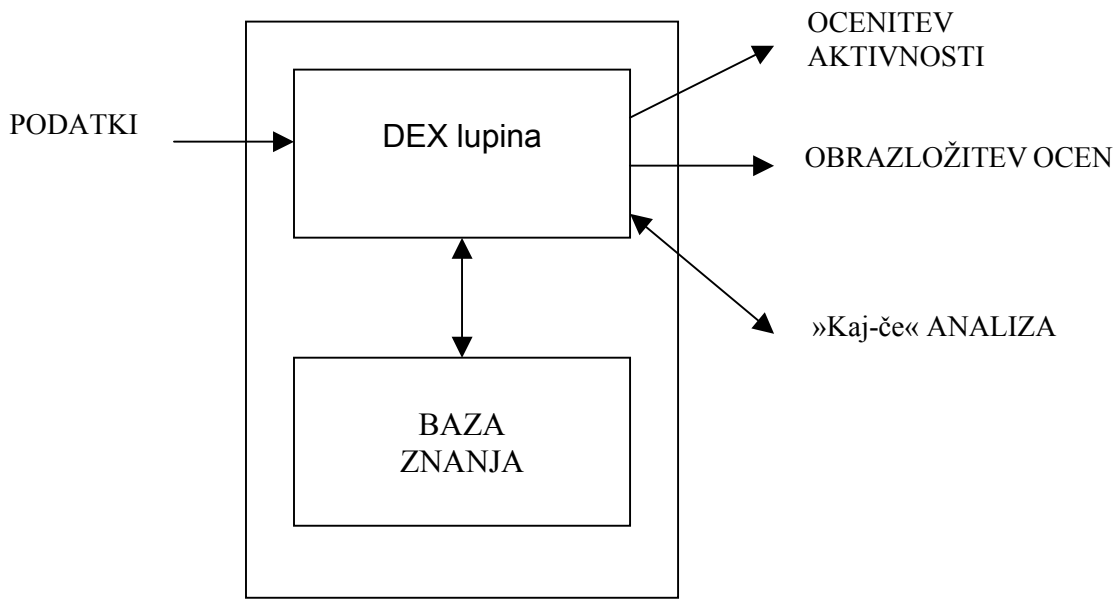
DEXi v osnovi zajema dva operativna gradnika:

1. Pridobljena baza znanja uporabniku pomaga pri načrtovanju drevesa kriterijev in odločitvenih pravil za posamezni problem. Gre za proces strukturiranja odločitvenega problema in izvabljanje znanja. Proces sproti nadzoruje računalniško orodje, ki preverja usklajenost pravil.

2. Drugi del DEXija, prikazan na sliki 10, uporabi pridobljeno bazo znanja za vrednotenje in analizo opcij. V začetku je vsaka opcija opisana z naborom vrednosti, ki ustrezajo mestu na odločitvenem drevesu. DEXi nato ovrednoti posamezno opcijo v skladu z bazo znanja (glede na strukturo drevesa kriterijev in definiranih odločitvenih pravil). Za vsako opcijo je izvedena primerna ocena.
Sledi analiza rezultatov, ki se odraža v eni ali več aktivnostih: (Rajkovič, Bohanec, Zupan, 2000, str. 2-3)

a. Obrazložitev vrednotenja:
   DEXi je sposoben razložiti, kako je bila pridobljena vsaka posamezna ocena v smislu kriterijskih vrednosti in uporabljenih odločitvenih pravil.
b. »Kaj-če« analiza:
   izvede se interaktivno s spreminjanjem opisa opcij, ponovnim vrednotenjem, primerjavo dobljenih rezultatov s prvotnimi rezultati.
c. Selektivna razlaga opcij:
   DEXi najde tiste podskupine kriterijev, ki izražajo najmočnejše ali najšibkejše značilnosti delnih opcij, in poroča o njih. Glavni namen je obrazložitev opcij z uporabo samo najbolj relevantnih informacij.

Slika 10: Shematična struktura odločitvenega sistema



Vir: Rajkovič V., 2000a, str.3

DEXi ponuja dodatek k odločitvam in je osnovan na modeliranju znanja. Takšna podpora omogoča pregledno odločitveno analizo z obrazložitvijo vrednotenih rezultatov in pojasnitev samega ozadja procesa. Odločitvena podpora je uporabniku

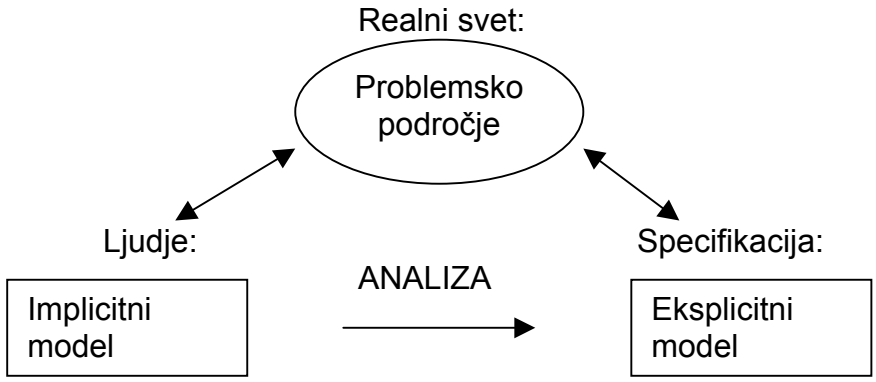
prijazna, kajti odločitveno znanje je predstavljeno enostavno, običajno z besedami, pravili in hierarhično postavitvijo kriterijev.

Vzroki za probleme v procesu odločanja in upravljanju skladnosti sistema:
1. Cilji so lahko negotovi, protislovni, neusklajeni, nepopolni.
2. Variante so lahko slabo ali nepopolno definirane. Veliko število variant otežuje odločitev.
3. Parametri, ki vplivajo na odločitev, so lahko slabo definirani, neznani, spregledani ali težko merljivi.
4. Omejitve virov so lahko časovne, kadrovske in druge.
5. Metodološke omejitve se pojavijo pri ocenjevanju kakovosti odločitve.

4.4.2. Ljudje kot viri informacij

Naloga analitikov je iz slabo definiranih, nejasnih, včasih celo nasprotujočih si informacij o nekem realnem problemu izluščiti jasne in eksplicitne zahteve. Modelira se del neke stvarnosti, ki jo imenujemo problemsko področje. (Solina, 1997, str. 123) Primeri takega problemskega področja so informacijski sistemi, sistem regulative, inšpekcije. Ena od glavnih nalog analize je ločevanje pomembnih informacij od nepomembnih podrobnosti. Ljudje, ki so vpleteni v neko problemsko področje, imajo svoj implicitni model, ki vsebuje raznovrstne informacije in znanja o tem področju, ki ga imajo ljudje v veliki meri za samoumevnega. Implicitni model je težko ubesediti, saj vsebuje navade, običaje, predsodke, celo nasprotujoča si dejstva. Naša naloga pri izdelavi odločitvenega modela je spremeniti implicitni model v eksplicitnega, ki je razumljiv vsem vpletenim ljudem.

Slika 11: Prikaz izdelave specifikacije eksplicitnega modela s pomočjo analize

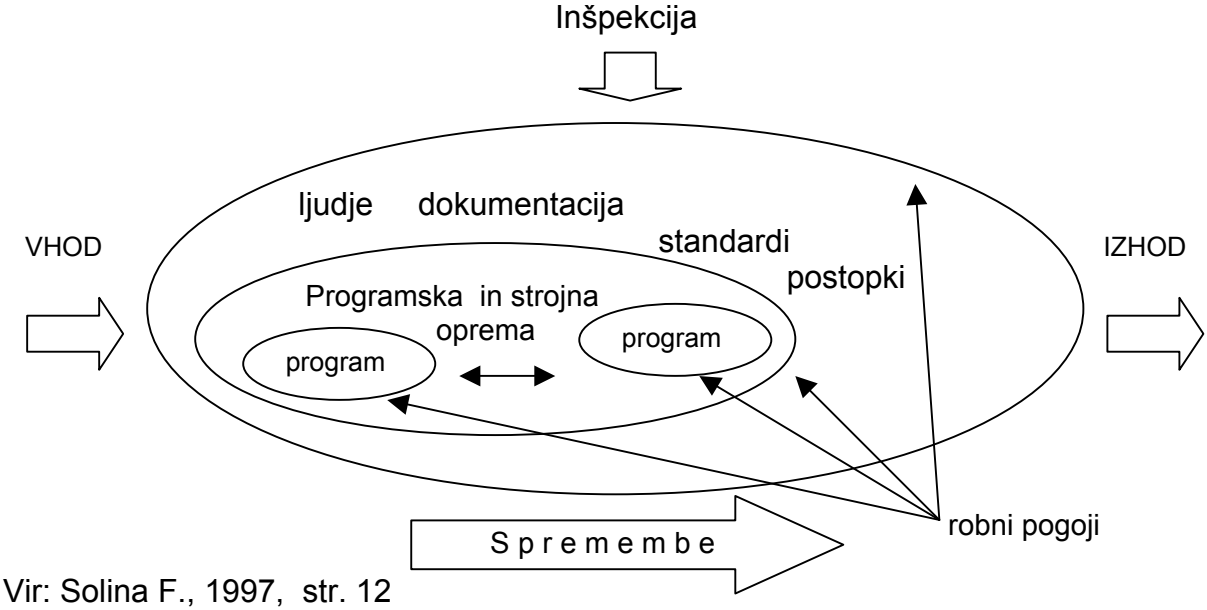


Vir: Solina F., 1997, str. 124

5. Inšpekcija

Inšpekcije opravljajo nadzor. Ameriška Regulativa določa dve specifični instanci, ki podjetje neposredno povezujeta z FDA. (Grunbaum, 2002, str. 36) Prva je sekcija §11.100(c), ki opredeljuje postopek potrditve elektronskega podpisa pri agenciji. Druga, ki je logično nadaljevanje prve, je inšpekcija FDA. Agencija mora imeti možnost presoje zapisov in sistemov, da potrdi zaupanje v pregledane podatke, ki jih podjetje posreduje FDA v okviru registracijskega dosjeja oz. so del interne dokumentacije, ki se redno presoja v okviru rednih sistemskih inšpekcij.

Slika 12: Načrtovanje inšpekcije določa, kateri del nekega problemskega okolja je predmet preiskave.



Vir: Solina F., 1997, str. 12

Presoja elektronskih procesov, vključno s spominskimi mediji, je seveda kompleksna aktivnost. Opredeljena je v sekciji §11.10(b), ki obravnava področje inšpektibilnosti.

FDA lahko izvede temeljito inšpekcijo šele takrat, ko se inšpektor lahko zanese na celovitost in točnost čitljive kopije elektronskih podatkov.

5.1. Definicija uspešne inšpekcije

Inšpekcija FDA je za podjetje uspešna, če ob koncu ni nobene pripombe na obrazcu FDA-483. Poseben poudarek je na dolgoročnem sodelovanju ter negovanju dobrih in verodostojnih odnosov z agencijo. Med trajanjem inšpekcije je odločilno korektno sodelovanje in uspešno odgovarjanje na vprašanja, ki so bili naslovljeni na posameznika oziroma podjetje ter odprava vseh morebitnih dvomov.

Vzroki za inšpekcijo so različni: (Malcolm Dixon, 2001, str. 1)
a) redne dvoletne inšpekcije (sistemske inšpekcije),
b) inšpekcije zaradi določenega vzroka (odpoklici, pretekli zaznamki v zgodovini inšpekcij),
c) inšpekcija za pridobitev dovoljenja za promet z zdravilom (*PAI*[47]) (izdelava in predaja registracijskega dosjeja, večje spremembe v proizvodnji ali v formulaciji zdravilnih učinkovin, sprememba lokacije proizvodnje itd.). (Guide to inspections of foreign P. M.; str. 5)

Po koncu vsakega pregleda, presoje in inšpekcije sledi priprava povzetka. To je strnjeno in jedrnato poročilo o aktivnostih in dobljenih ocenah. Te vrste preverjanj je treba jemati poleg ostalega tudi kot izkušnjo za pridobivanje novih spoznanj, rešitev in napotkov (Forstedt, 2001, str. 358), ki jih postopoma lahko vgradimo v uporabljeni model.

47 PAI - angl. ***P**re **A**pproval **I**nspection*

Podjetje kot skupek zelo kompleksnih sistemov ima svoje zakonitosti in življenjsko pot obvladovanja kakovosti na poti k odličnosti. Bolje ko je podjetje pripravljeno na odločilne inšpekcije, manj je poznejših stresnih stanj in uspešnejše je lahko tudi njegovo delovanje v globalnem tržnem sistemu.

5.2. Priprave na inšpekcijo

5.2.1. Vodenje inšpekcij

Za uspešen potek vodenje inšpekcij na sistemski ravni in ravni računalniških sistemov (Malcolm Dixon, 2001, str. 2-4):

a) Moramo poznati standarde, ki jih določajo
   - programi (FDA Investigations Operations Manual),
   - navodila (FDA Compliance Program Guidance Manual, FDA inspections Guides),
   - regulativa (Code of Federal Regulations; področje regulatornih zahtev, s poudarkom na tistih, ki opredeljujejo področje elektronskih zapisov in podpisov).

b) Pripraviti moramo interne programe, v katere zajamemo:
   - standarde podjetja,
   - ugotovitve prejšnjih inšpekcij FDA,
   - razvojne načrte (GAP[48] analiza) [49],
   - odgovornosti.

c) Določiti moramo pravila in odgovornosti ključnih posameznikov.

d) Ovrednoti usklajenost novih procesov, za katere pripravimo poleg analize skladnosti še raziskavo njegove ranljivosti v času prvih presoj in inšpekcijskih zagovorov, kajti sistem je nepreverjen in lahko skriva kritični odstop (gl. poglavje: Skrite in aktivne napake).

e) Zagotovimo, da osebje razume, kaj lahko pričakuje med samo inšpekcijo. Še zlasti to velja za skrbnika sistema, ki mora imeti potrebne kvalifikacije in izkušnje, ter odgovorno osebo, ki bo spremljevalec.

f) Priporočeno je, da tudi za obisk inšpekcije izdelamo standardni postopek delovanja (SOPs).

g) Pripraviti moramo predstavitev :
   - makro in mikro organizacijske sheme,
   - politike podjetja in postopke zagotavljanja kakovosti,
   - tehnoloških in informacijskih procesov,
   - načrtov validacij, protokolov in postopkov prilagajanja skladnosti,
   - uporabniških zahtev in specifikacij načrtovanja za informacijske sisteme,
   - postopkov in sprememb, ki smo jih izvedli po zadnji inšpekciji.

---

48 GAP - angl. *vrzel*

49 GAP analiza – Analiza vrzeli oziroma ugotavljanje neskladnosti v opazovanih sistemih.

h) Razviti moramo orodja, s katerimi bomo spremljali morebitne pripombe na in sprotno določali vire za korektivne aktivnosti.

i) V primeru potrebe po podrobni raziskavi in razčlenitvi shranjenih informacij (rezultatov analize …) moramo zagotoviti možnost učinkovitega restavriranja in preverjanja izvornih podatkov.

j) Upoštevati moramo pravila in nenehno delovati v skladu z varnostno politiko podjetja, v kateri so že upoštevane varnostne smernice regulative 21 CFR Part 11 (gl. poglavje: Varnost, Dobre prakse elektronskega arhiviranja).

k) Zagotoviti moramo, da je na voljo strokovna in regulatorno skladna pomoč (pri tem je treba upoštevati zahteve §11.10 21 CFR Part 11 glede kvalificiranosti osebja).

l) Predhodno izvedemo interne presoje računalniških sistemov z namenom analize samih procesov (gl. poglavje: Neskladnost sistemov, Napake v tehnologiji) in ključnih človeških faktorjev (gl. poglavje: Ljudje in človeški faktor).

5.2.2. Inšpektorji

Poznati moramo način delovanja inšpektorja in njegova pravila. To znanje smo si pridobili ob prejšnjih inšpekcijah, s pregledom različne dokumentacije in s seznanitvijo z izkušnjami drugih podjetij. Z inšpektorji se poleg formalnega sodelovanja vedno vzpostavi tudi neformalna zveza, ki običajno zaradi intuicije določene osebe nastane spontano in redko kot rezultat premišljene aktivnosti ter pripomore k dobrim ugotovitvam inšpekcije. V obeh primerih ravnamo z inšpektorjem s spoštovanjem, vljudno in profesionalno ter ga ne puščamo samega.

Načrte bodočih aktivnosti naredimo na osnovi podanih dnevnih odkritih neskladnosti. Inšpektorju moramo pozorno prisluhniti in zahtevati pojasnitev nejasnosti, ki so se pojavile med presojo, vendar le, če je to nujno potrebno.

Na vprašanja inšpektorja vedno odgovarja izvajalec procesa oz. skrbnik sistema, kajti le tako lahko dobi inšpektor pravilen vpogled v izvajanje oziroma v strokovnost osebja, ki vodi procese oz. izvaja skrbništvo nad sistemi. Komunikacija mora biti učinkovita in dobro organizirana, po potrebi vanjo vključimo strokovnjake s specifičnim znanjem.

Četudi je informacijski sistem močno odvisen od regulative (gl. poglavje: Neskladnost sistemov. npr. »tesna povezava«) oz. je model grajen na osnovi regulatornih zahtev 21 CFR Part 11, je ravno inšpektor tisti, ki poda prvo oceno skladnosti oziroma potrdi prizadevanja podjetja.

Pomembno je, da se zavedamo pojava »normalizacije odklona«, ki ga lahko delno obvladujemo le z neodvisnim delovanjem sistema zagotavljanja kakovosti. Če postane le-ta del celotnega sistema rešitev, postane sistem nesposoben odkrivati lastne odstope in postane dokaj ranljiv, posebej pri uvedbi novih sistemov, ki jih še niso pregledali neodvisni zunanji presojevalci.

5.2.3. Upravljanje znanja

Podatki se morajo zbirati na enem mestu in morajo biti v vsakem trenutku v primerni obliki dostopni ljudem, ki vodijo inšpekcijo. V novejšem času se kreirajo skupne baze znanja, kjer s pomočjo ekspertnih sistemov olajšamo procese spremljanja in odločanja.
Dokumente v pisni kakor tudi v elektronski obliki, ki jih odstopimo inšpektorjem, moramo dodatno označiti, ohraniti njihov vir nastanka (sledimo orginalu), jih opremiti z imenom podjetja in jih obravnavati kot zaupne. Za lasten arhiv si izdelamo natančno kopijo in pri tem upoštevamo zahteve sekcije §11.10 - 21 CFR Part 11, ki govori o kontroli sistemske dokumentacije.

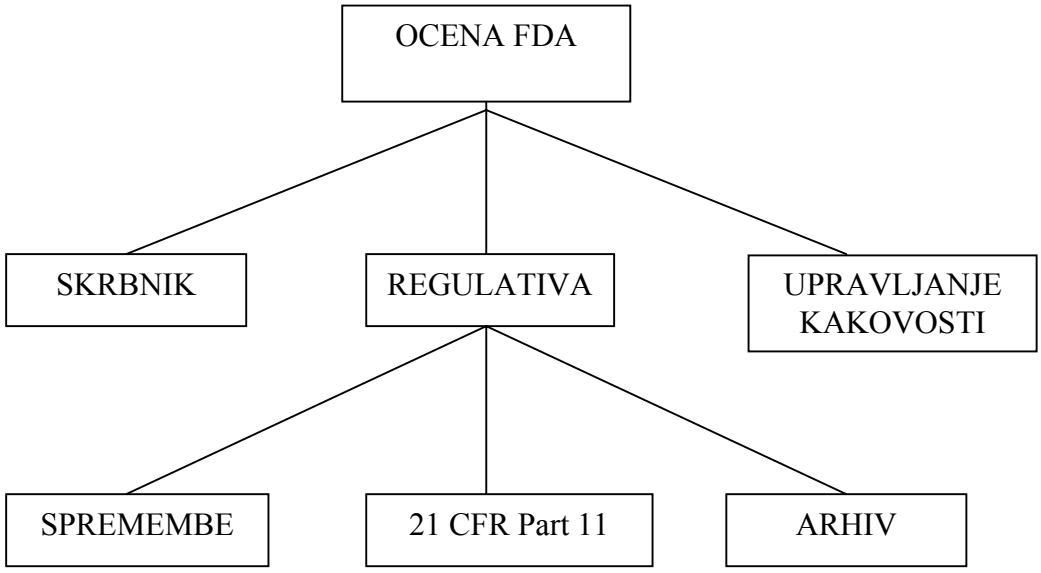
Sproti si ustvarjamo »problemsko matriko« (Malcolm Dixon, 2001, str. 8), ki nam predstavlja zbirko informacij za preglednejše razumevanje naše regulatorne ranljivosti. Praktično upravljanje z zapisi si podjetje uredi na osnovi operativnih potreb in glede na zaznavanje morebitnih tveganj.
Pristop za operativne potrebe je določen na osnovi zagotavljanja zaupanja vrednih elektronskih zapisov v času celotnega življenjskega cikla zapisa. Poslovna tveganja, ki so posledica izgube zapisov, zakrivanja podatkov, neopravljene inšpekcije, neustrezne odločitve zaradi napačnih informacijskih virov, lahko ocenimo zgolj kot verjetnost, da se bo nesrečni dogodek zgodil, oziroma na osnovi zaupanja v skladnost sistema.

Pri elektronskih zapisih in podpisih se lahko pojavijo naslednja poslovna tveganja:
1. uradna oporekanja zapisom oziroma zapisani vsebini,
2. nezaupanje v elektronsko podpisane zapise, če ti niso v skladu s predpisano regulativo.

Ocene tveganja se uporabijo za določitev zahtevane dokumentacije za validacijo elektronskega zapisa in elektronskega podpisa.

6. Odločitveni model

Slika 13: Shema odločitvenega drevesa, ki je izdelano na osnovi 21 CFR Part 11 kot del modela validacije računalniškega sistema



Odločitveno drevo sestavlja pet osnovnih atributov:

1. **Upravljanje kakovosti**
   Obravnavamo ga v sklopu celotnega procesa upravljanja kakovosti, ljudi, ki ga sooblikujejo, in zagotavljanja kakovosti.

2. **Skrbnik**
   Ugotavljamo njegovo primernost, ustrezno usposobljenost in vpliv »človeškega faktorja« na oceno skladnosti.

3. **21 CFR Part 11**
   Regulativo za elektronske zapise in elektronske podpise prikažemo v sklopu modela validacije računalniških sistemov.

4. **Spremembe**
   Predstavimo obravnavanje sprememb v življenjskem ciklu sistema in življenjskem ciklu zapisov.

5. **Arhiv**
   Ohranitev zapisov obravnavamo glede na skladnost z dobro prakso arhiviranja in v sklopu zahtev regulative 21 CFR Part 11.

Končno oceno variant, pri našem modelu je to ocena skladnosti sistema, bomo predstavili z zornega kota pričakovane ocenitve ameriške Agencije za prehrano in zdravila. Možne ocene so:

- kritični odstop: neposredno vpliva na varnost zdravila oziroma bolnika,
- večji odstop: neskladnost izdelka ali postopkov z registracijsko dokumentacijo,
- drugi odstop: ne spadajo med kritična ali večja, pa vendar kažejo odstop od GxP,
- ni odstopa: ni odstopa od GxP.

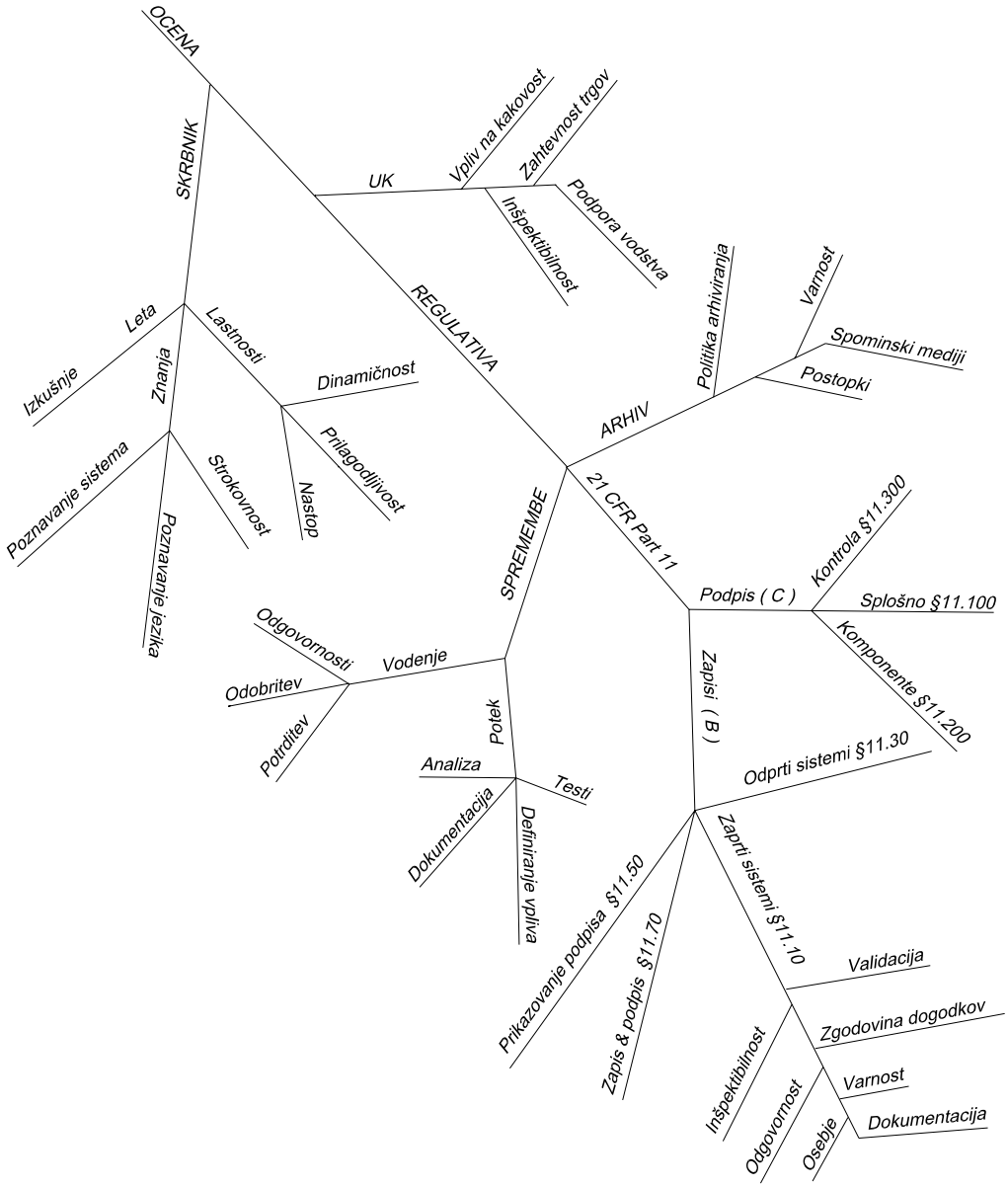
Ocena v tem primeru predstavlja stopnjo tveganja, da bo izdelano zdravilo oporečno ali da izdelek ne bo ustrezne kakovosti. To tveganje zmanjšamo s sistemom kontrole kakovosti, ki zagotavlja, da so vsi potrebni in bistveni preskusi opravljeni in da izdelki niso dani ne v uporabo ne v prodajo, dokler ni ocenjeno, da je njihova kakovost zadovoljiva.

Posredno je sistem kontrole zajet v procesu sprememb, ko sledi zahtevam okolja in odpravlja njegova neskladja z ugotovljenimi dejstvi oziroma odstopi.

6.1. Odločitveno drevo

Odločitveno drevo je hirarhična razvrstitev kriterijev in predstavlja osnovno strukturo odločitvenega modela. Zajeti so vsi kriteriji, ki bistveno vplivajo na odločitev.

Slika 14: Prikazuje drevo osnovnih parametrov za celovito oceno skladnosti računalniških sistemov z vidika inšpekcije Ameriške agencije za prehrano in zdravila.



Posebej želim opozoriti na izbiro ustrezne merske lestvice, to so zaloge vrednosti v podskupinah odločitvene veje 21 CFR Part 11, kjer s sistemsko klasifikacijo elektronskega zapisa v posameznih variantah (glej poglavje 6.2) določimo ali ima sistem zahtevane atribute regulative in s tem postane predmet naše ocenitve po določenem scenariju ali pa ne.Ta pristop omogoča prilagoditev modela celotnemu spektru različnih sistemskih aplikacij.

6.2. Klasifikacija po 21 CFR Part 11

Namen klasifikacije je:

- podrobno opisati kriterije, s katerimi lahko v skladu z regulativo 21 CFR Part 11 elektronske zapise, elektronske podpise in ročne podpise na elektronskih zapisih enačimo s papirnimi zapisi in ročnimi podpisi na papirju;
- izdelati model za ovrednotenje elektronskega zapisa glede na vpeljane zahteve;
- izdelati celovito strukturo regulatornih zahtev 21 CFR Part 11, ki bo osnova za izdelavo regulatorne veje odločitvenega drevesa.

Obravnavani zapis računalniškega sistema analiziramo po posameznih odločitvenih modulih od modula 1 (M1) do modula 7 (M7).

Z odločitvenimi moduli od 1 do 4 želimo izločiti tiste elektronske zapise, ki:
- ne ustrezajo definiciji regulatornih zahtev za elektronske zapise (modul 1),
- so faksirani ali skenirani papirni zapisi (modul 2),
- so dovoljeni samo v papirni oblike (modul 3),
- zahtevajo posebno presojo elektronskega zapisa (modul 4).

Modul 5 obravnava elektronski zapis brez podpisa. Modul 6 obravnava posamezne vrste elektronska podpisa.

Sledi vsebinski opis posameznih modulov (glej sliko 15):

a) modul 1 (M1– Regulativa se nanaša na širok spekter računalniških sistemov, ne samo na tiste, ki uporabljajo elektronske podpise. Obravnava tako nove kot že obstoječe sisteme.

O elektronskem zapisu govorimo:
- če se uporabnik odloča o stvareh, ki so povezane s sistemom kakovosti, s pomočjo računalniškega sistema in se aktivnost vpiše v zgodovino dogodkov;

- če so informacije, ki so posredovane ali predložene inšpekciji, izdelane s pomočjo računalniškega sistema;

- če je že samo delček izdelanih informacij za kupce ali »ad hoc« zapiskov rezultat računalniških procesov ali uporabe računalniških sistemov (npr. poročila o trendih, povzetki, zaključki, poročila o izjemah ...).

b) modul 2 (M2) – Obravnava papirne zapise, poslane z elektronskim medijem, npr. telefaksom ali optičnim čitalnikom.

c) modul 3 (M3) – Določena regulativa zahteva papirni zapis ali dokument. Za te oblike zapisa je elektronski zapis prepovedan. Primer tovrstnega zapisa je fizična kopija »signature-standard«[50] in »navodila-standard«[51], ki mora biti ohranjena.Papirni dokument za potrditev FDA-agenciji, da organizacija uporablja in da razume elektronski podpis enakovreden ročnemu.

---

50 »signatura-standard«- Izpisana avtentična referenčna signatura, ki je ustrezno overjena.

51 »navodilo-standard« - izpisano avtentično referenčno navodilo, ki je ustrezno overjeno.

d) modul 4 (M4) – Informacijska varnostna politika podjetja določa metode in postopke, ki zagotavljajo zasebnost, avtentičnost in celovitost informacij. Politika se nanaša tudi na sisteme z modemskim ali internetnim pristopom. Po definiciji (21 CFR Part 11) delimo sisteme na zaprte in odprte.

Tabela 6: Prikaz sekcij 21 CFR Part 11, ki obravnavajo odprti in zaprti sistem pri različnih scenarijih

		Sekcije Part 11 (z,o = obravnava / prazno polje = ne obravnava)									
Scenarij	ATRIBUTI	11.1 11.2 11.3	11.10	11.30	11.50	11.70	11.100	11.200(a)	11.200(b)	11.300 (a),(b),(d)	11.300 (c), (e)
1	Elektronski zapis	z	z								
	(brez podpisa)	o	o	o							
2	Ročni podpis,	z	z		z	z					
	izveden na e-zapisu	o	o	o	o	o					
3	e-podpis, ki temelji	z	z		z	z	z		z		
	na biometriji	o	o	o	o	o	o		o		
4	e-zapis, osnovan na	z	z		z	z	z	z		z	
	ID kodi in geslu	o	o	o	o	o	o	o		o	
5	e-podpis,	z	z		z	z	z	z			z
	ID koda in žeton	o	o	o	o	o	o	o			o

z - pomeni, da se regulativa nanaša na zaprti sistem
o - pomeni, da se regulativa nanaša na odprti sistem

Vir: Alcon, 9, 1997, str. 2.

e) modul 5 (M5) – Razlikujemo med »podpisom« in »identifikacijo«. Če je namen identifikacije overiti elektronski zapis, potem je identifikacija elektronski podpis. Če je namen samo identificirati, kdo je kaj naredil, to ni elektronski podpis.

Kje se bodo ali ne bodo uporabljali podpisi, ni odvisno od lastnika sistema ali politike podjetja, ampak jih narekujejo GxP zahteve.

Podpis ima običajno vse atribute, ki jih določa regulativa za elektronski podpis.

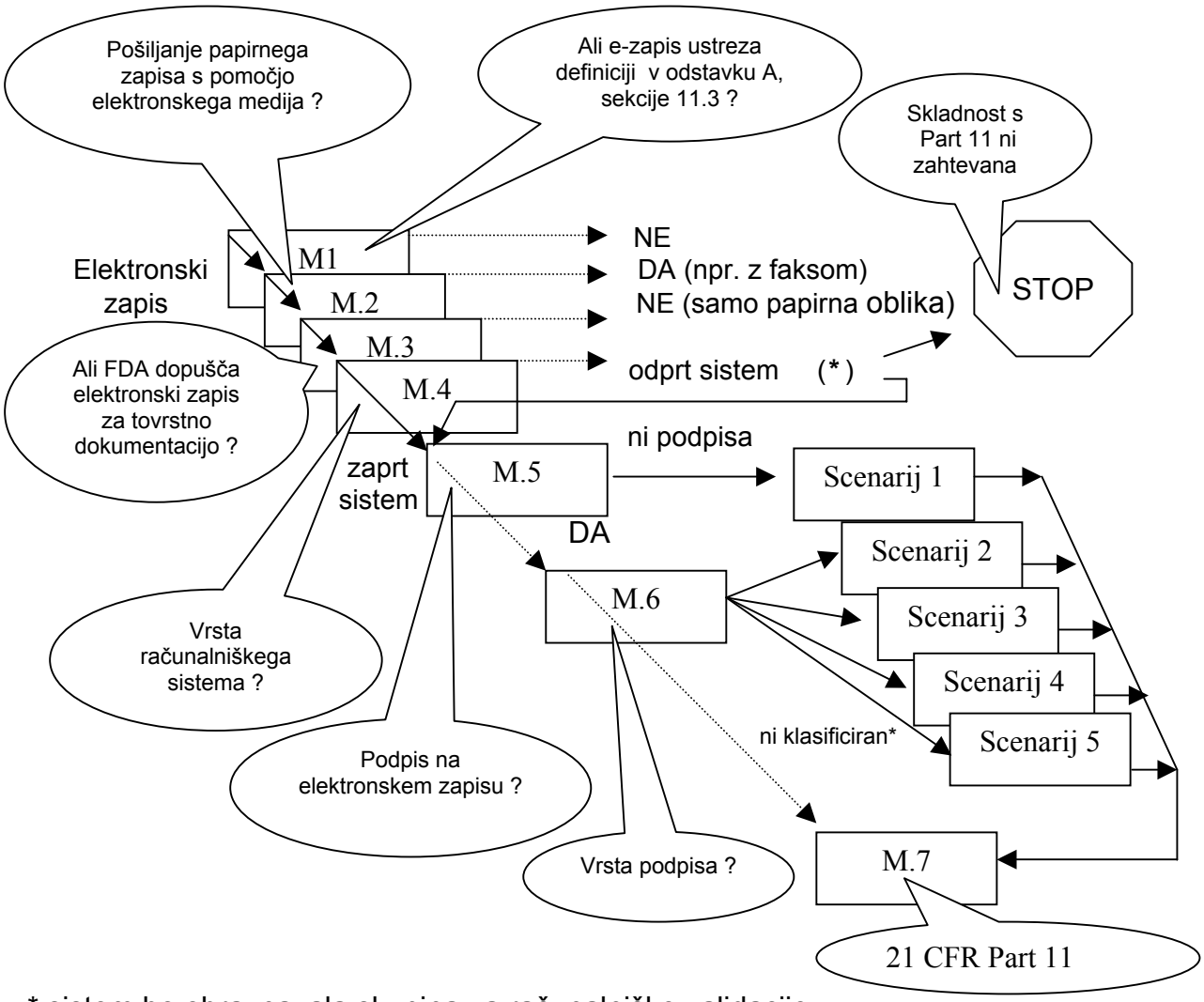
Atributi podpisa so izvedba in prikaz:

- izvedba je nebiometrična ali biometrična, pri čemer moramo zadostiti pogojem oziroma zahtevanim merilom (enkratnost, neponovljivost …);
- prikaz (datum in čas, tiskano ime posameznika, namen podpisa).

f) modul 6 (M6) – Metodo elektronskega podpisa izbiramo po predloženem scenariju za različne vrste podpisa. Če sistem nima potrebnih značilnosti, ga obravnavamo kot nekvalificiranega, naredimo samo delno ocenitev in skozi sekcijo §11.10 ter nadalje z ustrezno analizo ekspertne skupine za računalniško validacijo nadaljujemo postopek.

g) modul 7 (M7) – Glede na izbrani scenarij določimo po tabeli 6 osnovni potek odločitvenega drevesa.

Slika 15: Prikaz sistemske klasifikacije elektronskega zapisa



* sistem bo obravnavala skupina za računalniške validacije

Kjer je v tabeli 6. prazno polje, to v preslikavi na odločitveni model pomeni, da nima vpliva na delne in končne odločitve.

Da bi ugotovili skladnost predlaganih rešitev, izdelamo analizo skladnosti oziroma analizo vrzeli. Tako v sistemski rešitvi za posamezne računalniške in informacijske sisteme iščemo usklajenosti oziroma pomanjkljivosti glede na zahteve regulative. Rezultat posamezne presoje je lahko ugotovitev: da je rešitev skladna z regulativo, da rešitev ni skladna z regulativo ali da predvideni koncept nima zahtevane funkcionalnosti in zato ni predmet regulatornih zahtev. Začetno oceno moramo uskladiti in potrditi s sistemom upravljanja kakovosti, nato pa na tej osnovi predpišemo strategijo aktivnosti.

Zaloge vrednosti za posamezne skupine in podskupine seznama kriterijev v 21 CFR Part 11 so:

- *skladen*: interpretacija rešitve se popolnoma ujema z zahtevami 21 CFR Part 11;
- *ni v uporabi*: sistem nima zahtevane funkcionalnosti in ni predmet ocenitve;
- *ni skladen*: rešitev ni zadostna, ampak je pomanjkljiva in kot takšna ni zadovoljiva.

Poglavje B: Elektronski zapisi

6.2.1. §11.10: Nadzor za zaprte sisteme

A. **Validacija** - Računalniški sistem je validiran z upoštevanjem veljavnih standardov podjetja in regulatornih zahtev.

Zagotoviti moramo:

- A.1 *Natančnost* [§11.10(a)].

- A.2 *Zanesljivost* [§11.10(a)].
  (Glede na zahteve, za katere je bil sistem kvalificiran, preverjamo varnostne kriterije. Zanima nas trajanje življenjskega cikla sistema in morebitni odstopi sistema/porušitev sistema, netočni podatki …)

- A.3 *Dosledno nameravano delovanje* [§11.10(a)].
  (Sistem je načrtovan, izdelan in deluje v skladu s preddefiniranimi zahtevami in specifikacijami. To pomeni izvedbo validacije sistema glede na industrijske standarde.)

- A.4 *Sposobnost razločiti neveljavne in spremenjene zapise* [§11.10(a)].
  (Preverjamo nenormalne primere delovanja oziroma iščemo neskladnosti skozi zgodovino dogodkov ali druge sistemske funkcionalnosti. Uporabljamo teste, s katerimi potrdimo, da zaznavamo aktivnosti, kadar z zunanjimi programskimi orodji dodajamo, spreminjamo ali brišemo zapise. Posebno pozorno preverimo »ad-hoc« orodja za vzdrževanje podatkovne baze in preverimo, kdo ima do njih dostop. Pregledamo postopke sistemskega načrtovanja in uporabe, da izluščimo morebitne vgrajene mehanizme (kombinacije preverjanja vpisov, zaščite in validacije podatkov), ki preprečijo ali zaznajo spremembo zapisov. Posebno pazljivo je treba pregledati potek medprocesnih komunikacij med nadrejenimi in podrejenimi programi, ki so izvedene z naročeno kodo.)

B. **Inšpektibilnost** - Načrtovani in uporabljeni postopki oziroma kontrole morajo zagotavljati:
(Inšpekciji morajo biti za pregled na voljo strojna oprema, programska oprema, zgodovina dogodkov in dokumentacija.)

- B.1 *Generiranje točnih in popolnih kopij zapisov v človeku čitljivi in elektronski obliki, ki bodo na voljo za potrebe inšpekcij, ponovnih pregledov in kopiranje* [§11.10(b)].
  (Računalniški sistem mora biti sposoben prikazati samo bistvo zahtevanih elektronskih zapisov. Če ni posebej zahtevano, inšpektorjem ne dajemo celovitih podatkovnih baz ali tabel.
  Podjetje mora biti sposobno na zahtevo inšpekcije ustvariti posamezen zapis, katerikoli del zapisa zgodovine dogodkov in celotno bazo podatkov tako v elektronski kot papirni obliki. Napisani morajo biti postopki, kako te naloge izvedemo in v kakšnem formatu naj bodo elektronski zapisi pripravljeni. Zagotovi moramo, da so vsi zahtevani elektronski zapisi

označeni z oznako »zaupno«, s čimer preprečimo nenadzorovano odtekanje občutljivih informacij podjetja.
Na zahtevo inšpektorjev mora biti omogočen pregled strojne, programske in sistemske dokumentacije ter zgodovine dogodkov.
Elektronske zapisi prikazujemo v elektronskem in papirnem formatu ter določimo izjeme.
V primeru, da je računalniški sistem geografsko deljen, moramo imeti pripravljene postopke in politike za izvedbo sočasnih pregledov na posameznih lokacijah.)

- B.2 *Zaščito zapisov, ki mora zagotoviti njihovo točnost, in sposobnost ponovne vzpostavitve v celotnem obdobju hranjenja zapisov* [§11.10(c)].
  (Preverimo politiko ponovne vzpostavitve zapisov. Ugotovimo, ali sistem to omogoča in preverimo, ali obstaja standardni postopek za vzpostavitev zapisov sistema. Vse zahteve veljajo tako za elektronske zapise kot za zgodovino dogodkov.
  Zapisi morajo imeti določeno življenjsko dobo, ki mora biti usklajena s politiko arhiviranja podjetja. Shranjeni morajo biti v tehnološko nevtralnem formatu. Upoštevana mora biti dobra praksa elektronskega arhiviranja.)

C. **Varnost** - Načrtovani in uporabljeni varnostni postopki in kontrole morajo zagotavljati:

- C.1 *Sistemski dostop, ki je omejen na pooblaščene posameznike* [§11.10(d)]
  (Samo pooblaščenemu osebju je dovoljen fizični dostop do strežnikov, sistemskih konzol, kritičnih sestavnih delov …)

- C.2 *Kontrolo operativnosti sistema, ki zagotavlja ustrezno zaporedje korakov v procesu* [§11.10(f)].

- C.3 Preverjanje pooblastil, s čimer zagotovimo, da samo pooblaščeni posameznik lahko:
  - C.3.1 *Uporablja dostop* [§11.10(g)] (logični dostop).
  - C.3.2 *Elektronsko podpiše zapis* [§11.10(g)].
    (Zahteva ne pride do veljave, dokler računalniški sistem ne uporablja elektronskih podpisov.)
  - C.3.3 *Dostopa do vhodnih in izhodnih naprav računalniškega sistema* [§11.10(g)].
  - C.3.4 *Spreminja zapise* [§11.10(g)].
  - C.3.5 *Izvede specifične operacije* [§11.10(g)].

- C.4 *Preverjanje naprave ali terminala, ki določata veljavnost vira vhoda ali operacije* [§11.10(h)].

D. **Zgodovina dogodkov** - Načrtovani in uporabljeni postopki in kontrole za zgodovino dogodkov morajo zagotoviti:
(Tudi spremembe, ki jih izvedejo sistemski administratorji ali skrbniki podatkovnih baz neposredno na podatkovnih strukturah bodisi zaradi vzdrževanja bodisi korekcije, morajo biti zapisane v operativno zgodovino

dogodkov. V nasprotnem primeru je treba izvesti proceduralno kontrolo teh zunanjih orodij, da ohranimo celovitost podatkov.)

- D.1 Varnost [§11.10(e)].
  (Zgodovina dogodkov mora biti varovana na ravni sistemskega administratorja. Ne sme dopuščati ročnih popravkov in mora zaznati dodajanja, spremembe in brisanja. Mora imeti sposobnost zaznavanje posegov z zunanjimi programskimi orodji.)

- D.2 *Računalniško generiranje zgodovine dogodkov* [§11.10(e)]

- D.3 *Časovno in datumsko žigosanje* [§11.10(e)].
  (Datumski in časovni zapisi so narejeni v uporabnikovem lokalnem času oziroma datumu in se prednostno uporabljajo za evidentiranje človekovih aktivnosti. Natančni morajo biti na 1 minuto.)

- D.4 Neodvisnost zapisa datuma in časa od operaterjevih vnosov in aktivnosti, in sicer z naslednjimi postopki:
  (Regulativa ne opredeljuje strojnih operacij, ki tečejo v ozadju, kot so pisanje v polnilnik ali vmesno datoteko. Njen namen je zagotoviti celovito spremljanje človekovih aktivnosti. Ni treba vpisati vsak nepomemben vpis, ampak se je treba osredotočiti samo na »kritična« polja ali/in operacije. Agencija ne vztraja, da nove tehnologije, kot so tajnopisi (kriptografska tehnologija), vsebujejo zgodovino dogodkov, ker so že sami po sebi dovolj varni.

  - D.4.1 *Kreiranje elektronskih zapisov* [§11.10(e)].
    (Za kreiranja elektronskega zapisa je potrebna prijava.)
  - D.4.2 *Spreminjanje elektronskih zapisov* [§11.10(e)].
    (Za spreminjanje elektronskega zapisa je potrebna prijava.)
  - D.4.3 *Vzdrževanje elektronskih zapisov* [§11.10(e)].
    (Za vzdrževanje elektronskega zapisa je potrebna prijava.)
  - D.4.4 *Brisanje elektronskih zapisov* [§11.10(e)].
    (Za brisanje elektronskega zapisa je potrebna prijava.)

- D.5 *Neokrnjenost predhodno zapisane informacije po spremembi elektronskega zapisa* [§11.10(e)].

- D.6 *Potrebno dobo vzdrževanja zapisa zgodovine dogodkov* [§11.10(e)].
  (Vsaj tako dolgo, kot je doba hranjenja podrejenih zapisov.)

- D.7 *Dostopnost zgodovine dogodkov za pregled in kopiranje s strani FDA* [§11.10(e)].

E. **Kvalifikacija osebja** - Izbrano osebje mora imeti primerno izobrazbo, prakso in izkušnje za izvedbo izbranih nalog. Mednje štejemo naslednje skupine osebja:

(Pri zaposlenem osebju zahtevam zadostimo, če imamo sprotne točne opise dela, zapise o izobraževanju in postopkih izobraževanja. Velik del šolanja je izobraževanje o dobri proizvodni praksi. Za zunanje osebe je potrebno pridobiti relevantne dokumente o izobraževanjih in izvesti nadzor njihovih postopkov izobraževanja.)

- E.1 *Razvijalci računalniških sistemov* [§11.10(i)].
  (Kvalifikacija razvijalcev sistemov je prav tako pomembna. Validacija ne zmanjšuje potreb, da je osebje ustrezno izobraženo, poučeno in ima izkušnje.)

- E.2 *Vzdrževalci računalniških sistemov* [§11.10(i)].
- E.3 *Uporabniki računalniških sistemov* [§11.10(i)].

F. **Premišljenost in odgovornost** - Objava napisanih politik in/ali postopkov obvezuje posameznika, da jih upošteva ter da premišljeno in odgovorno izvaja aktivnosti, povezane z elektronskimi podpisi, da tako prepreči ponarejanje zapisov in podpisov.
(Napisani postopki opisujejo odgovornosti uporabnikov glede uporabe računalniških sistemov in definirajo periodično menjavo gesel, prepoved posojanja gesel in izogibanje enostavnim geslom. Ne smemo vgrajevati nepreverjene programske pakete in uporabljati protivirusnih programov. Obstajati mora napisana politika, ki zagotavlja posameznikovo zavedanje in odgovornost za aktivnosti, sprejete z uvedbo elektronskih podpisov.)

G. **Kontrola sistemske dokumentacije** - Urediti in uporabiti moramo ustrezne kontrole za obvladovanje sistemske dokumentacije, ki morajo zagotavljati:

- G.1. Naslednje zadostne kontrole dokumentacije za sistemsko delovanje in vzdrževanje, ki zajemajo tele postopke:
  (Upoštevati moramo »pozitivni« in »negativni« vidik teh zahtev. Zagotoviti moramo, da imajo pravi ljudje pravo sistemsko dokumentacijo in da občutljive sistemske dokumentacije ne vidijo napačni ljudje. Pomembno je tudi, da imajo zaposleni pravilno in zadnjo verzijo navodil za delo in izvedbo vzdrževalnih postopkov.)

  - G.1.1 *Distribucija dokumentacije* [§11.10(k) (1)].
    (Zajema preverjanje distribucijskih listov tako formalnih kot »ad-hoc«.)
  - G.1.2 *Dostop do dokumentacije* [§11.10(k) (1)].
    (Varovati je treba poslovno »občutljive« dokumente.)
  - G.1.3 *Uporaba dokumentacije* [§11.10(k) (1)].

- G.2. Postopke revizij, kontrole sprememb in vzdrževanje zgodovine dogodkov ter razvoj časovnega zaporedja in modifikacije sistemske dokumentacije [§11.10(k) (2)].

6.2.2. §11.30: Nadzor odprtih sistemov

H. **Nadzor odprtih sistemov** - Pri odprtih sistemih, ki so uporabljeni za ustvarjanje, spreminjanje, vzdrževanje in prenos zapisov, mora elektronski sistem vsebovati načrtovane postopke in kontrole za zagotovitev naslednjih atributov za elektronske zapise:

- H.1 *Avtentičnost*. [§11.30]
- H.2 *Celovitost.* [§11.30]
  (Dodaten vidik je strukturna celovitost zapisa. Struktura zapisa je njegov fizični in logični format. Povezava med podatkovnimi elementi, ki obsegajo zapis, bi naj ostala fizično in logično nedotaknjena.)
- H.3 *Zasebnost*.[§11.30]

Uporabljeni postopki in kontrole morajo vsebovati:

- H.4 Tiste postopke in kontrole, ki so vsebovane v [§11.10] in so primerne za odprte sisteme.[§11.30]

- H.5 *Dokumentiran tajnopis, kjer je primerno* [§11.30].

- H.6 *Uporaba standardov digitalnega podpisa, kjer je primerno* [§11.30].
  (Zaupanja vredne elektronske podpise v njihovem življenjskem ciklu lahko ohranimo primerno potrebam in ocenitvi tveganja na dva načina.(National Archives and Record Administration, 2000, str. 8)
  Prvi pristop: Ohranjanje ustrezne prvotne dokumentacije o validaciji zapisov, kot so verifikacija zaupanja v zapise, zbrane v času podpisa zapisa. Dokazovanje avtentičnosti s pomočjo prvotne dokumentacije.
  Drugi pristop: Ohraniti sposobnost za ponovitev validacije digitalnega podpisa. Proces ponovne validacije zahteva, da podjetje ohrani sposobnost ponovne validacije digitalnega podpisa, skupaj s samim elektronsko podpisanim zapisom. Dokazovanje avtentičnosti s pomočjo rekonstrukcije postopka overitve.)

6.2.3. §11.50: Prikazovanje podpisa

I. **Povezava podpis-zapis** - Elektronsko podpisani zapis mora vsebovati informacije, ki jasno prikazujejo:
(Treba je ločeno preveriti vsak zaslonski prikaz in poročila, proizvedena z računalniškim sistemom, pri katerih bi lahko bil vsebovan elektronski podpis. Zelo pomembni so podpisi na vpisna polja zaslona.)

- I.1 *Natisnjeno ime podpisnika* [§11.50 (a)(1)].
  (Nesprejemljivo je prikazovanje drugih informacij, kot so identifikacijske kode uporabnikov ali zaposlenih oziroma nadomestek za izpisano ime podpisa. Prikazano pravo ime in priimek podpisnika mora biti preverjeno.)

- I.2 *Datum in čas, ko je bil podpis izveden* [§11.50 (a)(2)].
  (Lokalni čas se zapiše na minuto natančno.)

- I.3 *Namen podpisa* [§11.50 (a)(3)].

Vse informacije identificirane v [§11.50 (a)(1)], [§11.50 (a)(2)], [§11.50(a)(3)] velja:

- I.4 *da imajo popolnoma enak nadzor kot elektronski zapisi* [§11.50(b)],

- I.5 *da so kot del človeku berljive oblike elektronskega zapisa (tako v elektronskem prikazu in/ali izpisu ali poročilu)* [§11.50 (b)].

6.2.4. §11.70: Povezava zapis-podpis

J. Elektronski podpisi in ročni podpisi, izvedeni na elektronske zapise, so povezani z njihovim prvotnim zapisom, s čimer zagotovimo, da podpisi ne bodo izrezani, kopirani ali kako drugače preneseni na neobičajen način.
(Proceduralne oziroma administrativne kontrole same niso dovolj za zaščito avtentičnosti in verodostojnosti elektronskega podpisa. Uporabiti moramo novejše tehnologije, kot so tajnopisi, digitalni podpisi in druge.
Zahtevano je, da spremembe elektronskih zapisov ne smejo prepisati prvotnih vnosov.)

Poglavje C: Elektronski podpisi

6.2.5. §11.100: Splošne zahteve za elektronske podpise

K. Splošne zahteve.

- K.1 *Vsak elektronski podpis naj bo svojstven posamezniku, unikaten in ne sme biti zlorabljen ali dodeljen nekomu drugemu* [§11.100 (a)].
(Pri ocenitvi skladnosti preverjamo, če napisana politika in postopki nedvoumno zagotavljajo ustrezno funkcionalnost. Dopustno je, da ima ena oseba več elektronskih podpisov, dokler je jasno, čemu je posamezni podpis namenjen, npr. pregledu, odobritvi. 21 CFR Part 11 ne prepoveduje podjetju za namen branja uporabe skupinske identifikacije kode/geslo.)

- K.2 *Preden podjetje dodeli, pooblašča ali kako drugače odobri posamezniku elektronski podpis, je potrebno preveriti identiteto posameznika* [§11.100 (b)].
(Zaposleni morajo imeti veljavno številko zaposlenega ali drugo identifikacijo, ki jim omogoča vstop v podjetje. Pogodbeni ali začasni zaposleni morajo biti preverjeni, preden vstopijo v delovno območje. Napisane morajo biti politike in postopki, ki posamezniku onemogočajo ponarejanje elektronskih podpisov drugih oseb.)

- K.3 *Organizacije, ki uporabljajo elektronske podpise, skladne z zahtevami FDA, morajo v primeru uporabe le-teh o tem obvestiti FDA. S tem obvestijo agencijo, da je zanje elektronski podpis enakovreden ročnemu podpisu* [§11.100 (c)].

- K.4 *Certifikat se bo predložil v papirni obliki in bo podpisan s tradicionalnim ročnim podpisom, ki ustreza regulativi FDA*. [§11.100 (c)(1)].

6.2.6. §11.200: Sestavni deli elektronskega podpisa in kontrole

L. **Nebiometrični elektronski podpisi** - Elektronski podpisi, ki niso osnovani na biometrični metodi, morajo izpolnjevati tele zahteve:

- L.1 *Vsebovati morajo najmanj dva jasna identifikacijska sestavna dela, kot sta identifikacijska koda in geslo* [§11.200 (a)(1)].
  (Tudi začetna identifikacija ob vstopu v sistem mora biti sestavljena iz dveh identifikacijskih sestavnih delov.)

- L.2 *Kadar posameznik izvede vrsto podpisov v posameznih stalnih periodah kontroliranega sistemskega dostopa, pri prvem podpisu uporabi vse sestavne dele elektronskega podpisa. Dodatno podpisovanje izvede z uporabo najmanj enega sestavnega dela elektronskega podpisa. Sistem je načrtovan tako, da ga lahko uporabi lahko samo ta posameznik* [§11.200 (a)(1)(i)].

- L.3 *Ko po pretečenem času, posameznik ne izvede enega ali več podpisov pri uporabi kontroliranega dostopa do sistema, se bo vsak naslednji podpis izvedel z uporabo vseh komponent elektronskega podpisa.* [§11.200 (a)(1)(ii)].

- L.4 *Podpis bo uporabil samo njegov pravi lastnik* [§11.200 (a)(2)].
  (Sistem ima lahko vgrajeno samodejno postavljanje identifikacijskih komponent na začetno vrednost le takrat, ko ima sistem vgrajeno funkcionalnost, ki prisili uporabnika v takojšnjo spremembo gesla po prvi identifikaciji z začetnim geslom ali, če je čas med postavljanjem osnovne konfiguracije gesel in zahtevani čas za prvo identifikacijo tako kratek, da so možnosti ponarejanja zapis-podpis minimalne.)

- L.5 *Elektronski podpis bo administriran in izveden tako, da poskus uporabe drugih oseb posameznikovega elektronskega podpisa razen pravega lastnika zahteva sodelovanje dveh ali več posameznikov*. [§11.200 (a)(3)]
  (V sistemih, kjer se elektronski podpis izvede z uporabo identifikacijske kode in gesla ter kjer so identifikacijske kode znane in enostavno določljive, je nesprejemljivo, da bi kdorkoli poznal posameznikovo geslo; to velja tudi za administratorja. Dosledno je treba nadzorovati programska orodja, s katerimi lahko spreminjamo elektronske zapise ali podpise; tako z uporabo ročnih postopkov, delegiranjem obveznosti in kontrole na osnovi novejših tehnologij.)

M. Biometrični elektronski podpisi

Elektronski zapisi, ki so osnovani na biometrični metodi, morajo biti načrtovani tako, da zagotovijo uporabo samo pravim lastnikom [§11.200 (b)]

6.2.7. §11.300: Kontrole za identifikacijsko kodo in geslo

N. **Kontrole identifikacijskih kod in gesel** - Osebe, ki uporabljajo elektronske podpise, ki so sestavljeni iz identifikacijske kode in gesla, morajo v svoje delovanje vključiti kontrole, ki zagotavljajo njihovo varnost in celovitost:

- N.1 *Kombinacija identifikacijske kode in gesla mora biti neponovljiva* [§11.300 (a)].

- N.2 *Obnavljanje gesel je treba periodično preverjati in revidirati* [§11.300(b)].
  (Pokrijemo takšne dogodke, kot so staranje gesel. Če računalniški sistem nima vgrajene funkcionalnosti, ki zahteva periodično obnavljanje gesel, morajo biti uvedeni ročni postopki in ustrezna zgodovina dogodkov. Poleg postopka za pretek gesla moramo vključevati tudi druge metode, kadar je to potrebno.)

- N.3 Pri napravah, ki vsebujejo ali proizvajajo identifikacijske kode ali gesla, moramo zagotoviti načrtovanje in uporabo naslednjih postopkov in kontrol:

  - N.3.1 *Če je naprava izgubljena, ukradena ali ne deluje, moramo ukiniti elektronsko avtorizacijo* [§11.300 (c)].
  - N.3.2 *Začasne ali trajne zamenjave morajo potekati pod strogim nadzorom* [§11.300 (c)].

- N.4 Varnostni ukrepi:

  - N.4.1 *Zaščititi identifikacijske kode in gesla pred nepooblaščeno uporabo* [§11.300(d)].
    (Obstajati morajo postopki in sistemske funkcije, s katerimi prekličemo pravico dostopa, kadar se poskušajo vnesti neveljavne kombinacije identifikacijske kode in gesla. Neaktivne uporabniške identifikacijske kode in gesla nepooblaščeno osebje ne sme aktivirati. Izvedeno mora biti ustrezno izobraževanje, s katerim zagotovimo, da osebje razume pomen gesel in posledice v primeru zlorabe.)

  - N.4.2 *Zaznan mora biti vsak poskus nepooblaščene uporabe identifikacijskih kod in/ali gesel* [§11.300 (d)].
    (Računalniški sistemi morajo zaznati nepooblaščeno uporabo sistema in o njej poročati. Enostavnih napak, npr. nepravilnega vnosa ob tipkanju, naj se ne obravnava kot poskus nepooblaščenega vstopa, ampak moramo biti pozorni na vzorce napak, posebej če si sledijo v kratkem zaporedju.)

  - N.4.3 *O vsakem poskusu nepooblaščene uporabe identifikacijskih kod in gesel je treba takoj poročati varnostni enoti in, če je potrebno, tudi vodstvu* [§11.300 (d)].
    (Obstajati morajo splošni postopki, ki predpisujejo pogoje pod katerimi varnostna struktura komunicira z vodstvom, prav tako morajo biti predpisane odgovornosti in zahtevane aktivnosti ob morebitnem vdoru. Postopki zahtevajo periodični pregled varnostne strukture vseh računalniških sistemov, ki jih obravnava 21 CFR Part 11, s katerim ugotovimo ali obstaja morebitna varnostna luknja.)

- N.5 *Naprave, na katerih uporabljamo identifikacijske kode in gesla ali jih same proizvajajo, moramo periodično testirati* [§11.300 (e)].
  (Zagotoviti moramo, da na napravi niso bile izvedene nepooblaščene spremembe in da so neokrnjene kljub uporabi in premeščanju.)

6.3. Skrbnik sistema

Ugotoviti moramo, ali je skrbnik sistema primeren in ustrezno usposobljen ter vpliv človeškega faktorja na oceno skladnosti. Pri usposobljenosti govorimo o potrebnih kvalifikacijah in izkušnjah. Pri tem ocenjujemo njegove dosežke, kot so dosežena raven splošne izobrazbe, pridobljeno znanje, izkušnje, priporočila in sprejemljivost njegovega vedenja.

Pri primernosti ugotavljamo, ali se kandidat ujema z ekipo, naravo dela, organizacijo podjetja in ali se je sposoben vključiti v timsko delo. Iščemo naslednje lastnosti:
- splošno nadarjenost,
- vsestranskost,
- kandidatovo lastno oceno osebnostnih kakovosti in lastnosti,
- kako dobro se bo skrbnik ujel z drugimi sodelavci.

Skrbnik sistema je med potekom ugotavljanja skladnosti sistemov odgovoren za njegov zagovor. Na končno oceno skladnosti pomembno vpliva subjektivni moment, ki se zrcali v načinu zagovora sistema. S tem je lahko ocena skladnosti boljša ali slabša od dejanskega stanja.

Zaloga vrednosti za skrbnika sistema:
- *odličen*: velika verjetnost, da dobi sistem boljšo oceno od dejanske,
- *dober*: sistem dobi dejansko oceno,
- *povprečen*: skrbnik nima vpliva na oceno sistema,
- *slabši*: obstaja verjetnost, da dobi sistem slabšo oceno od dejanske.

Skladnost sistema se posredno vrednoti s sposobnostjo osebe, ki ga predstavlja.

6.3.1. Znanje

Vrednotimo osnovno znanje, ki je formalno pridobljeno in potrjeno v sklopu izobraževanj, ter dodatno poznavanje sistemov v obliki »tihega znanja«.

Zaloge vrednosti za skrbnikova ključna znanja:
- *ustrezno*: skrbnik sistema ima vsa potrebna znanja,
- *zadovoljivo*: skrbnik sistema ima večino potrebnih znanj,
- *povprečno*: skrbnik sistema ima le del potrebnih znanj,
- *nezadovoljivo*: skrbnik sistema nima potrebnih znanj.

6.3.2. Strokovna izobrazba

Ocenjujemo formalno strokovno izobrazbo skrbnika sistema. Večinoma obravnavane teme zahtevajo strokovno poznavanje področja od osnovnih do specialističnih znanj, ki si jih pridobimo s formalno izobrazbo. Tudi sam skrbnik je del ocene skladnosti v okviru organizacijske sheme in ustrezne usposobljenosti.

Zaloge vrednosti za formalno strokovno izobrazbo skrbnika sistema:
- *0-2*: (0 - doktor znanosti, 1 - magister znanosti, 2 - visoka strokovna izobrazba)
- *3-4*: (3 - višja strokovna izobrazba, 4 - srednja strokovna izobrazba)
- *5*: (5 - nižja strokovna izobrazba)
- *6-9*: (6 -visoka kvalifikacija, 7 – kvalificiran, 8 - polkvalificiran, 9 – nekvalificiran)

6.3.3. Poznavanje sistema

Zanima nas osnovno formalno potrjeno znanje (izobraževanja, uvajanja ...) in strokovno poznavanje sistema v obliki »tihega znanja«, ki je zelo težko merljivo, vendar se lahko po nekem časovnem obdobju kaže v izstopajočih rezultatih v primerjavi z drugimi v okolici, tako v sami izvedbi skladnosti kot njenem zagovoru. Govorimo o uspešnih referencah skrbnika.

Zaloge vrednosti za skrbnikovo poznavanje sistema:
- *odlično*: skrbnik ima formalno znanje in dobre osebnostne reference,
- *dobro*: skrbnik ima formalno znanje,
- *povprečno*: skrbnikovo formalno znanje je nepopolno,
- *slabše*: skrbnikovo formalno znanje je zelo pomanjkljivo.

Reference skrbnika ne smemo zamenjati s pridobljenimi izkušnjami; slednje si skrbnik pridobi s časom.

6.3.4. Tuji jeziki

Ocenjevanje skladnosti poteka v mednarodnem prostoru, zato je uradni jezik angleščina. V tem jeziku je napisane tudi večina dokumentacije, zato je poznavanje jezika pomemben osnovni pogoj za medsebojno razumevanje in izražanje jasnih misli.

Zaloga vrednosti za skrbnikovo formalno poznavanje tujega jezika:
- *aktivno*: aktivno poznavanje angleškega jezika,
- *pasivno:* pasivno poznavanje angleškega jezika,
- *nepoznavanje*: nepoznavanje angleškega jezika.

6.3.5. Leta

Kriterij je tudi število delovnih let kandidata na določenem sistemu. V nekem obdobju sistem dodobra spoznamo in z njim »zaživimo«. To prinaša določene prednosti, vendar, kot smo ugotovili v raziskavi človeškega faktorja, tudi slabosti. Pomembno vlogo ima tretja stran, tj. »kontrola kakovosti«, ki lahko ocenjuje sistem neodvisno oziroma neobremenjeno.

Zaloga vrednosti:
- *dobro*: več kot 5 let,
- *povprečno*: od 1 do 5 let,
- *slabše*: do 1 leta.

Zaloge vrednosti se neposredno nanašajo na izkušnje.

6.3.6. Izkušnje

Zanimajo nas pridobljene izkušnje oziroma intuicija.
Zaloge vrednosti:
- *več kot 5 let*: več kot 5 let delovnih izkušenj in intuicija,
- *od 1 do 5 let*: med 1 in 5 let delovnih izkušenj,
- *0 let:* do 1 leta delovnih izkušenj.

6.3.7. Osebne lastnosti

Definiramo primernost kandidata kot skrbnika sistema. Označujejo ga njegov nastop, prilagodljivost in dinamičnost.
Zaloge vrednosti:

- *dobre:* skrbnik sistema ima več izrazitih dobrih lastnosti,
- *povprečne*: skrbnik sistema ima več dobrih lastnosti,
- *slabše*: skrbnik sistema ima manj dobrih lastnosti.

Pri vrednosti sestavljenih kriterijev se upoštevajo vplivi oziroma uteži posameznih kriterijev na višje kriterije.

6.3.8. Nastop

Merimo sposobnost za predstavitev sistema in postopkov. Od kandidata pričakujemo naslednje lastnosti:

- zaupanje vase (eksperti obvladujejo svoje področje);
- sposobnost pozornega poslušanja, izogibanje dvoumnostim ali sovražnostim;
- na vprašanja odgovarja jasno, vendar le tisto, kar je vprašan;
- pri nerazumevanju vprašanja prosi za pojasnilo;
- izkazuje spoštovanje do sodelavcev.

Pomembno je poznavanje internih postopkov, npr. Sistemskega splošnega postopka za vodenje inšpekcij in presoj partnerjev/kupcev v Lek d.d., Ljubljana, 2001.

Zaloge vrednosti:

- *ustrezno*: poseduje vse lastnosti dobrega nastopa,
- *zadovoljivo*: poseduje bistvene lastnosti dobrega nastopa,
- *povprečno*: poseduje le del lastnosti dobrega nastopa,
- *nezadovoljivo*: slab nastop.

Več ko ima skrbnik želenih lastnosti skrbnika sistema, ugodnejša je njegova ocena. Ocena je lahko zelo subjektivna, vendar je treba ocenjevati v duhu splošnih družbenih norm.

V analizi človeških faktorjev je prikazan pristop »naravne odločitve«, po katerem lahko podjetje odstop spremeni v prednost.

6.3.9. Prilagodljivost

Ocenjujemo skrbnikovo sposobnost prilagoditve različnim stanjem in delo z dokumentacijo.
Zaloge vrednosti:

- *ustrezno*: različnim stanjem se takoj prilagodi »naravni talent«,
- *zadovoljivo*: različnim stanjem se prilagodi s pomočjo učenja,
- *povprečno*: različnim stanjem se prilagodi odvisno od razpoloženja,
- *nezadovoljivo*: različnim stanjem se težko prilagodi.

Prilagodljivost lahko določimo z analizo človeških faktorjev z uporabo metode »naravne odločitve«. (gl. pogl. Ljudje in človeški faktor)

6.3.10. Dinamičnost

To je sposobnost hitrega iskanja rešitev in prevzemanja vlog. Pri tem je pomembno, kako so določene primarne vloge in odgovornosti ključnih oseb, ki so vpletene v posamezne dogodke. Osebje mora biti seznanjeno, kaj vse se lahko od njega pričakuje. Med potekom inšpekcije si ažurno zapisuje dogajanje (sodelujoči, pregledana dokumentacija, vprašanja in odgovori, želene spremembe postopkov ali korektivni ukrepi).

Zaloge vrednosti:

- *ustrezno*: izpolni vsa pričakovanja in izvaja potrebne aktivnosti,
- *zadovoljivo*: izvaja potrebne aktivnosti,
- *povprečno*: delno izpolni pričakovanja in izvaja le del aktivnosti,
- *nezadovoljivo*: ne izpolni naša pričakovanja.

6.4. Zagotavljanje kakovosti

Za doseganje celovite kakovosti mora obstajati celostno oblikovan in pravilno izvajan sistem zagotavljanja kakovosti, ki vključuje dobro proizvodno prakso in s tem tudi kontrolo kakovosti. Za vse dele sistema velja, da jih mora izvajati kompetentno osebje, v primernih prostorih, z ustrezno opremo in infrastrukturo. Za doseganje ciljne kakovosti farmacevtskega podjetja je odgovorno vodstvo, medtem ko je glavni nosilec za uvedbo in uporabo politike regulatorne skladnosti podjetja organizacijska funkcija zagotavljanja kakovosti.

Nastopa kot odgovorni nosilec vseh aktivnosti in postopkov za zagotavljanje kakovosti v podjetju, ki posamično ali skupno vplivajo na kakovost izdelka. Je nosilec izdelave splošnih smernic za izvajanje validacij računalniških sistemov in potrjevanja ustreznosti posameznih sistemov oziroma procesov podjetja (validacija računalniških sistemov) na osnovi izvedenih validacijskih aktivnosti v celoti.
Potek potrebne izvedbe je zapisan v planu validacije.
Zaloge vrednosti:

- *ustrezno:* sistem kakovosti je ustrezen,
- *delno ustrezno*: sistem kakovosti je pomanjkljiv,
- *neustrezno*: sistem kakovosti je neustrezen.

Izbrano zalogo vrednosti določa vrednost sestavljenih kriterijev (vpliv na kakovost, inšpektibilnost, zahtevnost trgov in podpora vodstva), pri čemer se upoštevajo vplivi oziroma uteži posameznih kriterijev na višje kriterije.

6.4.1. Vpliv na kakovost

Vpliv na kakovost obravnavamo v okviru ocenjevanja vpliva sistema na kakovost in varnost izdelka.
Poznamo naslednje kategorije odstopov:

- kritični odstop: neposredno vpliva na učinkovitost, varnost in neškodljivost zdravila,
- večji odstop: neskladnost izdelka ali postopkov z registracijsko dokumentacijo,
- drug odstop: ne spada med kritična ali večje, pa vendar gre za odstop od GxP,

- ni odstopa: ni odstopa od GxP.

Zaloga vrednosti pri vplivu možnih odstopov na kakovost izdelka:
- v*elik vpliv*: neposredno vpliva na učinkovitost, varnost in neškodljivost zdravila,
- s*rednji vpliv*: neskladnost izdelka ali postopkov z registracijsko dokumentacijo ne spada med kritična , pa vendar gre za odstop od GxP,
- m*ajhen* vpliv: nima bistvenega vpliva na kakovost

Zgornja kategorija odstopov že definira končno lastnost odstopa (upoštevati je treba kompleksnost morebitnega odstopa). Upoštevani so vsi znani vplivni faktorji in predstavlja trenutno oceno skladnosti, medtem ko nam zaloga vrednosti predstavlja samo morebitni vpliv na velikost odstopa.

6.4.2. Inšpektibilnost

Organizacija, ki ni skladna z zahtevano regulativo, lahko postane predmet enega od številnih ukrepov: prejme opozorilno pismo (npr. Form 483), ki povzročijo zastoj pri izdelavi zdravil ali celo njihove odpoklic s trga ali zaprtje obrata. Izbira ukrepa je odvisna od narave in obsega prekrška ter prejšnje zgodovine pregledov. Po drugi strani pa lahko te aktivnosti pomenijo poslovno priložnost, prinašajo izkušnje in so priložnost za pridobivanje novih spoznanj, ki jih lahko postopoma vgradimo v uporabljen model.

Bolje ko je podjetje pripravljeno na inšpekcijo, manj je poznejših stresnih stanj in uspešnejše je lahko njegovo delovanje.

Zaloga vrednosti za različne vrste nadzora narejena na posameznem informacijskem sistemu:
- *3*: uspešna inšpekcija regulatornih organov (FDA)
- *2*: uspešna zunanja presoja,
- *1*: uspešna partnerjeva presoja,
- *0*: ni bilo nobene uspešne presoje.

Ti kriteriji imajo vgrajeno nekakšno zgodovino dogodkov inšpektibilnosti sistema in predstavljajo že doseženo stopnjo skladnosti (ustrezne reference presoj, zapisnikov...).

Večje tveganje predstavljajo spremembe na sistemu ali spremembe na procesu, kot je prikazano tudi v modelu. V tem delu sta pomembna tako kvantitativna (gl. teorijo odstopov) kot kvalitativna komponenta presoj (multidisciplinarne presoje).

Inšpekcije delimo (Mlcolm Dixon, 2001, str. 6):

a) glede na doseg: sistemske inšpekcije FDA se lahko izvajajo v polnem obsegu, tako da se izvaja celovita ocena skladnosti ali pa se izvaja skrajšana inšpekcija, npr. če ima podjetje že dokumentirano ustrezno skladnost, nima odpoklicev ali drugih alarmantnih dogodkov v zadnjih dveh letih (poudarek je le na posameznih segmentih modela);

b) ciljane inšpekcije: inšpekcije se izvajajo v polnem obsegu in na področja, kjer so predhodno že bili odkriti odstopi.

6.4.3. Zahtevnost trgov

Ko vrednotimo zahtevnost trga, nas običajno ne zanima geografska lega, ampak za ta trg veljavna regulativa. Zdravilo kot izdelek mora biti vedno ustrezno, razlikujemo samo intenzivnost potrebnih aktivnosti za zagotovitev potrebne skladnosti z zakonodajo.
Zaloge vrednosti:

- *velika*: regulatorno zahtevni trgi,
- *srednja*: regulatorno običajni trgi,
- *mala*: nezahtevni trgi.

Informacijski sistemi, ki so načrtovani za zahtevne trge, so že po definiciji skladni tudi za ostale trge.

6.4.4. Podpora vodstva

Podpora vodstva podjetja procesu zagotavljanja skladnosti informacijskih sistemov pomeni poleg strateške usmeritve tudi zagotovitev ustreznih finančnih in človeških virov. Tu se pojavljajo številne pasti in nevarnosti. Odgovorno osebje mora imeti ozadje, znanje, izkušnje ali vire za zagotovitev skladnosti.

Največji izziv je ustrezna organizacijska struktura. Osebje, ki mu je dodeljena odgovornost za izvedbo, pogosto nima potrebnih pooblastil za doseganje sprememb v celotni strukturi organizacije. Delne in kompromisne rešitve povzročajo nestabilnosti v kompleksnih sistemih.

Zaloge vrednosti:

- *velika*: strateška usmeritev in pooblaščanje,
- *srednja*: strateška usmeritev,
- *majhna*: verbalna podpora,
- *nezadostna*: neopredeljeno.

6.5. Spremembe

Spremembe se v okviru odločitvenega modela obravnavajo in potrjujejo z ovrednotenjem elementov revalidacije. (Robert W. Stotz, 2002, str. 12) Formalno in dejansko se sprememba lahko uvede šele po uspešno zaključeni revalidaciji sistema. Pred uvedbo spremembe moramo izbrati odgovorne nosilce za njeno izvedbo in določiti potrebne človeške in finančne vire ter zanjo pridobiti odobritev.

Vzemimo, da imamo v času življenjskega cikla sistema množico S = $\{s_1, s_2, s_3,\ldots,s_n\}$, pri čemer je S končna množica sprememb, s je sprememba v postopku ali pa je že izvedena. Kadar ni večjih sprememb na sistemu ali so spremembe izvedene v smislu izboljšav, običajno govorimo o stabilnih in preverjenih sistemih. Večjo število sprememb ali sprememba zaradi kritične napake že zmanjšuje zaupanje v sisteme in lahko že pomeni določeno stopnjo neskladnosti v procesih podjetja. Največkrat se zgodijo v določenih segmentih sistema in predstavljajo napake v načrtovanju sistema.

Veliko utež vplivnosti posamezne spremembe daje analiza rizičnosti za kritične operacije; narejena mora biti tako temeljito kot analiza skladnosti.

Zaloge vrednosti za izvedeno spremembo:
- *odobrena*: sprememba se izvaja v skladu s postopki in politiko sprememb,
- *ni v uporabi*: sprememb ali ni ali pa so takšne, da ne potrebujejo potrditve skupine za spremembe,
- *ni odobrena:* sprememba je v postopku uvedbe oziroma še ni bila odobrena.

V primeru, da v samem življenjskem ciklu sistema ni bilo izvedene spremembe, izberemo odločitveno pravilo *ni v uporabi.*

6.5.1. Vpeljan sistem in odgovornosti za obvladovanje sprememb

V podjetju mora biti vpeljan sistem obvladovanja sprememb tako na organizacijski kot vsebinski (npr. računalniški sistemi) ravni. Zagotovljene in potrjene morajo biti dejanske ravni odgovornosti in pristojnosti.

Zaloga vrednosti:
- *primerna*: zagotovljene in potrjene so dejanske ravni odgovornosti;
- *pomanjkljiva*: ravni odgovornosti so postavljene preveč ohlapno oz. neformalno.

6.5.2. Analiza spremembe z možnimi tveganji na kritične operacije procesov

Izvede se analiza spremembe z možnimi tveganji za kritične operacije, pri katerih ugotavljamo vpliv spremembe na proces. Rezultate rizičnih analiz in morebitni vpliv na kritične operacije procesov potrjujemo s splošno predpisanimi postopki (npr. v okviru skupine za spremembe).

Zaloga vrednosti morebitnih tveganj:

- *kritično*: analiza spremembe ni bila narejena oziroma ni bila potrjena,
- *velika*: analiza sprememb prikazuje velik vpliv na kritične operacije,
- *majhna*: analiza sprememb prikazuje manjši vpliv na kritične operacije oziroma sploh nima vpliva.

6.5.3. Definiranje vpliva na regulatorni status računalniškega sistema

Izvede se analiza, s katero ovrednotimo vpliv spremembe na regulatorni status računalniškega sistema.

Zaloga vrednosti:
- *velik*: sprememba ima velik vpliv na regulatorni status,
- *majhen*: sprememba nima vpliva na regulatorni status računalniškega sistema.

6.5.4. Plan in izvedba testiranja

Ti testni postopki obravnavajo vse mejne vrednosti projekta, dovoljena območja predvidenih sprememb na računalniškem sistemu in vpliv spremembe na integralni sistem. Obravnavanje poteka v smislu načrtovanja celovitega plana testiranja same spremembe na nivoju računalniškega sistema.

V kasnejši izvedbi posameznih testov, potrjujemo pravilno funkcionalnost in zgradbo izvedenih sprememb glede na potrjeno specifikacijo uporabnika.
Z postopki želimo potrditi skladnost izvedenih sprememb z obstoječimi rešitvami in ohraniti celovitost že izvedenih predhodnih ustreznih rešitev.

Zaloga vrednosti:
- *zadovoljivo*: upoštevani so vsi testi postopkov načrtovanja,
- *nezadovoljivo*: nekateri testi postopkov načrtovanja niso upoštevani.

6.5.5. Popravilo vseh dokumentov in evidentiranje sprememb

Raven dokumentiranosti je odvisna od kritičnosti funkcij sistema, ki jih obravnavamo. Izvedemo obnovo delovne in kvalifikacijske dokumentacije, in sicer:
- obnovo uporabniških navodil,
- obnovo dokumentacije programa,
- obnova trenutnih operativnih standardnih postopkov delovanja.

Zaloga vrednosti:
- *obnovljeni*: uspešno izvedene zahtevane obnove, označevanje verzij dokumentov in dokumentirana zgodovina sprememb je ustrezna,
- *delno*: zahtevane obnove so nepopolne,
- *pomanjkljivo*: obnove niso izvedene v vsem obsegu, označevanje verzij dokumentov in dokumentirana zgodovina sprememb je pomanjkljiva.

6.5.6. Potrditev spremembe

Zaloge vrednosti za izvedeno spremembo:
- *odobrena*: sprememba je odobrena,
- *ni odobrena:* sprememba je v postopku uvedbe oziroma še ni bila odobrena.

6.6. Arhiv

Postavitev strategije elektronskega arhiviranja je pomembna, vendar pa sama po sebi ne predstavlja samodejnega zagotovila, da bo organizacija imela dolgoročni dostop do zaupanja vrednih in za obdelavo primernih elektronskih zapisov tudi še v prihodnosti.
Strategijo elektronskega arhiviranja je treba prevesti v »dobro prakso elektronskega arhiviranja«, s katero organizacija zagotavlja njeno uporabo.

Sledi pregled posameznih podrobnosti dobrih praks, ki so del podsistema odločitvenega modela. Pregled je razdeljen na politiko elektronskega arhiviranja, postopke, varnost in spominske medije.

Posebej obravnavamo metode in postopke za izmenjavo podatkov oziroma prehod na nov sistem, ki jih priporoča FDA z namenom lažjega in referenčnega zagovora uporabljenih rešitev.

6.6.1. Politika elektronskega arhiviranja

Politika elektronskega arhiviranja je pomembna, ker podpira jasen pogled na elektronske zapise in pomaga zagotoviti dosleden, enoten postopek obravnave in rabe. Politika definira objektiven pristop k elektronskemu arhiviranju, izražen v obveznosti podjetja do načel elektronskega arhiviranja, uvajanja »dobre prakse« elektronskega arhiviranja, identifikaciji individualne ali skupne odgovornosti podjetja in zagotavljanju periodičnega neodvisnega preverjanja aktivnosti elektronskega arhiviranja.

Zaloge vrednosti:
- *celovita*: zajeti vsi atributi elektronskega arhiviranja,
- *pomanjkljiva*: napisana politika je nepopolna,
- *nezadostna*: izpuščeni so ključni atributi elektronskega arhiviranja.

6.6.2. Postopki

Vse aktivnosti, ki so izpeljane iz dobre prakse elektronskega arhiviranja, morajo biti skladne s predpisanimi splošnimi in izpeljanimi postopki.

To dokumentacijo obravnavamo enako pazljivo in skrbno kot elektronske zapise same. Informacije v okviru zagotavljanja kontrole kakovosti arhiviranih podatkov postavimo v zbirno datoteko, ki ohranja povezavo z izvornimi elektronskimi zapisi.

Seznami zapisov so poslovna pravila, ki označujejo vrste zapisov in iztek življenjskega cikla zapisa.

Ti seznami morajo biti dopolnjeni:
- pri kreiranju novih zapisov,
- kadar vključitev dopolnjenega elektronskega zapisa vpliva na spremembo izteka prvotnega življenjskega cikla zapisa,
- kadar dodatno vključimo elektronski podpis.

Zaloge vrednosti:
- *skladni*: dokumentacija in aktivnosti ustrezajo predpisanim postopkom,
- *pomanjkljivi*: samo dokumentacija ali samo aktivnosti ustrezajo predpisanim postopkom,
- *nezadostni*: dokumentacija in aktivnosti ne ustrezajo predpisanim postopkom.

Pri prehodu na drug ali novejši sistem je treba izdelati popolne in točne kopije podatkov ter vseh pomožnih informacij, ki so potrebne za njeno celovitost v vsebini in kontekstu. Vsaka ponovna izmenjava podatkov mora biti dokumentirana in vzdrževana v življenjskem ciklu zapisa. Procesi transkripcije morajo biti validirani.

V ta namen običajno uporabljamo naslednje standardne metode in postopke, ki poteke validacij poenostavijo (Dollar, 2000, str. 31-32):javne standarde za izmenjavo podatkov, operativno aplikacijsko prenosljivost, migracije.

6.6.2.1. Javni standardi za izmenjavo podatkov

Uporaba javnih standardov za izmenjave podatkov obsega ključne komponente v programu, ki pomagajo zagotoviti nadaljevanje možne obdelave elektronskih zapisov kljub spremembam proizvajalcev ali tehnoloških platform skozi čas. Poznamo dve osnovni obliki izmenjav: XPORT za podatke in protokol ANDI za laboratorijske analize.

6.6.2.2. Operativna aplikacijska prenosljivost

Aplikacijska operativna prenosljivost je prav tako ključni element pri bodoči obdelavi elektronskih zapisov. Z uporabo dveh različnih aplikacijskih sistemov zagotovimo enake rezultate analiz.

Na žalost je aplikacijsko operativno prenosljivost v veliki meri težko doseči v laboratorijskih podatkovnih sistemih, v katerih se pojavljajo težave ob uporabi pravilnega integracijskega algoritma in širokega niza opcij za izvedbo interpretacij in analiz. Ni enostavne rešitve za dosego aplikacijske operativne prenosljivosti, ki bi dala natančno enak rezultat, kot takrat, ko se »surovi« (izmerjeni) podatki obdelujejo na različnih laboratorijskih podatkovnih sistemih.

Ohranjanje združljivosti znotraj posameznih verzij je ena pot za izgradnjo aplikacijske operativne prenosljivosti, toda to zahteva nadaljevanje revizije podatkov in večje nadgradnje.

6.6.2.3. Migracije

Migracija označuje prenos elektronskih zapisov s pomočjo tehnologije nevtralne podatkovne izmenjave ali aplikacijske operativne prenosljivosti brez izgube vsebine, konteksta ali funkcionalnosti. Migracija elektronskih zapisov s pridruženo programsko funkcionalnostjo k novim tehnološkim platformam zahteva pisanje posebnih programov za prestavitev zapisov in funkcionalnosti v želeno aplikacijsko okolje.

Deset »selitvenih korakov« (Brodie,1995, str. 35) za selitev zapuščenih podatkovnih baz lahko uporabimo kot model migracije. Posebno kodo selitve lahko testiramo z vzorčnim elektronskim zapisom za preverjanje podatkovne celovitosti in programske funkcionalnosti. Priporoča se izdelava pisnega poročila o migraciji, v katerem so zaznamovane vse težave, ki so se pojavile; predvidi se tudi rešitev težave.

6.6.3. Varnost

Za zaščito elektronskih zapisov pred spremembami, brisanjem ali izgubo kritičnih komponent elektronskega arhiviranja vpeljujemo nekaj različnih, toda povezanih dobrih praks.

Prva linija obrambe pred spremembami ali morebitno izgubo elektronskih zapisov je njihov prenos iz okolja uporabe. Najprej jih zajamemo na trajen spominski medij, nato pa shranimo v enciklopedijo zapisov. V njej lahko pristopamo do elektronskih zapisov, jih beremo, kopiramo, vendar nikakor ne spreminjamo ali brišemo.

Zaščita elektronskih zapisov pred spremembami, brisanjem ali izgubo lahko prav tako vključuje postavitev enciklopedije v polje, kjer je možnost naravnih nesreč minimalna. Na nadomestni lokaciji mora biti vzdrževana celotna obnovitvena arhivska zrcalna kopija elektronskih zapisov v enciklopediji, t. i. »fail safe«.
Zaloge vrednosti varnosti:

- *zadostna*: zapisi so preneseni na varnostno lokacijo z arhivsko zrcalno kopijo,
- *pomanjkljiva*: zapisi so preneseni na varnostno lokacijo brez arhivske zrcalne kopije,
- *nezadostna*: zapisi so shranjeni na mestu uporabe.

6.6.4. Spominski mediji

Magnetni in optični medij sta dandanes široko uporabljana digitalna spominska medija, kljub temu, da so robustni spominski mediji že sami po sebi vprašljivi in je zato njihova trajnost in sposobnost branja lahko tvegana. Odstopanje od dovoljenih specifikacij (nizka temperature, nižja relativna vlaga itd.) lahko pomembno spremenijo pričakovano življenjsko dobo. Ni zagotovila, da spominski medij ostane trajen in berljiv skozi celotno predvideno pričakovano življenjsko dobo.

Zaloge vrednosti spominskega medija:

- *celovito*: spominski medij je vzdrževan v mejah specifikacij,
- *pomanjkljivo*: spominski medij ni v mejah specifikacij.

6.6.4.1. Obnovitev spominskega medija

Elektronsko arhiviranje predvideva, da zapisi ostanejo aktivni dolgo v prihodnost kljub spremembam v informacijski tehnologiji. Eden od načinov ublažitve učinka tehnološkega staranja elektronskih zapisov je razširitev uporabnosti z obnovo.

Obnova spominskega medija zajema kopiranje elektronskih zapisov s starega spominskega medija na nov medij z enako specifikacijo formata. Celovitost kopiranja in ponovnega oblikovanja elektronskih zapisov je lahko potrjena z uvedbo postopkov zagotavljanja kakovosti podatkov (Dollar, 2000, str. 29), kot je generiranje s pomočjo »zgoščevalnih funkcij s prstnim odtisom« ali CRC zapisov, ki jih lahko primerjamo z ustreznimi »zgoščevalnimi funkcijami s prstnim odtisom« ali CRCs generiranimi zapisi po obnovi ali kopiranju.

Kriterij za izbiro medija je napovedana pričakovana življenjska doba, spominska kapaciteta, hitrost podatkovnega prenosa, ohranjanje združljivosti sistemov, možnost pomoči, primernost itd.

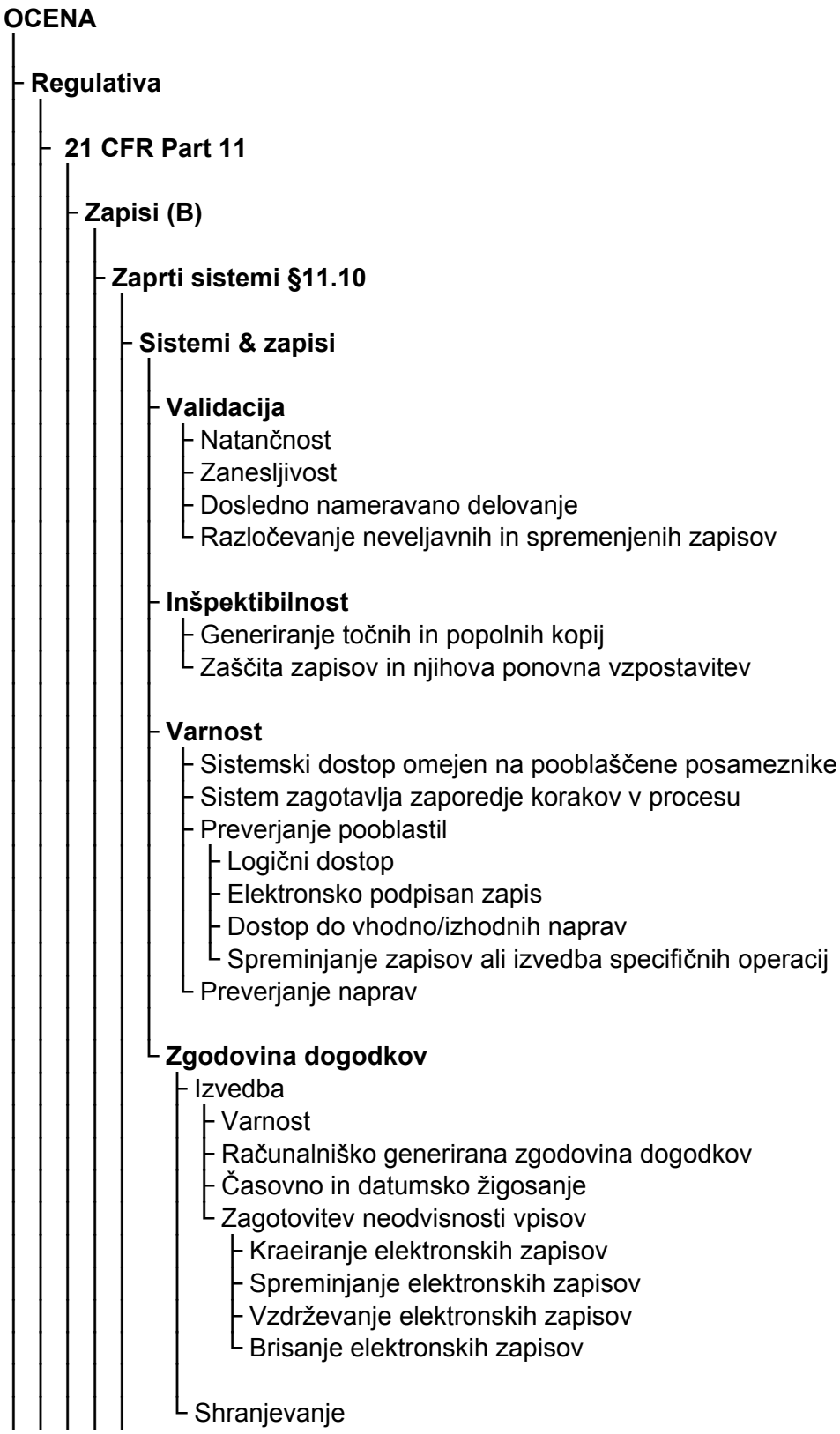
Čas, ko se zgodi kopiranje ali obnova, je odvisen od nadgradnje večjega sistema, instalacije nove tehnološke platforme, predvidene pričakovane življenjske dobe spominskega medija ali je posledica rezultata periodičnih inšpekcij.

Čas nadgradnje večjih sistemov ali instalacije nove tehnološke platforme je nekako nepredvidljiv. Obnova spominskega medija naj bi se izvedla vsakih deset let ali po koncu prve polovice realno pričakovane življenjske dobe za pogone, s katerimi beremo spominski medij. (Dollar, 2000, str. 30)

6.7. Izdelava drevesa kriterijev

6.7.1. Drevo kriterijev

Slika 16: Drevo kriterijev



- Spremembe ne smejo okrniti predhodnih informacij
- Vzdrževanje zapisa zgodovine dogodkov
- Dostopnost zgodovine dogodkov za pregled in kopiranje

Osebje in dokumentacija
- Kvalifikacija osebja
  - Razvijalcev računalniških sistemov
  - Vzdrževalcev računalniških sistemov
  - Uporabnikov računalniških sistemov
- Premišljenost in odgovornost
- Kontrola sistemske dokumentacije
  - Kontrola dokumentacije za sistemsko delovanje
    - Distribucija dokumentacije
    - Dostop do dokumentacije
    - Uporaba dokumentacije
  - Nadzor sistemske dokumentacije

Odprti sistemi §11.30
- Postopki in kontrole-atributi
  - Avtentičnost
  - Celovitost
  - Zasebnost
- Postopki in kontrole vsebujejo
  - Primerne postopke in kontrole iz §11.10
  - Dokumentiranje tajnopisa
  - Standarde digitalnega podpisa

Prikazovanje podpisa §11.50
- Elektronski podpis
  - Ime in priimek podpisnika
  - Datum in čas
  - Namen podpisa
- Povezava z zapisi
  - Nadzor
  - Čitljivost

Zapis in podpis §11.70
- Avtentičnost povezave

Podpisi (C)

Splošne zahteva za elektronske podpise §11.100
- Avtentičnost podpisa
- Identiteta posameznika
- Prijava uporabe
- Certifikat

Sestavni deli elektronskega podpisa in kontrole §11.200
- Nebiometrični elektronski podpisi
  - Identifikacijska koda in geslo

- Funkcionalnost neprekinjenega in prekinjenega dostopa
- Omogočena uporaba samo lastnikom podpisa
- Dodeljevanje nebiometričnih podpisov
- Biometrični elektronski podpisi

- **Kontrola za identifikacijsko kodo/ geslo §11.300**
  - Identifikacijska koda in geslo sta neponovljiva
  - Postopki in kontrole
    - Avtorizacija
    - Začasne ali trajne zamenjave
  - Varnostni ukrepi
    - Zaščita pred nepooblaščeno uporabo
    - Zaznavanje poskusa zlorabe
    - Poročanje o poskusu zlorabe
  - Periodično testiranje naprav

- **Spremembe**
  - Vodenje
    - Vpeljan sistem in odgovornosti za obvladovanje sprememb
    - Odobritev spremembe
    - Potrditev spremembe
  - Potek
    - Analiza spremembe z možnimi tveganji za kritične operacije
    - Definiranje vpliva na regulatorni status računalniškega sistema
    - Plan in izvedba testiranj
    - Popravilo vseh dokumentov in evidentiranje vseh sprememb

- **Arhiv**
  - Politika arhiviranja
  - Postopki
  - Varnost
  - Spominski mediji

- **Upravljanje kakovosti**
  - Vpliv na kakovost
  - Inšpektibilnost
  - Zahtevnost trgov
  - Podpora vodstva

- **Skrbnik**
  - Znanje
    - Poznavanje sistema
    - Poznavanje jezika
    - Strokovnost
  - Leta
    - Izkušnje
  - Osebne lastnosti
    - Nastop
    - Dinamičnost
    - Prilagodljivost

6.7.2. Osnovna odločitvena pravila

V programskem orodju DEXi so funkcije koristnosti predstavljene s preprostimi odločitvenimi pravili tipa »če-potem«. Vrednotenje odločitvenih pravil postavimo od listov do korena drevesa kriterijev.

Tabela, ki jo dobimo v korenu drevesa, predstavlja končno odločitveno tabelo.

Tabela 7: Končna tabela odločitvenih pravil

	Regulativa	**Skrbnik sistema**	**Upravljanje kakovosti**	**Ocena**
	33 %	14 %	53 %	
1	<=ni v uporabi	<=povprečen	**ustrezno**	**ni odstopa**
2	**skladen**	*	delno ustrezno	drugi
3	<=ni v uporabi	<=povprečen	delno ustrezno	drugi
4	<=delno skladen	**odličen**	delno ustrezno	drugi
5	**skladen**	**slabši**	<=delno ustrezno	drugi
6	<=ni v uporabi	**slabši**	**ustrezno**	drugi
7	delno skladen	**odličen**	<=delno ustrezno	drugi
8	delno skladen	<=povprečen	**ustrezno**	drugi
9	ni v uporabi	*	**neustrezno**	večji
10	ni v uporabi:delno skladen	**odličen**	**neustrezno**	večji
11	ni v uporabi	**slabši**	>=delno ustrezno	večji
12	delno skladen	dober:povprečen	delno ustrezno	večji
13	delno skladen	**slabši**	**ustrezno**	večji
14	**ni skladen**	<=dober	**ustrezno**	večji
15	**skladen**	*	**neustrezno**	**kritični**
16	>=delno skladen	>=dober	**neustrezno**	**kritični**
17	>=delno skladen	**slabši**	>=delno ustrezno	**kritični**
18	**ni skladen**	*	>=delno ustrezno	**kritični**
19	**ni skladen**	>=povprečen	*	**kritični**

Vir: Tabele odločitvenih pravil

Za posamezni sestavljeni kriterij DEXi že pripravi celotno tabelo možnih kombinacij vrednosti odvisnih spremenljivk. Izpolnimo samo zadnji stolpec, v katerem podamo vrednost sestavljenega kriterija za posamezno kombinacijo vrednosti odvisnih spremenljivk.

Pri zapisu odločitvenih pravil končne oceni skladnosti sistema izhajamo iz naslednjih predpostavk.

1. Posameznim zalogam vrednosti izbranemu kriteriju »Regulativa« ustrezajo naslednje ocene:
   zalogi vrednosti »skladen, ni v uporabi« ustreza ocena »ni odstopa«,
   zalogi vrednosti »delno skladen« ustreza ocena »večji«,
   zalogi vrednosti »ni skladen« ustreza ocena »kritični«.

2. Skrbnik sistema lahko oceno skladnosti v primeru robnih vrednosti zaloge vrednosti, kot je »odličen«, za eno raven predhodne ocene izboljša ali pa jo v primeru »slabši« za eno raven poslabša. V primeru, da ima kriterij »regulativa« zalogo vrednosti »ni v uporabi«, skrbnik sistema ne vpliva na predhodno ovrednoteno oceno.

3. V primeru, da ima kriterij »upravljanje kakovosti« zalogo vrednosti »neustrezno«, vedno govorimo o »kritični« oceni.
   Inšpektor običajno predhodno preveri sistem zagotavljanja kakovosti v podjetju. Če ugotovi, da je sistem napačno voden, se lahko aktivnosti inšpekcije s tem že končajo.

Posebej bi rad podrobneje prikazal osnovna odločitvena pravila, ki sem jih uporabil pri vrednotenju regulativne veje odločitvenega drevesa.

Na osnovni ravni imamo za posamezni atribut izbrane naslednje zaloge vrednosti: »*skladen, ni v uporabi, ni skladen«.* Njihovo oceno dobimo pri vrednotenju izbrane variante s pomočjo GAP analize sistema.

Izpeljanim atributom v prvem vozlišču z zalogo vrednosti: »*skladen, delno skladen, ni v uporabi, ni skladen«* določimo funkcijo koristnosti, ki določa njihovo vrednost glede na vrednost podrejenih atributov. Funkcijo koristnosti podamo z odločitvenimi pravili.

Poleg običajnih odločitvenih pravil upoštevamo naslednje povezave

- Če na vozlišču odločitvenega drevesa nastopa samo en atribut in ta »ni skladen«, potem se izpeljanemu atributu dodeli odločitveno pravilo »ni skladen«. S pravilom zagotovimo zaznavo spornega problemskega območja.

- Če nastopata dva ali več atributa in samo eden od atributov »ni skladen«, potem se izpeljanemu atributu dodeli odločitveno pravilo »delno skladen«. V praksi to pomeni, da sistem za obravnavano problemsko območje zahtevam regulative ne ustreza popolnoma, vendar pa smo odstop zaznali in ga v posameznih segmentih že obravnavamo.

Pri izpeljanem atributu v drugih vozliščih se omenjene odločitvena pravila nekoliko spremenijo.

- Če ima eden ali več atributov zalogo vrednosti »ni skladen«, potem se izpeljanemu atributu brez izjeme dodeli odločitveno pravilo »ni skladen«. V praksi to pomeni, da v teh odločitvenih tabelah zajamemo širše problemsko območje in je vsaka zaznava neskladnosti dejansko tako tudi ovrednotena.

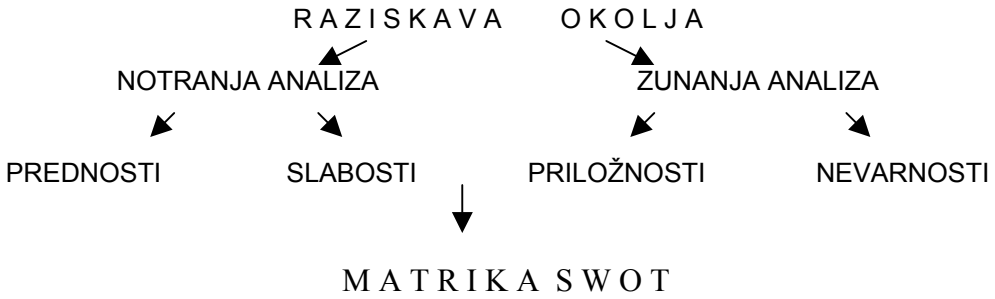
- Če je eden ali več atributov »delno skladnih«, potem se izpeljanemu atributu prav tako dodeli odločitveno pravilo »delno skladno«, razen v primeru, da je izpolnjeno prejšnje pravilo.

7. Kritična ocena ekspertnega sistema

7.1. Ovrednotenje ekspertnega sistema s pomočjo analize SWOT

Elementi, najpomembnejši za prihodnost podjetja, bolje poznani kot strateški faktorji, so združeni v kratici S.W.O.T. Sestavljena je iz štirih angleških besed: *strenghts* (prednosti), *weaknesses* (slabosti), *opportunitties* (priložnosti) in *threats (*nevarnosti), po katerih je analiza dobila ime.

Slika 17: Prikaz strukture analize SWOT



Vir: QuickMBA Strategic Managment

Z analizo prednosti in slabosti odkrivamo in ocenjujemo notranje dejavnike poslovanja. Prednosti so vsake sposobnosti ekspertnega sistema, s katerimi lahko dosežemo zastavljene cilje. Slabosti so tiste značilnosti, ki lahko ovirajo ali onemogočajo njihovo doseganje. Z analizo priložnosti in nevarnosti pa ocenjujemo zunanje dejavnike poslovanja. Priložnosti so razmere v zunanjem okolju, ki ob pravilnem izkoriščanju omogočajo doseganje zastavljenih ciljev. Nevarnosti pa so tisti dejavniki v okolju, na katere nimamo vpliva, lahko pa ogrozijo doseganje želenih ciljev.

Analiza SWOT je koristen pripomoček pri ocenjevanju določenega izdelka in možnosti, ki jih ima le-ta v danem okolju. Omogoča vrednotenje kvalitativnih in kvantitativnih podatkov. Analiza SWOT ima širok spekter možne uporabe. Z njeno pomočjo lahko ovrednotimo tudi ekspertni sistem za podporo odločanja v procesu celovite ocene skladnosti računalniških sistemov v podjetju z vidika inšpekcije ameriške Agencije za prehrano in zdravila.

Analiza poteka v dveh ločenih delih. Notranjo analizo tvorita pridobivanje potrebnih informacij o prototipu ekspertnega sistema in ocena zbranih informacij. Zunanja analiza pa je sestavljena iz zbiranja informacij o stanju v okolju in analiziranja dobljenih informacij.(Treven,1992, str. 644-653)

Na osnovi tako zastavljene metode dela sem opredelil:

- slabosti sistema, ki jih bo potrebno odpraviti;
- priložnosti, ki jih lahko spremenimo v prednosti;
- prednosti predlagane rešitve pred drugimi alternativami in nevarnosti iz okolja, ki lahko ogrozijo doseganje zastavljenih ciljev.

Odločitveni ekspertni sistem sem tako ovrednotil s pomočjo analize SWOT.

7.1.1. Prednosti

Ekspertni sistem s svojo zaokroženo vsebino in dobro strukturirano preglednostjo nadomešča ostale obsežne informacijske vire ter prinaša znanje, ki ga drugače iščemo pri različnih človeških ekspertih, in omogoča celovito oceno sistemov. Na tak način je ekspertni sistem močno poenostavil priprave podjetij na prihajajoče inšpekcije, saj zaposleni ob obstoječem načinu dela velik del svojih aktivnosti morali posvetiti vsakokratnim pregledom sistemov in študiju zahtevnih regulatornih besedil.

V podjetju uvedemo enoten sistem odločanja, kjer določena odločitvena pravila v bazi znanja izdelanega modela, zbrana iz različnih pisnih virov, na osnovi izkušenj in tihega znanja posameznih ekspertov, omogočajo pospešitev procesa ocenitve, saj v veliki meri izločijo potrebo, po vsakokratnem preverjanju obsežnih strokovnih vsebin.

Besedila so jasna in za uporabnika je dovolj, da odgovori na serijo vprašanj in prebere ponujeno rešitev. S tem zmanjšamo stroške priprave in skrajšamo čas za izdelavo različnih mnenj. Osredotočimo se lahko na akutne neskladnosti, ki bistveno vplivajo na morebitni odstop. Zaradi možnosti hitrega odziva v realnem času lahko pravočasno pripravimo ustrezne postopke.

Računalniški sistem omogoča hitre rešitve in sprotno analiziranje različnih pogledov; pri klasičnem načinu dela bi zato potrebovali preveč časa. Se zlasti to velja za situacije, kjer je potrebno oceniti kombinacijo večjega števila dejavnikov. Ekspertni sistemi pri sklepanju niso omejeni in zelo presegajo človekove kognitivne sposobnosti.

Proces celovite ocene skladnosti računalniških sistemov v podjetju z vidika inšpekcije ameriške Agencije za prehrano in zdravila z uporabo ekspertnega sistema postane standardiziran in prinaša določene nove kakovosti. Reševanje nesoglasij postane enostavnejše in preglednejše. Ne more se zgoditi, da se ne-bi identične okoliščine obravnavale na enak način. Ta slabost se kaže zlasti pri delu ljudi, ki so dovzetni za različne vplive, ki bolj ali manj okrnijo objektivnost in usklajenost pri odločanju.

Proces odločanja prinaša pomembne prednosti. Posebej izpostavljena je doslednost oziroma natančnost. Človek je kljub svojemu dobremu poznavanju področja in dolgoletnim izkušnjam nagnjen k pozabljanju in izpuščanju pomembnih podrobnosti. Ekspertni sistem to pomanjkljivost v veliki meri odpravlja in uporabniku sistematično podaja znanja, ga vodi skozi potrebne faze procesa in na ta način omogoča, da so v procesu odločanja vedno vsebovane vse ključne aktivnosti.

Povečamo zanesljivost sistemov in samo kakovost odločitev, ki jo omogočajo ekspertni sistemi. Izluščimo lahko določene zakonitosti in znanja ter s tem potrdimo ali ovržemo različna mnenja. Izvedemo lahko posamezne razlage odločitev oziroma aktivnosti, česar ekspert včasih noče ali ne more. Se pravi, da želimo zajeti čim več skritega znanja, obenem nam lahko služi kot inteligentni učbenik.

Sistem omogoča optimalno dolgoročno načrtovanje potrebnih terminskih, človeških in finančnih virov. Izpostavimo lahko ključne dejavnike, ki zahtevajo prednostno obravnavo, in dosledno preverjamo izvedene rešitve.

7.1.2. Slabosti

Če se želimo po eni strani z uporabo odločitvenega modela izogniti človeškim pomanjkljivostim, se na drugi strani srečamo z omejitvami in pomanjkljivostmi ekspertnega sistema.

Medtem ko so se človeški izvedenci sposobni bolj ali manj rutinsko prilagoditi spremenjenim zahtevam, je potrebno ekspertni model pri vsaki spremembi eksplicitno nadgraditi oziroma spremeniti določena znanja. Sistem ni sposoben povezati še tako očitnih vzročno-posledičnih zvez, ki v bazi znanja niso natančno opredeljene. To je posebno pomembno pri regulativi, kjer se lahko napačna informacija prenese v vse sisteme, ki jih ocenjujemo.

Vedno se je potrebno zavedati, da je model le približek realnemu svetu in da sisteme ocenjujemo "z očmi" ekspertov, ki so model gradili. Če so vnesena pravila, podatki in predpostavke napačni, so tudi rezultati odločitve lahko sporni.

Zavedati se moramo, da je inšpektor tisti, ki da prvo oceno skladnosti oziroma potrdi naša prizadevanja. Odloči se vedno človek na osnovi določenih objektivnih in subjektivnih meril, predpostavk in osebnega zaznavanja. Ekspertni sistemi nimajo sposobnosti čutnega zaznavanja in kreativne ustvarjalnosti, njihova obdelava podatkov in reševanje problemov sta zelo abstraktna, kar pomeni določene omejitve pri zagotavljanju realne ocene, kot bi jo podal inšpektor.

Pomanjkanje sposobnosti zdravega razumskega mišljenja lahko v določenih okoliščinah popolnoma spremeni sliko sistemov in ljudi, ki jih ocenjujemo. Se pravi, da ekspertno znanje ne da vedno optimalnega odgovora na zastavljeni problem.

Omejitve modela postavi tvorec glede na določene okoliščine v času razvoja. Ekspertni sistem se običajno ne zaveda svojih omejitev in lahko rešuje probleme tudi zunaj področja, ki ga pokriva.

7.1.3. Priložnosti

Prehod iz sedanjega okolja papirnih zapisov v okolje elektronskih zapisov zahteva razumevanje in hkrati pripravljenost farmacevtskih podjetij, da postanejo gibalo nenehnih sprememb. Napredna tehnologija upravljanja z znanjem omogoča hitre odzive na nenehne spremembe.

Pomembno priložnost predstavlja celovita ocena skladnosti v elektronski obliki z vsemi atributi, ki jih zahteva regulativa 21 CFR Part 11. Model se lahko uporabi kot osnovni koncept vključevanja odločitvenih sistemov v smernice FDA za bodoče inšpekcije preko elektronskih medijev.

Pričujoče delo predstavlja uspešen poskus poenotenja ekspertnega znanja, potrebnega za obvladovanje celotnega sistema skladnosti računalniških sistemov. Ker je področje primerljivo s številnimi drugimi, lahko predstavlja uspešna izgradnja in njegova izvedba spodbudo za razvoj podobnih sistemov na drugih področjih. Četudi ta vsebinsko največkrat niso primerljiva, pa so si procesi odločitve v ključnih elementih podobni do te mere, da to omogoča prenos konceptov in spoznanj, ki smo

jih dobili pri izgradnji sistema, tudi na ta področja, s tem pa bi lahko sledili razvoju metod in tehnik upravljanja z znanjem.
Omogočena je višja stopnja integracije podjetja na področju obvladovanja kakovosti sistemov in izdelkov ter povezovanja z informacijskimi sistemi znotraj podjetja. Vključujemo lahko druge metode in tehnike, ki jih prinaša intenzivni razvoj umetne inteligence.

7.1.4. Nevarnosti

Poleg priložnosti, ki lahko prispevajo k uspešni uporabi in nadaljnjemu razvoju, obstajajo v okolju določene nevarnosti, ki lahko ogrozijo cilje, ki smo si ji zastavili pri razvoju sistema.

V mnogih primerih farmacevtska podjetja delujejo v prepričanju, da lahko dosežejo regulatorno skladnost in uspešne inšpekcije že z nakupom rešitev, ki jih enostavno vgradijo v sistem podjetja brez kakršnihkoli sprememb. Dejansko je potrebno celo rešitve s popolno regulatorno funkcionalnostjo pravilno oblikovati in validirati, da dosežemo potrebno skladnost celotnega sistema.

Ameriška Agencija za prehrano in zdravila omenja osnovne nevarnosti in pasti, ki prežijo na podjetja, ki želijo laže, hitreje ter učinkovito uvesti in uporabljati skladne računalniške sisteme. (Qineito Trusted Information Managment, 2002, str. 3) Ker se srečujemo pri ekspertnem sistemu z enakimi zakonitostmi, so omenjeni dejavniki, ki predstavljajo grožnjo za uspešno uporabo ekspertnega sistema, identični.

Uporabniki nimajo zadostnega poznavanja ozadja, osnovnega računalniškega znanja in potrebnih izkušenj za učinkovito uporabo ekspertnega sistema.

Rešitve, ki jih ponuja napredna tehnologija na področju upravljanja z znanjem, lahko podjetje vodijo v preveliko odvisnost, lahko jih uporablja brez kančka kritičnosti ali pa uporabniki preprosto ne zaupajo informacijam, ki jih sistem ponudi, zato jih ne vključujejo v svojo delo.

Veliko nevarnost za neuspešno izvedbo predstavlja pomanjkanje finančnih in človeških virov za osnovno izgradnjo in nadaljnji razvoj sistema.
Uvedba ekspertnega sistema na splošno povzroča precejšnje spremembe v organizacijski strukturi in procedurah ter lahko spodleti, če okolica ni naklonjena spremembam ali če obstaja odpor do uporabe računalniške tehnologije.

Ko govorimo o ekspertnem sistemu, izvedenem s pomočjo računalniške tehnologije, se srečujemo z vsemi zahtevami, ki jih obravnavana regulativa 21 CFR Part 11, čeprav jih FDA za tovrstne aplikacije izrecno ne zahteva. Vendar je pomanjkanje elementov varnosti, zgodovine dogodkov, celovitost baze znanja... prav tako za podjetje neodgovorno in predstavlja veliko nevarnost za možno zlorabo ekspertnega sistema , ki bi jo izvedel nepooblaščeni ali naključni uporabnik (zaposleni, osebje FDA, konkurenca, proizvajalci sistemov..). V tem primeru ima lahko razkritje celotne strategije obvladovanja skladnosti računalniških sistemov dolgoročne negativne posledice, posebej v primeru izvedenih rešitev, za katere so bile odločitve sprejete na osnovi določenih tveganj.

Ekspertni sistem ima svoje razvojne zakonitosti, z različnimi razvojnimi težavami in odstopi. V "otroški dobi" uvajanja, ko še ni prekaljen in potrjen v praksi, predstavlja ogrožajoč dejavnik velika ranljivost sistema zaradi prisotnih skritih napak.

7.1.5. Matrika SWOT

Tabela 8: Prikazuje matriko SWOT za uporabo odločitvenega modela za celovito oceno skladnosti računalniških sistemov v podjetju z vidika inšpekcije ameriške Agencije za prehrano in zdravila.

Prednosti	Slabosti
• celovita ocena sistemov • uvedba enotnega sistem odločanja • preglednost in usklajenost • objektivnost ocen • hitro iskanje sistemskih neskladnosti • velik potencial ekspertnih znanj • sistem prijazen uporabniku • modularna struktura • nenehno dopolnjevanje in nadgradnja • možnost optimalnega dolgoročnega načrtovanje inšpekcij • prilagodljivost uporabnikom z različno ravnijo poznavanja problemskega področja	• nesposobnost sistema za učenje • model je le približek realnemu svetu • pomanjkanje sposobnosti čutnega zaznavanja in ustvarjalnosti • omejitve modela postavi človek glede na določene okoliščine v razvoju • pomanjkanje sposobnosti zdravega razumskega mišljenja
Priložnosti	**Nevarnosti**
• hitrejše in pravilnejše odločanje • pravočasne in točnejše informacije • boljše načrtovanje • povečano zadovoljstvo zaposlenih • sproščena kreativnost • celovita ocena skladnosti v elektronski obliki z vsemi atributi, ki jih zahteva 21 CFR Part 11 • možnost širitve uporabe sistema na druga področja • možnost povezovanje z informacijskimi sistemi znotraj podjetja • stopanje v koraku z razvojem metod in tehnik upravljanja z znanjem • hitri odzivi na nenehne spremembe • poenotenje ekspertnih znanj na enem mestu • možnost višje stopnje integracije podjetja na področju kakovosti sistemov in izdelkov	• pomanjkanje finančnih in človeških virov za osnovno izgradnjo in nadaljnji razvoj • okolica ni naklonjena spremembam in odpor do uporabe računalniške tehnologije • nezaupanje uvajanju tehnologij na področju upravljanja z znanjem; • poenostavljanje rešitev • nekritična uporaba sistema in preveliko zanašanje na odgovore, ki jih sistem ponuja • pomanjkanje elementov varnosti; • občutek ogroženosti ekspertov področij, na katerem se uvajajo napredne tehnologije • nepooblaščena uporaba virov s strani FDA ali konkurence • ranljivost sistema v razvojni fazi

7.1.6. Vzdrževanje in nadgradnja ekspertnega sistema

Čeprav je odločitev o začetku projekta morda videti preprosta, saj vodstvo podjetja lahko ideji »samo pritrdi ali zanika«. Posledice pa so v obeh primerih za podjetje daljnosežne: potrebno angažiranje lastnih sredstev, ljudi in usmerjanje dragocenih virov v nek projekt, katerega vizija ali cilji so jasni: v prvem primeru »stopati v korak s časom« ali pa » stopicati na mestu«.

V primeru projektov računalniških in informacijskih tehnologij, gre za dolgoročne projekte, ki vplivajo na notranjo učinkovitost podjetja in ustvarjanja množice novih priložnosti. Za oceno ekonomičnosti teh projektov, je potrebno upoštevati oprijemljive in neoprijemljive stroške ter prednosti. Oprijemljive prednosti so direktni prihranki npr. materialnih stroškov in stroškov dela. Težko pa je oceniti prednosti, ki izhajajo iz narave ustvarjanja novih priložnosti.

Vzdrževanje ekspertnega sistema obsega naslednje štiri glavne aktivnosti:

a. Popravki za odpravljanje neskladnosti.

b. Prilagajanje ekspertnega sistema spremembam v okolju. Pri tem se funkcionalnost ekspertnega sistema ne spremeni.

c. Razširitev zmogljivosti ekspertnega sistema, ki se ukvarja z novimi ali spremenjenimi zahtevami. Spremeniti moramo funkcijo sistema, izboljšamo lahko zmogljivosti ali uporabniški vmesnik in nadgradimo bazo znanj.

d. Preventivno vzdrževanje sistema, tako programske opreme kot podatkovne baze znanja, je namenjeno spremembam, ki izboljšajo možnost njihovega vzdrževanja (dopolnjevanje dokumentacije, izboljšava odločitvenih pravil itd.)

V bližnji prihodnosti bodo velik vpliv na obliko in način razvoja odločitvenih modelov imele metode, ki jih razvija umetna inteligenca. Pojavljajo se inteligentni asistenti kot ekspertni sistemi za pomoč pri procesih odločanja in vodenja.

Ker prihaja Agencija za prehrano in zdravila iz sveta, kjer se družba tehnološko najbolj razvija, lahko pričakujemo, da bo prav Agencija iskala pomoč v ekspertnih sistemih, se posluževala sodobnih orodij in globalnih omrežij za povečanje učinkovitosti nadzora.

Tako pogoste in hitre spremembe silijo farmacevtsko podjetje v nenehno prilagajanje in pripravljenost na nove izzive. Pojavljajo se številna nova etična vprašanja in podjetja so zaradi odvisnosti od računalniških sistemov vedno bolj informacijsko odprta in ranljiva.

Učinkovitost sistemov za podporo upravljanju, ki jih omogoča hiter razvoj informacijske tehnologije in podpornih programskih rešitev, vse bolj postaja prednost podjetja, ki zna izkoristiti informacijsko infrastrukturo in razpoložljive vire znanj. Drugačen pristop in način razmišljanja bi sčasoma prinesel potrebne izkušnje, znanja ter pomagal k razvoju potrebne kulture podjetja.

8. Zaključek

Aristotel je v svojem času kritično razmišljal o knjigi, rekoč, da knjiga ni primerna za izobraževanje, ker z njo ni mogoče nadomestiti procesa, ki se odvija med učiteljem in učencem. Kako je danes, vemo vsi. Knjiga učitelja res ni nadomestila, je pa prinesla marsikaj novega.

Tako je tudi z računalniki in z njimi povezano informacijsko tehnologijo. A pot do rešitev, neposredno uporabnih v farmacevtski industriji, ni preprosta. Jasno je le to, da sama uporaba tehnologije ni vedno prava oziroma ustrezna rešitev. In še najmanj je res, da lahko z njo popolnoma nadomestimo človeka.

Res je tudi, da prinaša računalniška in informacijska tehnologija v procese novo kakovost, ki jo je treba vedno na novo odkrivati in kritično ocenjevati. Brez tega je vsako spreminjanje raziskovalnih in proizvodnih procesov nepopolno in tega bi se morali zavedati vsi, ki nam je do njihove kakovosti.

Računalniška in informacijska tehnologija je torej postala pomemben del pri razvoju in izdelavi zdravila, saj nam olajša delo na praktično vseh ravneh delovanja.

Ko je ameriška Agencija za prehrano in zdravila začela aktivno uvajati smernice na področju elektronskih zapisov in elektronskih podpisov, je s tem farmacevtskim podjetjem omogočila formalni prestop v informacijsko dobo. Farmacevtska podjetja pa se morajo sama odločiti, kdaj bodo ta korak naredila, izbrati svoje poti razvoja in predvideti vse skrite pasti, ki jih prinaša uvajanje novih tehnologij.

Kot je zapisano v naslovu magistrskega dela, smo izdelali celovito oceno skladnosti računalniških sistemov v farmacevtskem podjetju z vidika inšpekcije ameriške Agencije za prehrano in zdravila s pomočjo kvalitativnega hierarhičnega odločitvenega modela. Njegova izgradnja je potekala sistematično, odgovorno in z jasno opredeljenimi cilji:

- postaviti elektronske zapise in elektronske podpise kot pomemben del validacije računalniških sistemov;

- ugotoviti zakonitosti posameznih elementov modela in njihove povezave;

- izdelati večparametrski odločitveni model za celovito oceno regulatorne skladnosti farmacevtskega podjetja z vidika 21 CFR Part 11;

- s pomočjo analize SWOT oceniti ekspertni sistem in možnosti, ki jih ima le-ta v okolju farmacevtskega podjetja.

Rezultati so celovito predstavljeni in cilji doseženi. Ugotovili smo, da za uspešen potek inšpekcije niso dovolj delne rešitve, kot tudi ne zadoščajo več samo izkušnje ali intuicija vodstva. Izzive, ki jih prinašajo zahteve za regulatorno skladnost, moramo pravilno umestiti v čas in prostor ter oceniti dejavnike tveganja in spremenljivosti. Takšen pregleden in zaokrožen pristop nam omogoča celovito razumevanje celotnega procesa regulatorne skladnosti. Podjetje lahko sedaj na osnovi novih spoznanj oblikuje učinkovito strategijo za zagotavljanje kakovosti na področju

elektronskih tehnologij. Inšpekcije postanejo manj stresne, uporabljene rešitve skladnejše.

Poseben doprinos predstavlja odločitveni model, v katerem so v obliki drevesa kriterijev prikazani in s pomočjo podanih zalog vrednosti ocenjeni atributi z vsemi njihovimi podsistemi, ki ključno vplivajo na uspešen potek inšpekcije: sistem upravljanja kakovosti, skrbnik sistemov, regulativa 21 CFR Part 11, proces sprememb in arhiv podatkov. Vsak od njih nosi določena tveganja, ki smo jih s poglobljeno analizo v okviru odločitvenega modela naredili določljive in obvladljive.

Farmacevtskemu podjetju tako omogočimo, da lahko na osnovi sodobnih orodij obvladuje zahtevne razvojne izzive. Vgrajena baza znanja in dobljene ocene predstavljajo razumljive kazalce, s pomočjo katerih se lahko podjetje v vsakem trenutku optimalno pripravi na zahteve inšpekcij, sprotno odpravlja morebitna ugotovljena neskladja in se na osnovi dobljenih analiz odloča za pravilno strategijo pri zagotavljanju regulatorne skladnosti računalniških sistemov podjetja.

S pravilnim umeščanjem atributov računalniških sistemov v prostor regulative dobimo celostno trenutno sliko, ki je osnova za kakovostno odločanje podjetja v danem trenutku o uporabi znanja, opreme, dragocenih finančnih in človeških virov tako v času priprave na inšpekcijo kot med njenim potekom.

Na osnovi rezultatov izdelane analize SWOT, bomo v podjetju izdelali strategijo za:

- postopno odpravo slabosti sistema;
- spremembo ponujenih priložnosti v prednosti, kjer je to le mogoče;
- ohranitev prednosti predlagane rešitve pred drugimi alternativami in učinkovito ukrepanje ob vsaki zaznavi nevarnosti iz okolja, ki bi lahko ogrozile doseganje zastavljenih ciljev.

Končni cilj je pridobiti in ohranjati polno zaupanje ameriške Agencije za prehrano in zdravila. Pri tem pričujoče delo predstavlja doprinos na področju elektronskih zapisov in elektronskih podpisov s pomočjo modeliranja ekspertnega znanja in sistemov za podporo odločanju.

9. Literatura in viri

9.1. Literatura

1. Alcon: Electronic Signature Questionnaire: Summary Rep., July 9, 1997, 6 str.

2. American Bar Association: Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, August 1, 1996, 125 str.

3. Bohanc M., Rajkovič V.: Multi-Attribute Decision Modeling: Industrial Applications of DEX: Informatica 23, 1999, str. 487-491

4. Bohanc M., Rajkovič V.: Večparametrski odločitveni modeli: Organizacija in kadri 7/95, str. 427

5. Chapman G. Kenneth, Winter F. Paul: Electronic Signatures: 21 CFR 11 Issues that Require More Discussion: Special edition, Implementing Electronic Records an Signatures, B.k., 2002, str. 49-55

6. Code of Federal Regulations, Title 21, Good and Drugs, Part 11, "Electronic Records; Electronic Signature; Finale Rule." FDA Register ,Vol. 62, No.54,pp.13429-13466, March 20, 1997, 14 str.

7. Department of Defense 5015.2: Design Criteria Standard for Electronic Record Managment Software Application, November 1997, DoD 5015.2, 1997, 29 str.

8. DEX – An expert system shell for multiatribute decision making. User's Manual, Josef Stefan Institute, Ljubljana, 1989

9. Dollar M. Charles: PDA/FDA Public Conference On Technical Implementation Part 11: Electronic Archiving: Requirements, Principles, Strategy, And Best Practices, June 19-20, Philadelphia, 2000, 39 str.

10. Forstedt Linda: How to Survive an FDA Computer Validation Audit, Journal of Validation Technology, August 2001, str. 354-358

11. Grunbaum A. Leonard: Comply with Federal Regulations: Controlling the Electronic Transfer of Clinical Trial Data: Special edition, Implementing Electronic Records an Signatures, B.k, 2002, str. 34-40

12. Joseph X. Phillips: Current 483 Findings Related to Process Validation: Preparing for FDA and Euro Regulatory Inspections, October 2001, 11 str.

13. Jurančič A., Rajkovič V.: Moč in nemoč računalniške podpore odločanja. [URL:http://www.drustvoinformatika.si/dogodki/arhiv/dsi2001/sekcija_d/jurancic_rajkovic.dot], 20.9.2002

14. Klein Gary, Sources of Power: How People Make Decisions, Cambridge, MA: The MIT Press, 1998, 321 str.

15. Lopez Orlando, McNell Consumer Healthcare, HR's Computer and Software Validation Processor; Testing Automated Manufacturing Processes, July.28, 2000 in Washington DC, 69 str.

16. Lopez Orlando: Overview of Technologies Supporting Security Requirements in 21 CFR Part 11: Part 2, Pharmaceutical Technology, March 2002, str. 48-62

17. Lopez Orlando: Technologies Supporting Security Requirements in 21 CFR Part 11: Part 1, Pharmaceutical Technology, February 2002, str. 36-46

18. Lopez Orlando: McNell Consumer Healthcare: 21 CFR Part 11 as CSV Model, Brussels, Yanuary 2001, 46 str.

19. Malcolm Dixon: Documentation and Organization Before the FDA Arrives: Preparing for FDA and Euro Regulatory Inspections, October 2001, 9 str.

20. Malcolm Dixon: Preparing Personnel for the FDA's Arrives: Preparing for FDA and Euro Regulatory Inspections, October 2001, 8 str.

21. National Archives and Record Administration: Record Managment Guidance for Agencies Implementing Electronic Signature Technologies, October 18, 2000, 18 str.

22. OECD (Organisation for economic co-operation an development): GLP consensus document, The application of the principles of GLP to computerised systems, Paris 1995, 15 str.

23. Qineito Trusted Information Managment, Inc: 21 CFR Part 11 Executive Whitepaper, April 16, 2002, 9 str.

24. Pavliha M., Bogataj M, Jerman B. B.,Klobučar T., Matas S., Puharič K., Vlačič P.: Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem: GV založba, Ljubljana 2002, 216 str.

25. Perrow, Charles: Normal Accidents, New York: Basic Books, 1984, 386 str.

26. PricewatherhouseCoopers, Joseph F. Noferi: Understanding the Electronic Signatures Rule and Its Application: Special edition, Implementing Electronic Records an Signatures, B.k, B.l, str. 59-69.

27. Rajkovič V., Bohanc M.,Zupan B.: Applications of Qualitative Multi-Attribute Decision Models in Health Care: International Journal of Medical Informatics, 2000, 20 str.

28. Rajkovič V., Šuterič O., Šusterič J., Bohanec M.: Kako storiti več za kakovost zdravstva in šolstva?: Prispevek za modro knjigo: Civilna družba v Sloveniji in Evropi, 2000, 8 str. [http://www.fow.inimb.si/programiranje/uros/files/SPO/ClanekModraKnjiga2000.pdf], 5.1.2003

29. Rogelj T.,Rajkovič V., Bohanec M.: Odločitvene metode in sistemi: Elektronsko študijsko gradivo, Ekonomska fakulteta, Ljubljana, 2001

30. McDowall R. D.: Digital Signatures: LC·GC Europe, February 2001, pharmaceutical file, str. 1-4

31. Reason James: Human Error, Cambridge: Cambridge University Press,1990

32. Robert W. Stotz: Electronic Records and Signatures :The FDA Perspective, Special edition, Implementing Electronic Records an Signatures,B.k., 2002, str. 10 -18

33. Rozman R., Kovač J., Koletnik F.: Managment, Gospodarski vestnik, Ljubljana, 1993, 312 str.

34. Smith Kevin: Analytical Data Management and Archiving: 21 CFR Part 11 Compliance and Beyond: Pharmaceutical Technology, May 2002, str. 44-48

35. Solina F.: Projektno vodenje razvoja programske opreme, Univerza v Ljubljani, Ljubljana, 1997, 212 str.

36. Stemberger Mark: Izgradnja odločitvenega modela s pomočjo projektnega pristopa, 7 str. [URL:http://lopes1.fov.unimb.si/PES_web/Izgradnja%20odlo%C4%8Ditvenega%20modela%202001_08_31.pdf], 18.2.2003

37. Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records: Electronic Signatures Final Rule Published in the Federal Register, Web page issued: March,2000: reformatted June 01, 2001 [URL:http://www.fda.gov/ora/compliance_ref/part11/frs/background/11cfr_fr_04.htm], 25.1.02

38. Toplišek J.:Elektronski podpisi: Usklajevanje tehnoloških in pravnih rešitev pri elektronskem poslovanju, Organizacija, Tematska številka 5/96, str. 291-300

39. Treven Sonja: SWOT analiza. Organizacija in kadri, Kranj, 25(1992), 9-10, str. 644-653

40. Weinger Matthew B., Pantiskas Carl, Wiklund Michael, Carstensen Peter: Incorporating Human Factor Into the Design of Medical Devices. JAMA, 280(17):1484, 1998

9.2. Viri

1. ANSI X9.17 Pseudo Random Number Generator (RNG): Technical Data Sheet: Document Number: I.IPA01-0087-USR Rev 03, October 2002, 5 str.

2. CCPI Confidential: 21 CFR 11 - Electronic Records: Electronic Signatures Assessment Worksheet, Internal Audit Document V 1.0, B. k., 22 str.

3. CDRH –Center for Devices and Radiological Health :General Principles of Software Validation; Final Guidance for Industry and FDA Staff, January 11, 2002, 43 str.

4. Electronic records and electronic signatures An Insight, Tescom, [URL:http://registration.tescom-usa.com/testconf/fda1102/presentation/workshop/1_insight.pdf],15.1.2003

5. FDA 21 Code of Federal Regulations Part 210,"Current Good Manufacturing Practice in Manufacturing, Processing, Packing, or Holding of Drugs; General, 1994
[URL:http://www.fda.gov/cder/dmpq/cgmpregs.htm], 12.9.2002

6. FDA 21 Code of Federal Regulations Part 211, "Current Good Manufacturing Practice for Finished Pharmaceuticals .", April 1996
[URL:http://www.fda.gov/cder/dmpq/cgmpregs.htm], 12.9.2002

7. GAMP 3 - Version 3.0: Guide For Validation of Automated Systems in Pharmaceutical Manufacture: Volume 1, Part 1:User guide, March 1998

8. GAMP 3 - Version 3.0: Guide For Validation of Automated Systems in Pharmaceutical Manufacture: Volume 2: Best Practice for User and Suppliers: March 1998

9. GAMP Special interest group (21 CFR Prat 11): Complying with 21 CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 01 September 2000

10. Webster's, New Universal Unabridged Dictionary: Glossary of Computerized system and software development terminology: Deluxe Second Edition, 1979, 75 str. [URL:http://www.fda.gov/ora/inspect ref/igs/gloss.html], 13.9.2002

11. Guidance for Industry: Computerized System Used in Clinical Trials, USFDA Guidance Document, April 1999, 14 str.

12. Guide to inspection of Computerized System and Drug Processing ('83) and CPG §7132a.11 ('84)
[URL:http://www.fda.gov/ora/inspct ref/csd.html], 12.9.2002

13. Guide to inspections of foreign Pharmaceutical Manufactures; 15 str.
[URL:http://www.fda.gov/ora/inspct ref/igs/fordrug.html],12.9.2002

14. Informacijski sistemi v proizvodnih podjetjih, INEA, Ljubljana, 2000, 5 str.

15. Jeff Rothenberg: “Metadata to Support Data Quality and Longevity”(Electronic file) 1700 Main Street; Santa Monica, CA 90407; March 1996, 15 str. [URL:http://www.computer.org/conferences/meta96/rothenberg_Paper/ieee.data-quality.html], 14.9.2002

16. Matthev G. Roberge: Factory Acceptance Tesing (FAT) of Pharmaceutical Equipment, Pharmaceutical Engineering, november/december 2000, str. 8-15

17. Merck Manufacturing Standards for Pharmaceutical Operations: Effective Date: May 2001, Issue January 2001, 58 str.

18. Michael L. Brodie, Michael Stonebraker; Migrating Legacy System: Gateways, Interfaces & the Incremental Approach,1995, str. 30-36

19. Michelle M. Gonzalez: Applied Terminology for the Pharmaceutical Industry: Pharmaceutical Engineering, January/February 2001, str. 46-56

20. Paule J. Motise: Guidance for Industry: 21 CFR Part 1: Electronic Records: Electronic Signatures: Maintenance of Electronic Records, July 2002, 24 str.

21. QuickMBA Strategic Managment [URL:http://www.rquickmba.com/strategy/swot], 20.2.03

22. Sistemski splošni postopek:Vodenje inšpekcij in presoj partnerjev /kupcev v Lek d.d., Ljubljana, 7.2001, 11 str.

23. Standard Guide for Analytical Data Interchange Protocol for Chromatographic Data, E-1948-98; American Society for Testing and Materials, 1988

24. URLS,”How the CRC algorithm works” [http://www2.rad.com/networks/1994/err_con/crc_how.htm], 13.9.2002

25. U.S. National Archives & Records Administrator, Part 1234 - Electronic Records Management. [URL:http://www.archives.gov/about_us/regulations/part_1234.html], 13.9.2002

26. XPORT Transport Format [URL:http://www.sas.com/software/industry/pht/fda/index.html], 15.9.2002

27. Wenniger, 1991,S.47 po Perrowu, 1987 [URL:http://www.rrz.uni-hamburg.de/psych-1/witt/Lehre/Folien12.pdf], 16.2.2003

28. Wheelen Thomas, Hunger David: Strategic management, Addison Wesley, 1996, 441str.

10. Priloga A – Izpisi odločitvenega modela

10.1. Drevo kriterijev

Drevo kriterijev

Kriterij	Opis
Ocena	Celovita ocena skladnosti.
├**Regulativa**	Regulativa zajema; Part 11, arhiv, sistem sprememb.
│ ├**21 CFR Part 11**	Regulativa na področju elekronskih zapisov in podpisov.
│ │ ├**Zapisi (poglavje B)**	Poglavje B; Elektronski podpisi.
│ │ │ ├**Zaprti sistemi**	Zaprti sistemi (11.10).
│ │ │ │ ├**Sistemi & zapisi**	Sistemi & zapisi.
│ │ │ │ │ ├**Validacija**	Validacija računalniških sistemov.
│ │ │ │ │ │ ├Natačnost	Preverjanje natačnosti sistema.
│ │ │ │ │ │ ├Zanesljivost	Preverjanje zanesljivosti sistema.
│ │ │ │ │ │ ├Dosledno delovanje	Validacija glede na industrijske standarde.
│ │ │ │ │ │ └Razločevanje	Razločevanje neveljavnih in spremenjenih zapisov.
│ │ │ │ │ ├**Inšpektibilnost**	Inšpektibilnost sistema.
│ │ │ │ │ │ ├Točne in popolne kopije	Generiranje točnih in popolnih kopij zapisov.
│ │ │ │ │ │ └Zaščita zapisov	Zaščita zapisov in njihova ponovna vzpostavitev.
│ │ │ │ │ ├**Varnost**	Načrtovani in uporabljeni varnostni postopki.
│ │ │ │ │ │ ├Fizični dostop	Fizični dostop omejen na pooblaščene posameznike.
│ │ │ │ │ │ ├Zaporedje korakov	Sistem zagotavlja ustrezno zaporedje korakov.
│ │ │ │ │ │ ├**Preverjanje pooblastil**	Preverjanje pooblastil.
│ │ │ │ │ │ │ ├Logični dostop	Samo pooblaščeni posameznik lahko uporablja dostop.
│ │ │ │ │ │ │ ├Elek. podpisan zapis	Pooblaščeni posameznik elektronsko podpiše zapis.
│ │ │ │ │ │ │ ├I/O naprave	Dostop do vhodno/izhodnih naprav sistema.
│ │ │ │ │ │ │ └Spreminjanje zapisov	Spreminjanje zapisov ali izvedba specifičnih operacij.
│ │ │ │ │ │ └Preverjanje naprav	Preverjanje naprav ali terminalov.
│ │ │ │ │ └**Zgodovina dogodkov**	Načrtovani in uporabljeni postopki in kontrole.
│ │ │ │ │ ├**Izvedba**	Izvedba zgodovine dogodkov.
│ │ │ │ │ │ ├Varnost	Varovanje zgodovine dogodkov.
│ │ │ │ │ │ ├Samodejnost	Računalniško generirana zgodovina dogodkov.
│ │ │ │ │ │ ├Žigosanje	Časovno in datumsko žigosanje.
│ │ │ │ │ │ └**Neodvisni vpisi**	Zagotovitev neodvisnih vpisov.
│ │ │ │ │ │ ├Kreiranje	Kreiranje elektronskih zapisov.
│ │ │ │ │ │ ├Spreminjanje	Spreminjanje elektronskih zapisov.
│ │ │ │ │ │ ├Vzdrževanje	Vzdrževanje elektronskih zapisov.
│ │ │ │ │ │ └Brisanje	Brisanje elektronskih zapisov.
│ │ │ │ │ └**Shranjevanje**	Shranjevanje zgodovine dogodkov.
│ │ │ │ │ ├Spremembe	Spremembe ne smejo okrniti predhodnih informacij.
│ │ │ │ │ ├Vzdrževanje	Vzdrževanje zgodovine dogodkov.
│ │ │ │ │ └Dostopnost	Dostopnost za pregled in kopiranje.
│ │ │ │ └**Osebje in dokumentacija**	Osebje in dokumentacija.
│ │ │ │ ├**Kvalifikacija osebja**	Kvalifikacija osebja.
│ │ │ │ │ ├Razvijalcev	Razvijalci računalniških sistemov.
│ │ │ │ │ ├Vzdrževalcev	Vzdrževalci računalniških sistemov.
│ │ │ │ │ └Uporabnikov	Uporabniki računalniških sistemov.
│ │ │ │ ├Odgovornosti	Premišljenost in odgovornost.
│ │ │ │ └**Kontrola dokumentacije**	Kontrola sistemske dokumentacije.
│ │ │ │ ├**Kontrola**	Kontrola dokumentacije za sistemsko delovanje.
│ │ │ │ │ ├Distribucija	Distribucija dokumentacije.
│ │ │ │ │ ├Dostop	Dostop do dokumentacije.
│ │ │ │ │ └Uporaba	Uporaba dokumentacije.
│ │ │ │ └Sistemska dokumentacija	Nadzor sistemske dokumentacije.
│ │ │ ├**Odprti sistemi**	Odprti sistemi (11.30).
│ │ │ │ ├**Postopki in kontrole**	Postopki in kontrole ter atributi.
│ │ │ │ │ ├Avtentičnost	Zahtevana avtentičnost.
│ │ │ │ │ ├Celovitost	Zahtevana celovitost.
│ │ │ │ │ └Zasebnost	Zahtevana zasebnost.
│ │ │ │ └**Postopki in kontrole ter vsebine**	Postopki in kontrole in vsebine.
│ │ │ │ ├Transformacija	Transformacija primernih pravil iz zaprtih sistemov.
│ │ │ │ ├Tajnopis dokumentov	Tajnopis dokumentov.
│ │ │ │ └Digitalni podpis	Standardi digitalnega podpisa.
│ │ │ ├**Prikazovanje podpisa**	Prikazovanje podpisa (11.50).
│ │ │ │ ├**Elektronski podpis**	Elektronski podpis.

Ime in priimek podpisnika	Vpisano ime in priimek podpisnika.
Datum in čas	Vpisan datum in čas.
Namen podpisa	Vpisan namen podpisa.
Povezava z zapisi	Povezava z podpisov z prvotnim zapisom.
Nadzor	Podpisi imajo enak nadzor kot elektronski zapisi.
Čitljivost	Človeku beljiva oblika.
Zapis & Podpis	Zapis & Podpis (11.70) .
Avtentičnost povezave	Avtentičnost povezave med zapisom in podpisom.
Podpisi (poglavje C)	Poglavje C ; Elektronski podpisi.
Splošne zahteve	Splošne zahteve za elektronske podpise (11.100).
Avtentičnost podpisa	Podpis naj bo svojsten posamezniku, unikaten.
Identiteta posameznika	Preverjanje identitete posameznika.
Prijava uporabe	Prijava pri FDA.
Certifikat	Certifikat v papirni obliki, ki ustreza FDA regulativi.
Komponente	Komponente elektronskega podpisa in kontrole (11.200).
Nebiometrični	Nebiometrični elektronski podpisi.
ID in geslo	Identifikacijska koda in geslo.
Funkcionalnost dostopa	Funkcionalnost neprekinjenega in prekinjenega dostopa.
Omogočena uporaba	Omogoča uporaba samo lastnikom podpisa.
Dodeljevanje	Dodeljevanje nebiometričnih podpisov.
Biometrični	Biometrični elektronski podpisi.
ID/geslo	Kontrola za identifikacijsko kodo/geslo (11.300).
ID	Identifikacijska koda je neponovljiva in preverjena.
Postopki in kontrole	Uvedeni postopki in kontrole.
Avtorizacija	Avtorizacija.
Zamenjave	Začasne ali trajne zamenjave.
Varnostni ukrepi	Varnostni ukrepi.
Nepooblaščena uporaba	Zaščita pred nepooblaščeno uporabo.
Zaznavanje zlorabe	Zaznavanje poskusa zlorabe.
Poročanje poskusa zlorabe	Poročanje poskusa zlorabe.
Testiranje naprav	Periodično testiranje naprav.
Spremembe	Celovito obvladovanje sprememb.
Vodenje	Vodenje sprememb.
Odobritev spremembe	Odobritev spremembe.
Sistem in nivoji odgovornosti	Vpeljan sistem in nivoji odgovornosti.
Potrditev spremembe	Potrditev spremembe.
Potek	Potek procesa spremembe.
Analiza spremembe	Analiza spremembe z možnimi tveganji.
Definiranje vpliva	Definiranje vpliva na regulatorni status.
Plan in izvedba testiranj	Plan in izvedba testiranj.
Dokumentacija	Popravilo vseh dokumentov in evidentiranje.
Arhiv	Arhiv elektronskih podatkov.
Politika arhiviranja	Politika arhiviranja podjetja.
Postopki	Aktivnost iz dobre prakse elektronskega arhiviranja.
Varnost	Varnost elektronskih zapisov.
Spominski mediji	Uporabljeni spominski mediji.
Skrbnik sistema	Kandidat, ki skrbi za razvojne faze sistema.
Znanja	Zahtevana ključna znanja.
Strokovna izobrazba	Formalna strokovna izobrazba skrbnika sistema.
Poznavanje sistema	Strokovno poznavanje sistema - "tiho znanje".
Poznavanje jezika	Formalno potrjeno poznavanje jezikov.
Leta	Pridobljene izkušnje.
Izkušnje	Pridobljene izkušnje.
Osebne lastnosti	Primernost za določeno delo.
Nastop	Sposobnost predstaviteve sistema in postopkov.
Prilagodljivost	Sposobnost prilagoditve različnim situacijam.
Dinamičnost	Sposobnost hitrega iskanja rešitev in prezemanje vlog.
Upravljanje kakovosti	Nosilec za implementacijo politike regulatorne skladnosti.
Vpliv na kakovost	Vpliv sistema na kakovost in varnost izdelka.
Inšpektibilnost	Vrste inšpekcij.
Zahtevnost trgov	Zahtevnost trgov.
Podpora vodstva	Podpora vodstva zagotavljanju skladnosti.

10.2. Zaloge vrednosti

Zaloge vrednosti

Kriterij	Zaloga vrednosti
Ocena	***ni odstopa***; drugi; večji; **kritični**
Regulativa	***skladen***; ni v uporabi; delno skladen; **ni skladen**
21 CFR Part 11	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Zapisi (poglavje B)	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Zaprti sistemi	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Sistemi & zapisi	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Validacija	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Natačnost	***skladen***; ni v uporabi; **ni skladen**
Zanesljivost	***skladen***; ni v uporabi; **ni skladen**
Dosledno delovanje	***skladen***; ni v uporabi; **ni skladen**
Razločevanje	***skladen***; ni v uporabi; **ni skladen**
Inšpektibilnost	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Točne in popolne kopije	***skladen***; ni v uporabi; **ni skladen**
Zaščita zapisov	***skladen***; ni v uporabi; **ni skladen**
Varnost	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Fizični dostop	***skladen***; ni v uporabi; **ni skladen**
Zaporedje korakov	***skladen***; ni v uporabi; **ni skladen**
Preverjanje pooblastil	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Logični dostop	***skladen***; ni v uporabi; **ni skladen**
Elek. podpisan zapis	***skladen***; ni v uporabi; **ni skladen**
I/O naprave	***skladen***; ni v uporabi; **ni skladen**
Spreminjanje zapisov	***skladen***; ni v uporabi; **ni skladen**
Preverjanje naprav	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Zgodovina dogodkov	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Izvedba	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Varnost	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Samodejnost	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Žigosanje	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Neodvisni vpisi	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Kreiranje	***skladen***; ni v uporabi; **ni skladen**
Spreminjanje	***skladen***; ni v uporabi; **ni skladen**
Vzdrževanje	***skladen***; ni v uporabi; **ni skladen**
Brisanje	***skladen***; ni v uporabi; **ni skladen**
Shranjevanje	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Spremembe	***skladen***; ni v uporabi; **ni skladen**
Vzdrževanje	***skladen***; ni v uporabi; **ni skladen**
Dostopnost	***skladen***; ni v uporabi; **ni skladen**
Osebje in dokumentacija	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Kvalifikacija osebja	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Razvijalcev	***skladno***; ni v uporabi; **ni skladen**
Vzdrževalcev	***skladen***; ni v uporabi; **ni skladen**
Uporabnikov	***skladen***; ni v uporabi; **ni skladen**
Odgovornosti	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Kontrola dokumentacije	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Kontrola	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Distribucija	***skladen***; ni v uporabi; **ni skladen**
Dostop	***skladen***; ni v uporabi; **ni skladen**
Uporaba	***skladen***; ni v uporabi; **ni skladen**
Sistemska dokumentacija	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Odprti sistemi	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Postopki in kontrole	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Avtentičnost	***skladen***; ni v uporabi; **ni skladen**
Celovitost	***skladen***; ni v uporabi; **ni skladen**
Zasebnost	***skladen***; ni v uporabi; **ni skladen**
Postopki in kontrole ter vsebine	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Transformacija	***skladen***; ni v uporabi; **ni skladen**
Tajnopis dokumentov	***skladen***; ni v uporabi; **ni skladen**
Digitalni podpis	***skladen***; ni v uporabi; **ni skladen**
Prikazovanje podpisa	***skladen***; delno skladen; ni v uporabi; **ni skladen**

Elektronski podpis	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Ime in priimek podpisnika	***skladen***; ni v uporabi; **ni skladen**
Datum in čas	***skladen***; ni v uporabi; **ni skladen**
Namen podpisa	***skladen***; ni v uporabi; **ni skladen**
Povezava z zapisi	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Nadzor	***skladen***; ni v uporabi; **ni skladen**
Čitljivost	***skladen***; ni v uporabi; **ni skladen**
Zapis & Podpis	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Avtentičnost povezave	***skladen***; ni v uporabi; **ni skladen**
Podpisi (poglavje C)	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Splošne zahteve	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Avtentičnost podpisa	***skladen***; ni v uporabi; **ni skladen**
Identiteta posameznika	***skladen***; ni v uporabi; **ni skladen**
Prijava uporabe	***skladen***; ni v uporabi; **ni skladen**
Certifikat	***skladen***; ni v uporabi; **ni skladen**
Komponente	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Nebiometrični	***skladen***; delno skladen; ni v uporabi; **ni skladen**
ID in geslo	***skladen***; ni v uporabi; **ni skladen**
Funkcionalnost dostopa	***skladen***; ni v uporabi; **ni skladen**
Omogočena uporaba	***skladen***; ni v uporabi; **ni skladen**
Dodeljevanje	***skladen***; ni v uporabi; **ni skladen**
Biometrični	***skladen***; delno skladen; ni v uporabi; **ni skladen**
ID/geslo	***skladen***; delno skladen; ni v uporabi; **ni skladen**
ID	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Postopki in kontrole	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Avtorizacija	***skladen***; ni v uporabi; **ni skladen**
Zamenjave	***skladen***; ni v uporabi; **ni skladen**
Varnostni ukrepi	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Nepooblaščena uporaba	***skladen***; ni v uporabi; **ni skladen**
Zaznavanje zlorabe	***skladen***; ni v uporabi; **ni skladen**
Poročanje poskusa zlorabe	***skladen***; ni v uporabi; **ni skladen**
Testiranje naprav	***skladen***; delno skladen; ni v uporabi; **ni skladen**
Spremembe	***odobreba***; ni v uporabi; **ni odobrena**
Vodenje	***ustreza***; **neustreza**
Odobritev spremembe	***odobrena***; **ni odobrena**
Sistem in nivoji odgovornosti	***primerna***; **pomanjkljiva**
Potrditev spremembe	***potrjena***; **ni potrjena**
Potek	***ustreza***; ni v uporabi; **neustreza**
Analiza spremembe	**kritična**; velika; ***majhna***
Definiranje vpliva	***velik***; **majhen**
Plan in izvedba testiranj	***zadovoljivo***; **nezadovoljivo**
Dokumentacija	***zadovoljivo***; ni v uporabi; **nezadovoljivo**
Arhiv	***izvedeno***; delno; **pomankljivo**
Politika arhiviranja	***celovita***; pomanjkljiva; **nezadostna**
Postopki	***skladni***; pomanjkljivi; **nezadostni**
Varnost	***zadostna***; pomanjkljiva; **nezadostna**
Spominski mediji	***celovito***; **pomanjkljivo**
Skrbnik sistema	***odličen***; dober; povrečen; **slabši**
Znanja	***ustrezno***; zadovoljivo; povprečen; **nezadovoljivo**
Strokovna izobrazba	***0-2***; 3-4; 5 ; **6-9**
Poznavanje sistema	***odlično***; dobro; povprečno; **slabše**
Poznavanje jezika	***aktivno***; pasivno; **ne poznavanje**
Leta	***dobro***; povprečno; **slabše**
Izkušnje	**5 let naprej**; 1-5; ***0 let***
Osebne lastnosti	***dobro***; povprečno; **slabše**
Nastop	***ustrezno***; zadovoljivo; povprečen; **nezadovoljivo**
Prilagodljivost	***ustrezno***; zadovoljivo; povprečen; **nezadovoljivo**
Dinamičnost	***ustrezno***; zadovoljivo; povprečen; **nezadovoljivo**
Upravljanje kakovosti	***ustrezno***; delno ustrezno; **neustrezno**
Vpliv na kakovost	***velik***; srednji; **majhen**
Inšpektibilnost	***3***; 2; 1; **0**

├Zahtevnost trgov	***velika***; srednja; **mala**
└Podpora vodstva	***velika***; srednja; majhna; **nezadostna**

Ocena

Celovita ocena skladnosti.

1. ***ni odstopa*** Ne kažejo odstop od GMP.
2. drugi Ne spadajo med kritične ali večje, pa vendar kažejo odstop od GMP.
3. večji Neskladnost izdelka ali postopkov z registracijsko dokumentacijo.
4. **kritični** Vplivajo na varnost zdravilo.

Regulativa

Regulativa zajema; Part 11, arhiv, sistem sprememb.

1. ***skladen*** - skladno z zahtevami; Part11, arhiv, spremembe
2. ni v uporabi - ni predmet ocenitve
3. delno skladen - delna skladnost
4. **ni skladen** - ni skladno z zahtevami; Part11, arhiv, spremembe

21 CFR Part 11

Regulativa na področju elekronskih zapisov in podpisov.

1. ***skladen*** - skladno z zahtevo Part 11
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo Part 11

Zapisi (poglavje B)

Poglavje B; Elektronski podpisi.

1. ***skladen*** - skladno z zahtevo Elektronsko zapisi
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo Elektronski zapisi

Zaprti sistemi

Zaprti sistemi (11.10).

1. ***skladen*** - skladno z zahtevo 11.10
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo 11.10

Sistemi & zapisi

Sistemi & zapisi.

1. ***skladen*** - skladno z zahtevo A, B, C, D
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo A, B, C, D

Validacija

Validacija računalniških sistemov.

1. ***skladen*** - skladno z zahtevo A
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo A

Natačnost

Preverjanje natačnosti sistema.

1. ***skladen*** - skladno z zahtevo A.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo A.1

Zanesljivost

Preverjanje zanesljivosti sistema.

1. ***skladen*** - skladno z zahtevo A.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo A.2

Dosledno delovanje

Validacija glede na industrijske standarde.

1. ***skladen*** - skladno z zahtevo A.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo A.3

Razločevanje

Razločevanje neveljavnih in spremenjenih zapisov.

1. ***skladen*** - skladno z zahtevo A.4
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo A.4

Inšpektibilnost

Inšpektibilnost sistema.

1. ***skladen*** - skladno z zahtevo B
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo B

Točne in popolne kopije

Generiranje točnih in popolnih kopij zapisov.

1. ***skladen*** - skladno z zahtevo B.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo B.1

Zaščita zapisov

Zaščita zapisov in njihova ponovna vzpostavitev.

1. ***skladen*** - skladno z zahtevo B.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo B.2

Varnost

Načrtovani in uporabljeni varnostni postopki.

1. ***skladen*** - skladno z zahtevo C
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo C

Fizični dostop

Fizični dostop omejen na pooblaščene posameznike.

1. ***skladen*** - skladno z zahtevo C.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo C.1

Zaporedje korakov

Sistem zagotavlja ustrezno zaporedje korakov.

1. ***skladen*** - skladno z zahtevo C.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo C.2

Preverjanje pooblastil

Preverjanje pooblastil.

1. ***skladen*** - skladno z zahtevo C.3
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo C.3

Logični dostop

Samo pooblaščeni posameznik lahko uporablja dostop.

1. ***skladen*** - skladno z zahtevo C.3.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo C.3.1

Elek. podpisan zapis

Pooblaščeni posameznik elektronsko podpiše zapis.

1. ***skladen*** - skladno z zahtevo C.3.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo C.3.2

I/O naprave

Dostop do vhodno/izhodnih naprav sistema.

1. ***skladen*** - skladno z zahtevo C.3.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo C.3.3

Spreminjanje zapisov

Spreminjanje zapisov ali izvedba specifičnih operacij.

1. ***skladen*** - skladno z zahtevo C.3.4
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - skladno z zahtevo C.3.4

Preverjanje naprav

Preverjanje naprav ali terminalov.

1. ***skladen*** - skladno z zahtevo C.4
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo C.4

Zgodovina dogodkov

Načrtovani in uporabljeni postopki in kontrole.

1. ***skladen*** - skladno z zahtevo D.
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo D.

Izvedba

Izvedba zgodovine dogodkov.

1. ***skladen*** - skladno z zahtevami D.1, D.2, D.3
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami D.1, D.2, D.3

Varnost

Varovanje zgodovine dogodkov.

1. ***skladen*** - skladno z zahtevo D.1
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo D.1

Samodejnost

Računalniško generirana zgodovina dogodkov.

1. ***skladen*** - skladno z zahtevo D.2
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo D.2

Žigosanje

Časovno in datumsko žigosanje.

1. ***skladen*** - skladno z zahtevo D.3
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo D.3

Neodvisni vpisi

Zagotovitev neodvisnih vpisov.

1. ***skladen*** - skladno z zahtevo D.4
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo D.4

Kreiranje

Kreiranje elektronskih zapisov.

1. ***skladen*** - skladno z zahtevo D.4.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo D.4.1

Spreminjanje

Spreminjanje elektronskih zapisov.

1. ***skladen*** - skladno z zahtevo D.4.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo D.4.2

Vzdrževanje

Vzdrževanje elektronskih zapisov.

1. ***skladen*** - skladno z zahtevo D.4.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo D.4.3

Brisanje

Brisanje elektronskih zapisov.

1. ***skladen*** - skladno z zahtevo D.4.4
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo D.4.4

Shranjevanje

Shranjevanje zgodovine dogodkov.

1. ***skladen*** - skladno z zahtevo D.5, D.6, D.7
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo D.5, D.6, D.7

Spremembe

Spremembe ne smejo okrniti predhodnih informacij.

1. ***skladen*** - skladno z zahtevo D.5
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo D.5

Vzdrževanje

Vzdrževanje zgodovine dogodkov.

1. ***skladen*** - skladno z zahtevo D.6
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo D.6

Dostopnost

Dostopnost za pregled in kopiranje.

1. ***skladen*** - skladno z zahtevo D.6
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo D.6

Osebje in dokumentacija

Osebje in dokumentacija.

1. ***skladen*** - skladno z zahtevami E, F, G
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo E, F, G

Kvalifikacija osebja

Kvalifikacija osebja.

1. ***skladen*** - skladno z zahtevami E.1, E.2, E.3
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami E.1, E.2, E.3

Razvijalcev

Razvijalci računalniških sistemov.

1. ***skladno*** - skladno z zahtevo E.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo E.1

Vzdrževalcev

Vzdrževalci računalniških sistemov.

1. ***skladen*** - skladno z zahtevo E.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo E.2

Uporabnikov

Uporabniki računalniških sistemov.

1. ***skladen*** - skladno z zahtevo E.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo E.3

Odgovornosti

Premišljenost in odgovornost.

1. ***skladen*** - skladno z zahtevo F.
2. delno skladen - delno skladen
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo F.

Kontrola dokumentacije

Kontrola sistemske dokumentacije.

1. ***skladen*** - skladno z zahtevami G.1, G.2
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami G.1, G.2.

Kontrola

Kontrola dokumentacije za sistemsko delovanje.

1. ***skladen*** - skladno z zahtevo G.1
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo G.1

Distribucija

Distribucija dokumentacije.

1. ***skladen*** - skladno z zahtevo G.1.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo G.1.1

Dostop

Dostop do dokumentacije.

1. ***skladen*** - skladno z zahtevo G.1.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo G.1.2

Uporaba

Uporaba dokumentacije.

1. ***skladen*** - skladno z zahtevo G.1.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo G.1.3

Sistemska dokumentacija

Nadzor sistemske dokumentacije.

1. ***skladen*** - skladno z zahtevo G.2
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo G.2

Odprti sistemi

Odprti sistemi (11.30).

1. ***skladen*** - skladno z zahtevo 11.30
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo 11.30

Postopki in kontrole

Postopki in kontrole ter atributi.

1. ***skladen*** - skladno z zahtevami H.1, H.2, H.3
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami H.1, H.2, H.3

Avtentičnost

Zahtevana avtentičnost.

1. ***skladen*** - skladno z zahtevo H.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo H.1

Celovitost

Zahtevana celovitost.

1. ***skladen*** - skladno z zahtevo H.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo H.2

Zasebnost

Zahtevana zasebnost.

1. ***skladen*** - skladno z zahtevo H.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo H.3

Postopki in kontrole ter vsebine

Postopki in kontrole in vsebine.

1. ***skladen*** - skladno z zahtevi H.4, H.5, H.6
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami H.4, H.5, H.6

Transformacija

Transformacija primernih pravil iz zaprtih sistemov.

1. ***skladen*** - skladno z zahtevo H.4
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo H.4

Tajnopis dokumentov

Tajnopis dokumentov.

1. ***skladen*** - skladno z zahtevo H.5
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo H.5

Digitalni podpis

Standardi digitalnega podpisa.

1. ***skladen*** - skladno z zahtevo H.6
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo H.6

Prikazovanje podpisa

Prikazovanje podpisa (11.50).

1. ***skladen*** - skladno z zahtevo 11.50
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo 11.50

Elektronski podpis

Elektronski podpis.

1. ***skladen*** - skladno z zahtevo I.1, I.2, I.3
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami I.1, I.2, I.3

Ime in priimek podpisnika

Vpisano ime in priimek podpisnika.

1. ***skladen*** - skladno z zahtevo I.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo I.1

Datum in čas

Vpisan datum in čas.

1. ***skladen*** - skladno z zahtevo I.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo I.2

Namen podpisa

Vpisan namen podpisa.

1. ***skladen*** - skladno z zahtevo I.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo I.3

Povezava z zapisi

Povezava z podpisov z prvotnim zapisom.

1. ***skladen*** - skladno z zahtevama I.4, I.5
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevama I.4, I.5

Nadzor

Podpisi imajo enak nadzor kot elektronski zapisi.

1. ***skladen*** - skladno z zahtevo I.4
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo I.4

Čitljivost

Človeku beljiva oblika.

1. ***skladen*** - skladno z zahtevo I.5
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo I.5

Zapis & Podpis

Zapis & Podpis (11.70) .

1. ***skladen*** - skladno z zahtevo 11.70
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo 11.70

Avtentičnost povezave

Avtentičnost povezave med zapisom in podpisom.

1. ***skladen*** - skladno z zahtevo J
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo J

Podpisi (poglavje C)

Poglavje C ; Elektronski podpisi.

1. ***skladen*** - skladno z zahtevo Elektronski podpisi
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo Elektronski podpisi

Splošne zahteve

Splošne zahteve za elektronske podpise (11.100).

1. ***skladen*** - skladno z zahtevami K.1, K.2, K.3, K.4
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami K.1, K.2, K.3, K.4

Avtentičnost podpisa

Podpis naj bo svojsten posamezniku, unikaten.

1. ***skladen*** - skladno z zahtevo K.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo K.1

Identiteta posameznika

Preverjanje identitete posameznika.

1. ***skladen*** - skladno z zahtevo K.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo K.2

Prijava uporabe

Prijava pri FDA.

1. ***skladen*** - skladno z zahtevo K.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo K.3

Certifikat

Certifikat v papirni obliki, ki ustreza FDA regulativi.

1. ***skladen*** - skladno z zahtevo K.4
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo K.4

Komponente

Komponente elektronskega podpisa in kontrole (11.200).

1. ***skladen*** - skladno z zahtevo 11.200
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo 11.200

Nebiometrični

Nebiometrični elektronski podpisi.

1. ***skladen*** - skladno z zahtevami L.1, L.2, L.3, L.4
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevami L.1, L.2, L.3, L.4

ID in geslo

Identifikacijska koda in geslo.

1. ***skladen*** - skladno z zahtevo L.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo L.1

Funkcionalnost dostopa

Funkcionalnost neprekinjenega in prekinjenega dostopa.

1. ***skladen*** - skladno z zahtevo L.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo L.2

Omogočena uporaba

Omogoča uporaba samo lastnikom podpisa.

1. ***skladen*** - skladno z zahtevo L.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo L.3

Dodeljevanje

Dodeljevanje nebiometričnih podpisov.

1. ***skladen*** - skladno z zahtevo L.4
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo L.4

Biometrični

Biometrični elektronski podpisi.

1. ***skladen*** - skladno z zahtevo M
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo M

ID/geslo

Kontrola za identifikacijsko kodo/geslo (11.300).

1. ***skladen*** - skladno z zahtevo 11.300
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo 11.300

ID

Identifikacijska koda je neponovljiva in preverjena.

1. ***skladen*** - skladno z zahtevo N.1, N.2
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo N.1, N.2

Postopki in kontrole

Uvedeni postopki in kontrole.

1. ***skladen*** - skladno z zahtevo N.3
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo N.3

Avtorizacija

Avtorizacija.

1. ***skladen*** - skladno z zahtevo N.3.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo N.3.1

Zamenjave

Začasne ali trajne zamenjave.

1. ***skladen*** - skladno z zahtevo N.3.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo N.3.2

Varnostni ukrepi

Varnostni ukrepi.

1. ***skladen*** - skladno z zahtevo N.4
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo N.4

Nepooblaščena uporaba

Zaščita pred nepooblaščeno uporabo.

1. ***skladen*** - skladno z zahtevo N.4.1
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo N.4.1

Zaznavanje zlorabe

Zaznavanje poskusa zlorabe.

1. ***skladen*** - skladno z zahtevo N.4.2
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo N.4.2

Poročanje poskusa zlorabe

Poročanje poskusa zlorabe.

1. ***skladen*** - skladno z zahtevo N.4.3
2. ni v uporabi - ni predmet ocenitve
3. **ni skladen** - ni skladno z zahtevo N.4.3

Testiranje naprav

Periodično testiranje naprav.

1. ***skladen*** - skladno z zahtevo N.5
2. delno skladen - delna skladnost
3. ni v uporabi - ni predmet ocenitve
4. **ni skladen** - ni skladno z zahtevo N.5

Spremembe

Celovito obvladovanje sprememb.

1. ***odobreba*** - sprememba se izvaja v skladu s postopki in politiko sprememb
2. ni v uporabi - sprememba ni predmet ocenitve
3. **ni odobrena** - sprememba je v postopku uvedbe oziroma ni bila odobrena

Vodenje

Vodenje sprememb.

1. ***ustreza*** - vodenje spremembe ustrezno
2. **neustreza** - vodenje spremembe neustrezno

Odobritev spremembe

Odobritev spremembe.

1. ***odobrena*** - sprememba je odobrena
2. **ni odobrena** - sprememba ni odobrena

Sistem in nivoji odgovornosti

Vpeljan sistem in nivoji odgovornosti.

1. ***primerna*** - zagotovljene in potrjene so dejanske ravni odgovornosti
2. **pomanjkljiva** - ravni odgovornosti so postavljene preveč ohlapno oz. neformalno

Potrditev spremembe

Potrditev spremembe.

1. ***potrjena*** - sprememba je potrjena
2. **ni potrjena** - sprememba ni potrjena

Potek

Potek procesa spremembe.

1. ***ustreza*** - potek spremembe ustrezen
2. ni v uporabi - sprememba ni predmet ocenitve
3. **neustreza** - potek spremembe neustrezen

Analiza spremembe

Analiza spremembe z možnimi tveganji.

1. **kritična** - analiza sprememb ni bila narejena oziroma ni bila potrjena
2. velika - analiza sprememb prikazuje velik vpliv na kritične operacije
3. ***majhna*** - analiza sprememb prkazuje manjši vpliv na kritične operacije

Definiranje vpliva

Definiranje vpliva na regulatorni status.

1. ***velik*** - sprememba ima velik vpliv na regulatorni status
2. **majhen** - sprememba nima vpliva na regulatorni status

Plan in izvedba testiranj

Plan in izvedba testiranj.

1. ***zadovoljivo*** - izdelan plan testiranj in testiranja so izvedena
2. **nezadovoljivo** - ni izdelan plan testiranj ali testiranja niso izvedena

Dokumentacija

Popravilo vseh dokumentov in evidentiranje.

1. ***zadovoljivo*** - označevanje verzij dokumentov in dokumentirana zgodovina sprememb je ustrezna
2. ni v uporabi - sprememba ni predmet ocenitve
3. **nezadovoljivo** - označevanje verzij in dokumentirana zgodovina sprememb je pomanjkljiva

Arhiv

Arhiv elektronskih podatkov.

1. ***izvedeno*** - arhiviranje ustrezno izvedeno
2. delno - arhiviranje izvedeno nepopolno
3. **pomankljivo** - arhiviranje izvedeno pomanjkljivo

Politika arhiviranja

Politika arhiviranja podjetja.

1. ***celovita*** - zajeti vsi atrebuti elektronskega arhiviranja
2. pomanjkljiva - napisana politika je nepopolna
3. **nezadostna** - izpuščeni ključni atributi elektronskega arhiviranja

Postopki

Aktivnost iz dobre prakse elektronskega arhiviranja.

1. ***skladni*** - dokumentacija in aktivnosti ustrezajo predpisanim postopkom
2. pomanjkljivi - samo dokumentacija ali samo aktivnosti ustrezajo predpisanim postopkom
3. **nezadostni** - dokumentacija in aktivnosti ne ustrezajo predpisanim postopkom

Varnost

Varnost elektronskih zapisov.

1. ***zadostna*** - zapisi so preneseni na varnostno lokacijo z arhivsko zrcalno kopijo
2. pomanjkljiva - zapisi so preneseni na varnostno lokacijo brez arhivske zrcalne kopije
3. **nezadostna** - zapisi so shranjeni na mestu uporabe

Spominski mediji

Uporabljeni spominski mediji.

1. ***celovito*** - spominski medij je vzdrževan v mejah specifikacij in dobre prakse
2. **pomanjkljivo** - spominski medij ni v mejah specifikacij in dobre prakse

Skrbnik sistema

Kandidat, ki skrbi za razvojne faze sistema.

1. ***odličen*** - velika verjetnost, da dobi sistem boljšo oceno od dejanske
2. dober - sistem dobi dejansko oceno
3. povrečen - skrbnik nima vpliva na oceno sistema
4. **slabši** - obstaja verjetnost, da dobi sistem slabšo oceno od dejanske

Znanja

Zahtevana ključna znanja.

1. ***ustrezno*** - skrbnik sistema ima vsa potrebna znanja
2. zadovoljivo - skrbnik sistema ima večino potrebnih znanj
3. povprečen - skrbnik sistema ima le del potrebnih znanj
4. **nezadovoljivo** - skrbnik sistema nima potrebnih znanj

Strokovna izobrazba

Formalna strokovna izobrazba skrbnika sistema.

1. ***0-2*** - 0-Dr., 1- Mr. , 2- visoka strokovna izobrazba
2. 3-4 - 3-višja strokovna izobrazba, 4-srednja strokovna izobrazba
3. 5 - 5-nižja strokovna izobrazba
4. **6-9** - 6-visoka kvalifikacija, 7-kvalificiran, 8-polkvalificiran, 9-nekvalificiran

Poznavanje sistema

Strokovno poznavanje sistema - "tiho znanje".

1. ***odlično*** - skrbnik ima formalno znanje in dobre osebnostne reference
2. dobro - skrbnik ima formalno znanje
3. povprečno - skrbnikovo formalno znanje je nepopolno
4. **slabše** - skrbnikovo formalno znanje je zelo pomanjkljivo

Poznavanje jezika

Formalno potrjeno poznavanje jezikov.

1. ***aktivno*** - aktivno poznavanje angleškega jezika
2. pasivno - pasivno poznavanje angleškega jezika
3. **ne poznavanje** - nepoznavanje angleškega jezika

Leta

Pridobljene izkušnje.

1. ***dobro*** - več kot 5 let
2. povprečno - od 1 do 5 let
3. **slabše** - do 1 leta

Izkušnje

Pridobljene izkušnje.

1. **5 let naprej** - več kot 5 let delovnih izkušnj in intuicija
2. 1-5 - med 1 no 5 let delovnih izkušenj
3. ***0 let*** - do 1 leta delovnih izkušenj

Osebne lastnosti

Primernost za določeno

1. ***dobro*** - skrbnik sistema ima več izrazitih dobrih
2. povprečno - skrbnik sistema ima več dobrih
3. **slabše** - skrbnik sistema ima manj dobrih

Nastop

Sposobnost predstaviteve sistema in

1. ***ustrezno*** - poseduje vse lastnosti dobrega
2. zadovoljivo - poseduje bistvene lastnosti dobrega
3. povprečen - poseduje le del lastnosti dobrega
4. **nezadovoljivo** - slab nastop

Prilagodljivost

Sposobnost prilagoditve različnim

1. ***ustrezno*** - različnim stanjem se takoj prilagodi "naravni
2. zadovoljivo - različnim stanjem se prilagodi spomočjo
3. povprečen - različnim stanjem se prilagodi odvisno od
4. **nezadovoljivo** - različnim stanjem se težko

Dinamičnost

Sposobnost hitrega iskanja rešitev in prezemanje

1. ***ustrezno*** - izpolni vsa pričakovanja in izvaja potrebe
2. zadovoljivo - izvaja potrebne
3. povprečen - delno izpolni pričakovanja in izvaja le del
4. **nezadovoljivo** - ne zpolni naša

Upravljanje kakovosti

Nosilec za implementacijo politike regulatorne

1. ***ustrezno*** - sistem upravljanja kakovosti je
2. delno ustrezno - sistem upravljanja kakovosti je
3. **neustrezno** - sistem upravljanja kakovosti je

Vpliv na kakovost

Vpliv sistema na kakovost in varnost

1. ***velik*** - večji odstop v
2. srednji - odstop v kakovosti
3. **majhen** - nima bistvenega vpliva na

Inšpektibilnost

Vrste inšpekcij.

1. ***3*** - 3 : uspešna inšpekcija s strani regulatornih
2. 2 - 2 : uspešna zunanja
3. 1 - 1 : uspešna partnerjeva
4. **0** - 0 : ni nilo nobene uspešne

Zahtevnost trgov

Zahtevnost trgov.

1. ***velika*** - regulatorno zahtevni
2. srednja - regulatorno običajni
3. **mala** - nezahtevni trgi

10.3. Tabele odločitvenih pravil

Podpora vodstva

Podpora vodstva zagotavljanju skladnosti.

1. ***velika*** - strateška usmeritev in pooblaščanje
2. srednja - strateška usmeritev
3. majhna - verbalna podpora
4. **nezadostna** - neopredeljeno

Tabele odločitvenih pravil

	Regulativa	Skrbnik sistema	Upravljanje kakovosti	Ocena
	33%	14%	53%	
1	<=ni v uporabi	<=povrečen	***ustrezno***	***ni odstopa***
2	***skladen***	*	delno ustrezno	drugi
3	<=ni v uporabi	<=povrečen	delno ustrezno	drugi
4	<=delno skladen	***odličen***	delno ustrezno	drugi
5	***skladen***	**slabši**	<=delno ustrezno	drugi
6	<=ni v uporabi	**slabši**	***ustrezno***	drugi
7	delno skladen	***odličen***	<=delno ustrezno	drugi
8	delno skladen	<=povrečen	***ustrezno***	drugi
9	ni v uporabi	*	**neustrezno**	večji
10	ni v uporabi:delno skladen	***odličen***	**neustrezno**	večji
11	ni v uporabi	**slabši**	>=delno ustrezno	večji
12	delno skladen	dober:povrečen	delno ustrezno	večji
13	delno skladen	**slabši**	***ustrezno***	večji
14	**ni skladen**	<=dober	***ustrezno***	večji
15	***skladen***	*	**neustrezno**	**kritični**
16	>=delno skladen	>=dober	**neustrezno**	**kritični**
17	>=delno skladen	**slabši**	>=delno ustrezno	**kritični**
18	**ni skladen**	*	>=delno ustrezno	**kritični**
19	**ni skladen**	>=povrečen	*	**kritični**

	21 CFR Part 11	Spremembe	Arhiv	Regulativa
	18%	34%	48%	
1	***skladen***	<=ni v uporabi	***izvedeno***	***skladen***
2	ni v uporabi	<=ni v uporabi	***izvedeno***	***skladen***
3	<=ni v uporabi	<=ni v uporabi	delno	delno skladen
4	delno skladen	<=ni v uporabi	<=delno	delno skladen
5	*	*	**pomankljivo**	**ni skladen**
6	*	**ni odobrena**	*	**ni skladen**
7	**ni skladen**	*	*	**ni skladen**

	Zapisi (poglavje B)	Podpisi (poglavje C)	21 CFR Part 11
	50%	50%	
1	***skladen***	***skladen***	***skladen***
2	***skladen***	ni v uporabi	***skladen***
3	ni v uporabi	***skladen***	***skladen***
4	<=ni v uporabi	delno skladen	delno skladen
5	delno skladen	<=ni v uporabi	delno skladen
6	ni v uporabi	ni v uporabi	ni v uporabi
7	*	**ni skladen**	**ni skladen**
8	**ni skladen**	*	**ni skladen**

	Zaprti sistemi	Odprti sistemi	Prikazovanje podpisa	Zapis & Podpis	Zapisi (poglavje B)
	25%	26%	26%	23%	
1	***skladen***	***skladen***	***skladen***	***skladen***	***skladen***
2	***skladen***	***skladen***	***skladen***	ni v uporabi	***skladen***
3	***skladen***	***skladen***	ni v uporabi	***skladen***	***skladen***
4	***skladen***	***skladen***	ni v uporabi	ni v uporabi	***skladen***
5	***skladen***	ni v uporabi	***skladen***	***skladen***	***skladen***
6	***skladen***	ni v uporabi	***skladen***	ni v uporabi	***skladen***
7	***skladen***	ni v uporabi	ni v uporabi	***skladen***	***skladen***
8	***skladen***	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***
9	ni v uporabi	***skladen***	***skladen***	***skladen***	***skladen***
10	ni v uporabi	***skladen***	***skladen***	ni v uporabi	***skladen***
11	ni v uporabi	***skladen***	ni v uporabi	***skladen***	***skladen***
12	ni v uporabi	***skladen***	ni v uporabi	ni v uporabi	***skladen***
13	ni v uporabi	ni v uporabi	***skladen***	***skladen***	***skladen***
14	ni v uporabi	ni v uporabi	***skladen***	ni v uporabi	***skladen***
15	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***	***skladen***
16	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen	delno skladen
17	<=ni v uporabi	<=ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
18	<=ni v uporabi	delno skladen	<=ni v uporabi	<=ni v uporabi	delno skladen
19	delno skladen	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen
20	delno skladen	delno skladen	***skladen***	*	delno skladen
21	ni v uporabi	***skladen***	delno skladen	*	delno skladen
22	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
23	***skladen***	*	*	**ni skladen**	**ni skladen**
24	<=delno skladen	***skladen***	*	**ni skladen**	**ni skladen**
25	*	***skladen***	***skladen***	**ni skladen**	**ni skladen**
26	<=delno skladen	*	>=delno skladen	**ni skladen**	**ni skladen**
27	*	*	>=ni v uporabi	**ni skladen**	**ni skladen**
28	*	*	**ni skladen**	*	**ni skladen**
29	*	>=delno skladen	>=delno skladen	**ni skladen**	**ni skladen**
30	*	>=ni v uporabi	*	**ni skladen**	**ni skladen**
31	*	**ni skladen**	*	*	**ni skladen**
32	>=ni v uporabi	*	***skladen***	**ni skladen**	**ni skladen**
33	>=ni v uporabi	>=delno skladen	*	**ni skladen**	**ni skladen**
34	**ni skladen**	*	*	*	**ni skladen**

	Sistemi & zapisi	Osebje in dokumentacija	Zaprti sistemi
	50%	50%	
1	***skladen***	***skladen***	***skladen***
2	***skladen***	ni v uporabi	***skladen***
3	ni v uporabi	***skladen***	***skladen***
4	<=ni v uporabi	delno skladen	delno skladen
5	delno skladen	<=ni v uporabi	delno skladen
6	ni v uporabi	ni v uporabi	ni v uporabi
7	*	**ni skladen**	**ni skladen**
8	**ni skladen**	*	**ni skladen**

	Validacija	Inšpektibilnost	Varnost	Zgodovina dogodkov	Sistemi & zapisi
	25%	26%	25%	24%	
1	***skladen***	***skladen***	***skladen***	***skladen***	***skladen***
2	***skladen***	***skladen***	***skladen***	ni v uporabi	***skladen***
3	***skladen***	***skladen***	ni v uporabi	***skladen***	***skladen***
4	***skladen***	***skladen***	ni v uporabi	ni v uporabi	***skladen***
5	***skladen***	ni v uporabi	***skladen***	***skladen***	***skladen***
6	***skladen***	ni v uporabi	***skladen***	ni v uporabi	***skladen***
7	***skladen***	ni v uporabi	ni v uporabi	***skladen***	***skladen***
8	***skladen***	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***
9	ni v uporabi	***skladen***	***skladen***	***skladen***	***skladen***
10	ni v uporabi	***skladen***	***skladen***	ni v uporabi	***skladen***
11	ni v uporabi	***skladen***	ni v uporabi	***skladen***	***skladen***
12	ni v uporabi	***skladen***	ni v uporabi	ni v uporabi	***skladen***
13	ni v uporabi	ni v uporabi	***skladen***	***skladen***	***skladen***
14	ni v uporabi	ni v uporabi	***skladen***	ni v uporabi	***skladen***
15	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***	***skladen***
16	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen	delno skladen
17	<=ni v uporabi	<=ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
18	<=ni v uporabi	delno skladen	<=ni v uporabi	<=ni v uporabi	delno skladen
19	delno skladen	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen
20	delno skladen	***skladen***	ni v uporabi	*	delno skladen
21	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
22	***skladen***	*	*	**ni skladen**	**ni skladen**
23	*	*	<=delno skladen	**ni skladen**	**ni skladen**
24	*	*	**ni skladen**	*	**ni skladen**
25	*	>=delno skladen	*	**ni skladen**	**ni skladen**
26	*	**ni skladen**	*	*	**ni skladen**
27	>=ni v uporabi	*	*	**ni skladen**	**ni skladen**
28	**ni skladen**	*	*	*	**ni skladen**

	Natačnost	Zanesljivost	Dosledno delovanje	Razločevanje	Validacija
	25%	25%	25%	25%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
4	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
5	***skladen***	<=ni v uporabi	<=ni v uporabi	**ni skladen**	delno skladen
6	<=ni v uporabi	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
7	<=ni v uporabi	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
8	***skladen***	<=ni v uporabi	**ni skladen**	<=ni v uporabi	delno skladen
9	<=ni v uporabi	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
10	<=ni v uporabi	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
11	***skladen***	**ni skladen**	<=ni v uporabi	<=ni v uporabi	delno skladen
12	<=ni v uporabi	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
13	<=ni v uporabi	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
14	**ni skladen**	***skladen***	<=ni v uporabi	<=ni v uporabi	delno skladen
15	**ni skladen**	<=ni v uporabi	***skladen***	<=ni v uporabi	delno skladen
16	**ni skladen**	<=ni v uporabi	<=ni v uporabi	***skladen***	delno skladen
17	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
18	*	*	**ni skladen**	**ni skladen**	**ni skladen**
19	*	**ni skladen**	*	**ni skladen**	**ni skladen**
20	*	**ni skladen**	**ni skladen**	*	**ni skladen**
21	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
22	>=ni v uporabi	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
23	>=ni v uporabi	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
24	**ni skladen**	*	*	**ni skladen**	**ni skladen**
25	**ni skladen**	*	**ni skladen**	*	**ni skladen**
26	**ni skladen**	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**
27	**ni skladen**	**ni skladen**	*	*	**ni skladen**

	Točne in popolne kopije	Zaščita zapisov	Inšpektibilnost
	50%	50%	
1	***skladen***	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	***skladen***
3	***skladen***	**ni skladen**	delno skladen
4	**ni skladen**	***skladen***	delno skladen
5	ni v uporabi	ni v uporabi	ni v uporabi
6	>=ni v uporabi	**ni skladen**	**ni skladen**
7	**ni skladen**	>=ni v uporabi	**ni skladen**

	Fizični dostop	Zaporedje korakov	Preverjanje pooblastil	Preverjanje naprav	Varnost
	32%	32%	18%	18%	
1	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***	***skladen***
2	<=ni v uporabi	<=ni v uporabi	***skladen***	ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	ni v uporabi	***skladen***	***skladen***
4	***skladen***	<=ni v uporabi	ni v uporabi	ni v uporabi	***skladen***
5	<=ni v uporabi	***skladen***	ni v uporabi	ni v uporabi	***skladen***
6	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen	delno skladen
7	<=ni v uporabi	<=ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
8	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
9	*	*	*	**ni skladen**	**ni skladen**
10	*	*	**ni skladen**	*	**ni skladen**
11	*	**ni skladen**	*	*	**ni skladen**
12	**ni skladen**	*	*	*	**ni skladen**

	Logični dostop	Elek. podpisan zapis	I/O naprave	Spreminjanje zapisov	Preverjanje pooblastil
	25%	25%	25%	25%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
4	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
5	***skladen***	<=ni v uporabi	<=ni v uporabi	**ni skladen**	delno skladen
6	<=ni v uporabi	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
7	<=ni v uporabi	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
8	***skladen***	<=ni v uporabi	**ni skladen**	<=ni v uporabi	delno skladen
9	<=ni v uporabi	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
10	<=ni v uporabi	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
11	***skladen***	**ni skladen**	<=ni v uporabi	<=ni v uporabi	delno skladen
12	<=ni v uporabi	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
13	<=ni v uporabi	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
14	**ni skladen**	***skladen***	<=ni v uporabi	<=ni v uporabi	delno skladen
15	**ni skladen**	<=ni v uporabi	***skladen***	<=ni v uporabi	delno skladen
16	**ni skladen**	<=ni v uporabi	<=ni v uporabi	***skladen***	delno skladen
17	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
18	*	*	**ni skladen**	**ni skladen**	**ni skladen**
19	*	**ni skladen**	*	**ni skladen**	**ni skladen**
20	*	**ni skladen**	**ni skladen**	*	**ni skladen**
21	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
22	>=ni v uporabi	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
23	>=ni v uporabi	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
24	**ni skladen**	*	*	**ni skladen**	**ni skladen**
25	**ni skladen**	*	**ni skladen**	*	**ni skladen**
26	**ni skladen**	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**
27	**ni skladen**	**ni skladen**	*	*	**ni skladen**

	Izvedba	Shranjevanje	Zgodovina dogodkov
	50%	50%	
1	***skladen***	***skladen***	***skladen***
2	***skladen***	ni v uporabi	***skladen***
3	ni v uporabi	***skladen***	***skladen***
4	<=ni v uporabi	delno skladen	delno skladen
5	delno skladen	<=ni v uporabi	delno skladen
6	ni v uporabi	ni v uporabi	ni v uporabi
7	*	**ni skladen**	**ni skladen**
8	**ni skladen**	*	**ni skladen**

	Varnost	Samodejnost	Žigosanje	Neodvisni vpisi	Izvedba
	25%	25%	25%	25%	
1	***skladen***	***skladen***	***skladen***	***skladen***	***skladen***
2	***skladen***	***skladen***	***skladen***	ni v uporabi	***skladen***
3	***skladen***	***skladen***	ni v uporabi	***skladen***	***skladen***
4	***skladen***	***skladen***	ni v uporabi	ni v uporabi	***skladen***
5	***skladen***	ni v uporabi	***skladen***	***skladen***	***skladen***
6	***skladen***	ni v uporabi	***skladen***	ni v uporabi	***skladen***
7	***skladen***	ni v uporabi	ni v uporabi	***skladen***	***skladen***
8	***skladen***	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***
9	ni v uporabi	***skladen***	***skladen***	***skladen***	***skladen***
10	ni v uporabi	***skladen***	***skladen***	ni v uporabi	***skladen***
11	ni v uporabi	***skladen***	ni v uporabi	***skladen***	***skladen***
12	ni v uporabi	***skladen***	ni v uporabi	ni v uporabi	***skladen***
13	ni v uporabi	ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
14	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***	***skladen***
15	<=delno skladen	<=ni v uporabi	<=ni v uporabi	delno skladen	delno skladen
16	<=ni v uporabi	<=delno skladen	<=ni v uporabi	delno skladen	delno skladen
17	<=ni v uporabi	<=ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
18	<=ni v uporabi	<=ni v uporabi	delno skladen:ni v uporabi	delno skladen	delno skladen
19	<=ni v uporabi	delno skladen	<=ni v uporabi	<=ni v uporabi	delno skladen
20	delno skladen	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen
21	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
22	*	*	*	**ni skladen**	**ni skladen**
23	*	*	**ni skladen**	*	**ni skladen**
24	*	**ni skladen**	*	*	**ni skladen**
25	**ni skladen**	*	*	*	**ni skladen**

	Kreiranje	Spreminjanje	Vzdrževanje	Brisanje	Neodvisni vpisi
	28%	22%	25%	24%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
4	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
5	***skladen***	<=ni v uporabi	<=ni v uporabi	**ni skladen**	delno skladen
6	<=ni v uporabi	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
7	<=ni v uporabi	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
8	***skladen***	<=ni v uporabi	**ni skladen**	<=ni v uporabi	delno skladen
9	<=ni v uporabi	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
10	<=ni v uporabi	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
11	***skladen***	**ni skladen**	<=ni v uporabi	<=ni v uporabi	delno skladen
12	<=ni v uporabi	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
13	<=ni v uporabi	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
14	**ni skladen**	<=ni v uporabi	***skladen***	<=ni v uporabi	delno skladen
15	**ni skladen**	ni v uporabi	<=ni v uporabi	***skladen***	delno skladen
16	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
17	*	*	**ni skladen**	**ni skladen**	**ni skladen**
18	*	**ni skladen**	*	**ni skladen**	**ni skladen**
19	*	**ni skladen**	**ni skladen**	*	**ni skladen**
20	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
21	>=ni v uporabi	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
22	>=ni v uporabi	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
23	**ni skladen**	*	*	**ni skladen**	**ni skladen**
24	**ni skladen**	***skladen***	>=ni v uporabi	*	**ni skladen**
25	**ni skladen**	*	>=ni v uporabi	>=ni v uporabi	**ni skladen**
26	**ni skladen**	*	**ni skladen**	*	**ni skladen**
27	**ni skladen**	**ni skladen**	*	*	**ni skladen**

	Spremembe	Vzdrževanje	Dostopnost	Shranjevanje
	33%	33%	33%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
4	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
5	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
6	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
7	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
8	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
9	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
10	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
11	*	**ni skladen**	**ni skladen**	**ni skladen**
12	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
13	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
14	**ni skladen**	*	**ni skladen**	**ni skladen**
15	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
16	**ni skladen**	**ni skladen**	*	**ni skladen**

	Kvalifikacija osebja	Odgovornosti	Kontrola dokumentacije	Osebje in dokumentacija
	33%	32%	34%	
1	***skladen***	***skladen***	***skladen***	***skladen***
2	***skladen***	***skladen***	ni v uporabi	***skladen***
3	***skladen***	ni v uporabi	***skladen***	***skladen***
4	***skladen***	ni v uporabi	ni v uporabi	***skladen***
5	ni v uporabi	***skladen***	***skladen***	***skladen***
6	ni v uporabi	***skladen***	ni v uporabi	***skladen***
7	ni v uporabi	ni v uporabi	***skladen***	***skladen***
8	<=ni v uporabi	<=ni v uporabi	delno skladen	delno skladen
9	<=ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
10	delno skladen	<=ni v uporabi	<=ni v uporabi	delno skladen
11	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
12	ni v uporabi	**ni skladen**	delno skladen	ni v uporabi
13	*	*	**ni skladen**	**ni skladen**
14	<=delno skladen	**ni skladen**	*	**ni skladen**
15	*	**ni skladen**	***skladen***	**ni skladen**
16	*	**ni skladen**	>=ni v uporabi	**ni skladen**
17	**ni skladen**	*	*	**ni skladen**

	Razvijalcev	Vzdrževalcev	Uporabnikov	Kvalifikacija osebja
	33%	33%	33%	
1	***skladno***	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
4	***skladno***	<=ni v uporabi	**ni skladen**	delno skladen
5	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
6	***skladno***	**ni skladen**	<=ni v uporabi	delno skladen
7	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
8	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
9	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
10	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
11	*	**ni skladen**	**ni skladen**	**ni skladen**
12	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
13	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
14	**ni skladen**	*	**ni skladen**	**ni skladen**
15	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
16	**ni skladen**	**ni skladen**	*	**ni skladen**

	Kontrola	Sistemska dokumentacija	Kontrola dokumentacije
	50%	50%	
1	***skladen***	***skladen***	***skladen***
2	***skladen***	ni v uporabi	***skladen***
3	ni v uporabi	***skladen***	***skladen***
4	<=ni v uporabi	delno skladen	delno skladen
5	delno skladen	<=ni v uporabi	delno skladen
6	ni v uporabi	ni v uporabi	ni v uporabi
7	*	**ni skladen**	**ni skladen**
8	**ni skladen**	*	**ni skladen**

	Distribucija	Dostop	Uporaba	Kontrola
	33%	33%	33%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
4	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
5	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
6	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
7	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
8	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
9	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
10	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
11	*	**ni skladen**	**ni skladen**	**ni skladen**
12	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
13	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
14	**ni skladen**	*	**ni skladen**	**ni skladen**
15	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
16	**ni skladen**	**ni skladen**	*	**ni skladen**

	Postopki in kontrole	Postopki in kontrole ter vsebine	Odprti sistemi
	50%	50%	
1	***skladen***	***skladen***	***skladen***
2	***skladen***	ni v uporabi	***skladen***
3	ni v uporabi	***skladen***	***skladen***
4	<=ni v uporabi	delno skladen	delno skladen
5	delno skladen	<=ni v uporabi	delno skladen
6	ni v uporabi	ni v uporabi	ni v uporabi
7	*	**ni skladen**	**ni skladen**
8	**ni skladen**	*	**ni skladen**

	Avtentičnost	Celovitost	Zasebnost	Postopki in kontrole
	29%	38%	33%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
4	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
5	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
6	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
7	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
8	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
9	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
10	*	**ni skladen**	>=ni v uporabi	**ni skladen**
11	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
12	**ni skladen**	*	**ni skladen**	**ni skladen**
13	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
14	**ni skladen**	**ni skladen**	*	**ni skladen**

	Transformacija	Tajnopis dokumentov	Digitalni podpis	Postopki in kontrole ter vsebine
	33%	33%	33%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
4	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
5	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
6	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
7	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
8	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
9	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
10	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
11	*	**ni skladen**	**ni skladen**	**ni skladen**
12	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
13	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
14	**ni skladen**	*	**ni skladen**	**ni skladen**
15	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
16	**ni skladen**	**ni skladen**	*	**ni skladen**

	Elektronski podpis	Povezava z zapisi	Prikazovanje podpisa
	50%	50%	
1	***skladen***	***skladen***	***skladen***
2	***skladen***	ni v uporabi	***skladen***
3	ni v uporabi	***skladen***	***skladen***
4	<=ni v uporabi	delno skladen	delno skladen
5	delno skladen	<=ni v uporabi	delno skladen
6	ni v uporabi	ni v uporabi	ni v uporabi
7	*	**ni skladen**	**ni skladen**
8	**ni skladen**	*	**ni skladen**

	Ime in priimek podpisnika	Datum in čas	Namen podpisa	Elektronski podpis
	33%	33%	33%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
4	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
5	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
6	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
7	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
8	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
9	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
10	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
11	*	**ni skladen**	**ni skladen**	**ni skladen**
12	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
13	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
14	**ni skladen**	*	**ni skladen**	**ni skladen**
15	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
16	**ni skladen**	**ni skladen**	*	**ni skladen**

	Nadzor	Čitljivost	Povezava z zapisi
	50%	50%	
1	***skladen***	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	***skladen***
3	***skladen***	**ni skladen**	delno skladen
4	**ni skladen**	***skladen***	delno skladen
5	ni v uporabi	ni v uporabi	ni v uporabi
6	>=ni v uporabi	**ni skladen**	**ni skladen**
7	**ni skladen**	>=ni v uporabi	**ni skladen**

	Avtentičnost povezave	Zapis & Podpis
	100%	
1	***skladen***	***skladen***
2	ni v uporabi	ni v uporabi
3	**ni skladen**	**ni skladen**

	Splošne zahteve	Komponente	ID/geslo	Podpisi (poglavje C)
	33%	33%	33%	
1	***skladen***	***skladen***	***skladen***	***skladen***
2	***skladen***	***skladen***	ni v uporabi	***skladen***
3	***skladen***	ni v uporabi	***skladen***	***skladen***
4	***skladen***	ni v uporabi	ni v uporabi	***skladen***
5	ni v uporabi	***skladen***	***skladen***	***skladen***
6	ni v uporabi	***skladen***	ni v uporabi	***skladen***
7	ni v uporabi	ni v uporabi	***skladen***	***skladen***
8	<=ni v uporabi	<=ni v uporabi	delno skladen	delno skladen
9	<=ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
10	delno skladen	<=ni v uporabi	<=ni v uporabi	delno skladen
11	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
12	*	*	**ni skladen**	**ni skladen**
13	*	**ni skladen**	*	**ni skladen**
14	**ni skladen**	*	*	**ni skladen**

	Avtentičnost podpisa	Identiteta posameznika	Prijava uporabe	Certifikat	Splošne zahteve
	25%	25%	25%	25%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
4	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
5	***skladen***	<=ni v uporabi	<=ni v uporabi	**ni skladen**	delno skladen
6	<=ni v uporabi	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
7	<=ni v uporabi	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
8	***skladen***	<=ni v uporabi	**ni skladen**	<=ni v uporabi	delno skladen
9	<=ni v uporabi	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
10	<=ni v uporabi	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
11	***skladen***	**ni skladen**	<=ni v uporabi	<=ni v uporabi	delno skladen
12	<=ni v uporabi	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
13	<=ni v uporabi	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
14	**ni skladen**	***skladen***	<=ni v uporabi	<=ni v uporabi	delno skladen
15	**ni skladen**	<=ni v uporabi	***skladen***	<=ni v uporabi	delno skladen
16	**ni skladen**	<=ni v uporabi	<=ni v uporabi	***skladen***	delno skladen
17	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
18	*	*	**ni skladen**	**ni skladen**	**ni skladen**
19	*	**ni skladen**	*	**ni skladen**	**ni skladen**
20	*	**ni skladen**	**ni skladen**	*	**ni skladen**
21	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
22	>=ni v uporabi	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
23	>=ni v uporabi	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
24	**ni skladen**	*	*	**ni skladen**	**ni skladen**
25	**ni skladen**	*	**ni skladen**	*	**ni skladen**
26	**ni skladen**	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**
27	**ni skladen**	**ni skladen**	*	*	**ni skladen**

	Nebiometrični	Biometrični	Komponente
	50%	50%	
1	***skladen***	***skladen***	***skladen***
2	***skladen***	ni v uporabi	***skladen***
3	ni v uporabi	***skladen***	***skladen***
4	<=ni v uporabi	delno skladen	delno skladen
5	delno skladen	<=ni v uporabi	delno skladen
6	ni v uporabi	ni v uporabi	ni v uporabi
7	*	**ni skladen**	**ni skladen**
8	**ni skladen**	*	**ni skladen**

	ID in geslo	Funkcionalnost dostopa	Omogočena uporaba	Dodeljevanje	Nebiometrični
	27%	24%	25%	24%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
4	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
5	***skladen***	<=ni v uporabi	<=ni v uporabi	**ni skladen**	delno skladen
6	<=ni v uporabi	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
7	<=ni v uporabi	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
8	***skladen***	<=ni v uporabi	**ni skladen**	<=ni v uporabi	delno skladen
9	<=ni v uporabi	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
10	<=ni v uporabi	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
11	***skladen***	**ni skladen**	<=ni v uporabi	<=ni v uporabi	delno skladen
12	<=ni v uporabi	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
13	<=ni v uporabi	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
14	**ni skladen**	<=ni v uporabi	***skladen***	<=ni v uporabi	delno skladen
15	**ni skladen**	***skladen***	<=ni v uporabi	ni v uporabi	delno skladen
16	**ni skladen**	ni v uporabi	<=ni v uporabi	***skladen***	delno skladen
17	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
18	*	*	**ni skladen**	**ni skladen**	**ni skladen**
19	*	**ni skladen**	*	**ni skladen**	**ni skladen**
20	*	**ni skladen**	**ni skladen**	*	**ni skladen**
21	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
22	>=ni v uporabi	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
23	>=ni v uporabi	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
24	**ni skladen**	*	*	**ni skladen**	**ni skladen**
25	**ni skladen**	***skladen***	>=ni v uporabi	***skladen***	**ni skladen**
26	**ni skladen**	*	**ni skladen**	*	**ni skladen**
27	**ni skladen**	>=ni v uporabi	>=ni v uporabi	>=ni v uporabi	**ni skladen**
28	**ni skladen**	**ni skladen**	*	*	**ni skladen**

	ID	Postopki in kontrole	Varnostni ukrepi	Testiranje naprav	ID/geslo
	25%	25%	25%	25%	
1	***skladen***	***skladen***	***skladen***	***skladen***	***skladen***
2	***skladen***	***skladen***	***skladen***	ni v uporabi	***skladen***
3	***skladen***	***skladen***	ni v uporabi	***skladen***	***skladen***
4	***skladen***	***skladen***	ni v uporabi	ni v uporabi	***skladen***
5	***skladen***	delno skladen	delno skladen	***skladen***	***skladen***
6	***skladen***	delno skladen	delno skladen	ni v uporabi	***skladen***
7	***skladen***	ni v uporabi	***skladen***	***skladen***	***skladen***
8	***skladen***	ni v uporabi	***skladen***	ni v uporabi	***skladen***
9	***skladen***	ni v uporabi	ni v uporabi	***skladen***	***skladen***
10	***skladen***	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***
11	ni v uporabi	***skladen***	***skladen***	***skladen***	***skladen***
12	ni v uporabi	***skladen***	***skladen***	ni v uporabi	***skladen***
13	ni v uporabi	***skladen***	ni v uporabi	***skladen***	***skladen***
14	ni v uporabi	***skladen***	ni v uporabi	ni v uporabi	***skladen***
15	ni v uporabi	ni v uporabi	***skladen***	***skladen***	***skladen***
16	ni v uporabi	ni v uporabi	***skladen***	ni v uporabi	***skladen***
17	ni v uporabi	ni v uporabi	ni v uporabi	***skladen***	***skladen***
18	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen	delno skladen
19	<=ni v uporabi	***skladen***	delno skladen	<=ni v uporabi	delno skladen
20	<=ni v uporabi	delno skladen	***skladen***	<=ni v uporabi	delno skladen
21	<=ni v uporabi	delno skladen	ni v uporabi	<=ni v uporabi	delno skladen
22	<=ni v uporabi	ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
23	delno skladen	<=ni v uporabi	<=ni v uporabi	<=ni v uporabi	delno skladen
24	delno skladen:ni v uporabi	<=ni v uporabi	delno skladen	<=ni v uporabi	delno skladen
25	delno skladen:ni v uporabi	delno skladen	<=ni v uporabi	<=ni v uporabi	delno skladen
26	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
27	*	*	*	**ni skladen**	**ni skladen**
28	*	*	**ni skladen**	*	**ni skladen**
29	*	**ni skladen**	*	*	**ni skladen**
30	**ni skladen**	*	*	*	**ni skladen**

	Avtorizacija	Zamenjave	Postopki in kontrole
	50%	50%	
1	***skladen***	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	***skladen***
3	***skladen***	**ni skladen**	delno skladen
4	**ni skladen**	***skladen***	delno skladen
5	ni v uporabi	ni v uporabi	ni v uporabi
6	>=ni v uporabi	**ni skladen**	**ni skladen**
7	**ni skladen**	>=ni v uporabi	**ni skladen**

	Nepooblaščena uporaba	Zaznavanje zlorabe	Poročanje poskusa zlorabe	Varnostni ukrepi
	33%	33%	33%	
1	***skladen***	<=ni v uporabi	<=ni v uporabi	***skladen***
2	<=ni v uporabi	***skladen***	<=ni v uporabi	***skladen***
3	<=ni v uporabi	<=ni v uporabi	***skladen***	***skladen***
4	***skladen***	<=ni v uporabi	**ni skladen**	delno skladen
5	<=ni v uporabi	***skladen***	**ni skladen**	delno skladen
6	***skladen***	**ni skladen**	<=ni v uporabi	delno skladen
7	<=ni v uporabi	**ni skladen**	***skladen***	delno skladen
8	**ni skladen**	***skladen***	<=ni v uporabi	delno skladen
9	**ni skladen**	<=ni v uporabi	***skladen***	delno skladen
10	ni v uporabi	ni v uporabi	ni v uporabi	ni v uporabi
11	*	**ni skladen**	**ni skladen**	**ni skladen**
12	>=ni v uporabi	>=ni v uporabi	**ni skladen**	**ni skladen**
13	>=ni v uporabi	**ni skladen**	>=ni v uporabi	**ni skladen**
14	**ni skladen**	*	**ni skladen**	**ni skladen**
15	**ni skladen**	>=ni v uporabi	>=ni v uporabi	**ni skladen**
16	**ni skladen**	**ni skladen**	*	**ni skladen**

	Vodenje	Potek	Spremembe
	57%	43%	
1	***ustreza***	***ustreza***	***odobreba***
2	*	ni v uporabi	ni v uporabi
3	*	**neustreza**	**ni odobrena**
4	**neustreza**	***ustreza***	**ni odobrena**

	Odobritev spremembe	Sistem in nivoji odgovornosti	Potrditev spremembe	Vodenje
	33%	33%	33%	
1	***odobrena***	***primerna***	***potrjena***	***ustreza***
2	*	*	**ni potrjena**	**neustreza**
3	*	**pomanjkljiva**	*	**neustreza**
4	**ni odobrena**	*	*	**neustreza**

	Analiza spremembe	Definiranje vpliva	Plan in izvedba testiranj	Dokumentacija	Potek
	30%	0%	40%	30%	
1	***majhna***	*	***zadovoljivo***	***zadovoljivo***	***ustreza***
2	*	*	*	ni v uporabi	ni v uporabi
3	<=velika	*	*	***zadovoljivo***	**neustreza**
4	*	*	*	**nezadovoljivo**	**neustreza**
5	*	*	**nezadovoljivo**	***zadovoljivo***	**neustreza**

	Politika arhiviranja	Postopki	Varnost	Spominski mediji	Arhiv
	19%	19%	19%	44%	
1	***celovita***	***skladni***	***zadostna***	***celovito***	***izvedeno***
2	<=pomanjkljiva	<=pomanjkljivi	pomanjkljiva	***celovito***	delno
3	<=pomanjkljiva	pomanjkljivi	<=pomanjkljiva	***celovito***	delno
4	pomanjkljiva	<=pomanjkljivi	<=pomanjkljiva	***celovito***	delno
5	*	*	*	**pomanjkljivo**	**pomankljivo**
6	*	*	**nezadostna**	*	**pomankljivo**
7	*	**nezadostni**	*	*	**pomankljivo**
8	**nezadostna**	*	*	*	**pomankljivo**

	Znanja	Leta	Osebne lastnosti	Skrbnik sistema
	19%	44%	37%	
1	ustrezno	<=povprečno	dobro	odličen
2	<=povprečen	dobro	dobro	odličen
3	ustrezno	dobro	>=povprečno	dober
4	ustrezno	<=povprečno	povprečno	dober
5	*	dobro	povprečno	dober
6	zadovoljivo:povprečen	povprečno	dobro	dober
7	nezadovoljivo	dobro	<=povprečno	dober
8	<=povprečen	povprečno	slabše	povrečen
9	ustrezno	slabše	<=povprečno	povrečen
10	<=povprečen	slabše	dobro	povrečen
11	zadovoljivo:povprečen	<=povprečno	slabše	povrečen
12	zadovoljivo:povprečen	povprečno	>=povprečno	povrečen
13	povprečen	>=povprečno	povprečno	povrečen
14	povprečen	slabše	<=povprečno	povrečen
15	nezadovoljivo	povprečno	dobro	povrečen
16	*	slabše	slabše	slabši
17	zadovoljivo	slabše	>=povprečno	slabši
18	nezadovoljivo	*	slabše	slabši
19	nezadovoljivo	>=povprečno	>=povprečno	slabši
20	nezadovoljivo	slabše	*	slabši

	Strokovna izobrazba	Poznavanje sistema	Poznavanje jezika	Znanja
	42%	23%	35%	
1	0-2	<=dobro	<=pasivno	ustrezno
2	0-2	<=povprečno	aktivno	ustrezno
3	<=3-4	odlično	<=pasivno	ustrezno
4	0-2	povprečno	pasivno	zadovoljivo
5	0-2	slabše	aktivno	zadovoljivo
6	3-4	dobro	<=pasivno	zadovoljivo
7	3-4	dobro:povprečno	aktivno	zadovoljivo
8	<=3-4	<=povprečno	ne poznavanje	povprečen
9	0-2	slabše	pasivno	povprečen
10	3-4	povprečno	>=pasivno	povprečen
11	3-4:5	povprečno	pasivno	povprečen
12	3-4	slabše	aktivno	povprečen
13	5	<=povprečno	<=pasivno	povprečen
14	>=5	odlično	aktivno	povprečen
15	*	slabše	ne poznavanje	nezadovoljivo
16	>=3-4	slabše	>=pasivno	nezadovoljivo
17	>=5	*	ne poznavanje	nezadovoljivo
18	>=5	slabše	*	nezadovoljivo
19	6-9	*	>=pasivno	nezadovoljivo
20	6-9	>=dobro	*	nezadovoljivo

	Izkušnje	Leta
	100%	
1	5 let naprej	dobro
2	1-5	povprečno
3	0 let	slabše

	Nastop	Prilagodljivost	Dinamičnost	Osebne lastnosti
	38%	32%	30%	
1	***ustrezno***	***ustrezno***	*	***dobro***
2	***ustrezno***	<=povprečen	***ustrezno***	***dobro***
3	<=povprečen	***ustrezno***	***ustrezno***	***dobro***
4	***ustrezno***	povprečen	<=povprečen	***dobro***
5	***ustrezno***	zadovoljivo	>=zadovoljivo	povprečno
6	<=povprečen	zadovoljivo	zadovoljivo:povprečen	povprečno
7	***ustrezno***	zadovoljivo:povprečen	**nezadovoljivo**	povprečno
8	***ustrezno***	**nezadovoljivo**	<=povprečen	povprečno
9	<=povprečen	**nezadovoljivo**	***ustrezno***	povprečno
10	zadovoljivo:povprečen	***ustrezno***	>=zadovoljivo	povprečno
11	zadovoljivo:povprečen	<=povprečen	zadovoljivo:povprečen	povprečno
12	>=zadovoljivo	***ustrezno***	zadovoljivo:povprečen	povprečno
13	zadovoljivo:povprečen	zadovoljivo:povprečen	<=povprečen	povprečno
14	zadovoljivo:povprečen	>=zadovoljivo	***ustrezno***	povprečno
15	>=zadovoljivo	zadovoljivo:povprečen	***ustrezno***	povprečno
16	**nezadovoljivo**	***ustrezno***	<=povprečen	povprečno
17	**nezadovoljivo**	<=povprečen	***ustrezno***	povprečno
18	*	**nezadovoljivo**	**nezadovoljivo**	**slabše**
19	>=zadovoljivo	>=zadovoljivo	**nezadovoljivo**	**slabše**
20	>=zadovoljivo	**nezadovoljivo**	>=zadovoljivo	**slabše**
21	**nezadovoljivo**	*	**nezadovoljivo**	**slabše**
22	**nezadovoljivo**	>=zadovoljivo	>=zadovoljivo	**slabše**
23	**nezadovoljivo**	**nezadovoljivo**	*	**slabše**

	Vpliv na kakovost	Inšpektibilnost	Zahtevnost trgov	Podpora vodstva	Upravljanje kakovosti
	22%	26%	12%	41%	
1	velik	3	*	<=srednja	ustrezno
2	velik	<=2	*	velika	ustrezno
3	*	3	velika	<=srednja	ustrezno
4	*	3	*	velika	ustrezno
5	velik	<=1	mala	velika	ustrezno
6	*	3	mala	<=srednja	ustrezno
7	*	<=2	mala	velika	ustrezno
8	majhen	3	*	<=majhna	ustrezno
9	majhen	<=2	*	<=srednja	ustrezno
10	majhen	<=1	>=srednja	velika	ustrezno
11	majhen	<=2	mala	<=majhna	ustrezno
12	majhen	<=1	mala	<=srednja	ustrezno
13	majhen	*	mala	velika	ustrezno
14	velik	3	>=srednja	majhna	delno ustrezno
15	<=srednji	3	mala	majhna	delno ustrezno
16	<=srednji	2	*	srednja	delno ustrezno
17	<=srednji	2:1	>=srednja	srednja	delno ustrezno
18	<=srednji	1	<=srednja	velika	delno ustrezno
19	*	1	velika	velika	delno ustrezno
20	<=srednji	1	srednja	<=srednja	delno ustrezno
21	*	1	srednja	srednja	delno ustrezno
22	velik	1	mala	srednja:majhna	delno ustrezno
23	srednji	3	velika	majhna	delno ustrezno
24	srednji	<=1	srednja	srednja	delno ustrezno
25	srednji	<=2	mala	majhna	delno ustrezno
26	srednji	2	<=srednja	<=srednja	delno ustrezno
27	srednji	>=2	<=srednja	velika	delno ustrezno
28	srednji	>=1	*	velika	delno ustrezno
29	srednji	1	>=srednja	<=srednja	delno ustrezno
30	srednji	>=1	mala	<=srednja	delno ustrezno
31	>=srednji	0	<=srednja	velika	delno ustrezno
32	>=srednji	0	mala	srednja	delno ustrezno
33	majhen	3	mala	nezadostna	delno ustrezno
34	majhen	2:1	<=srednja	majhna	delno ustrezno
35	majhen	1	velika	<=majhna	delno ustrezno
36	majhen	>=1	velika	<=srednja	delno ustrezno
37	majhen	1	<=srednja	srednja:majhna	delno ustrezno
38	majhen	>=1	<=srednja	srednja	delno ustrezno
39	majhen	1	*	majhna	delno ustrezno
40	majhen	>=1	mala	majhna	delno ustrezno
41	majhen	0	<=srednja	<=srednja	delno ustrezno
42	majhen	0	*	srednja	delno ustrezno
43	majhen	0	mala	srednja:majhna	delno ustrezno
44	velik	*	velika	>=majhna	neustrezno
45	<=srednji	*	*	nezadostna	neustrezno
46	*	*	<=srednja	nezadostna	neustrezno
47	velik	2	*	>=majhna	neustrezno
48	<=srednji	>=2	<=srednja	>=majhna	neustrezno
49	*	>=2	*	nezadostna	neustrezno
50	<=srednji	>=1	velika	>=srednja	neustrezno
51	velik	0	*	*	neustrezno
52	<=srednji	0	<=srednja	>=srednja	neustrezno
53	*	0	<=srednja	>=majhna	neustrezno
54	srednji	*	srednja	>=majhna	neustrezno
55	srednji	>=1	*	>=majhna	neustrezno