UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA KRITIČNOSTI RAČUNALNIŠKIH SISTEMOV GLEDE NA REGULATIVO O ELEKTRONSKIH ZAPISIH IN ELEKTRONSKIH PODPISIH

Ljubljana, maj 2002 Robert Hribar

Pričujoče delo je prikaz večparametrskega odločitvenega modela za analizo kritičnosti računalniških sistemov glede na regulativo o elektronskih zapisih in elektronskih podpisih.

Na osnovi študija literature, viharjenja možganov in izvedenih posvetovanj so bili določeni osnovni kriteriji, ki jih nato logično združujemo na višjih ravneh do končne ravni kritičnosti računalniškega sistema. Za vsak kriterij so navedeni razlaga, pomen, uporaba in zaloga vrednosti, ki jih lahko zavzame. Prikazana so tudi odločitvena pravila in posamezne uteži, kako se nižji kriteriji združujejo v kriterije višjega reda.

Z modelom lahko v kratkem času ocenimo in primerjamo kritičnost skupine računalniških sistemov glede na regulativo, odkrijemo njihove prednosti in slabosti ter učinkovito odpravimo neskladnosti, najprej pri bolj in nato pri manj kritičnih sistemih, dokler ne zagotovimo popolne skladnosti.

Z modelom na podlagi analiz lažje in bolje načrtujemo investicijske projekte, izbiramo med možnimi dobavitelji, izobrazimo vse, vpletene v proces ocenjevanja, načrtujemo nabavo, izvedbo, validacijo in uporabo računalniškega sistema, ki je skladen z regulativo o elektronskih zapisih in elektronskih podpisih.

Na osnovi ocene in analize vzorčnih računalniških sistemov je model ustrezno validiran.

Ključne besede:

– računalniški sistem,
– analiza kritičnosti,
– elektronski zapis,
– elektronski podpis,
– farmacevtska industrija,
– večparametrski odločitveni model,
– odločitveni proces,
– DEXi.

Critical analysis of computer systems with respect to the electronic records and electronic signature regulations

The task presents a multi-attribute decision model for critical analysis of computer systems in pharmaceutical industry with respect to the electronic records and electronic signature regulations.

The basic attributes, defined on the basis of literature study, brainstorming and performed consultations, had been logically integrated into higher levels till the highest level of criticality of the computer system was reached. The description, the meaning, the use and the value domain are shown for each attribute. We also present the decision rules and weights for the integration of the lower attributes to the attributes of a higher level.

Our model enables short time evaluation and comparison of critical points in a group of computer systems with respect to the regulations and shows their strengths and weaknesses. It enables efficient correction of non-compliances, first with more critical systems and later with less critical ones, till full compliance is reached for all of them.

On the basis of the performed analysis, our model can be also used for more efficient investment planning, selection of suppliers and training of all individuals involved in the evaluation process. The presented model enables optimisation of purchasing, implementation, validation and use of computer systems that comply with the electronic records and electronic signature regulations.

On the basis of the evaluation and analysis of the selected sample computer systems, the model was appropriately validated.

Keywords:

- Computer System,
- Critical Analysis,
- Electronic Record,
- Electronic Signature,
- Pharmaceutical Industry
- Multi-attribute Decision Model,
- Decision Process,
- DEXi.

1. Uvod

1.1 Opredelitve

Elektronski zapisi in elektronski podpisi so se pojavili z uporabo računalniških sistemov. Namen regulative o elektronskih zapisih in podpisih je dvojen: postaviti kriterije za zagotovitev varnosti, celovitosti in pristnosti elektronskih zapisov v celotni dobi hranjenja ter zagotoviti, da so elektronski podpisi na elektronskih zapisih zaupni in zanesljivi (Title 21, Food and Drugs, Part 11, "Electronic Records; Electronic Signatures: Final Rule.", 1997). S tem elektronski podpisi postanejo enakovredni ročnim podpisom.

Računalniške sisteme in elektronske zapise srečamo v farmacevtski industriji praktično povsod. Mednje sodijo tako krmilniški sistemi (PLK[1] za vodenje naprav) kot programska oprema na ravni korporacije (programi za materialno poslovanje).

Računalniški sistemi, v katerih nastajajo elektronski zapisi in so uporabljeni elektronski podpisi, so lahko:

- krmilni sistemi in proizvodna oprema,
- laboratorijska oprema z nadzornim računalniškim sistemom,
- kontrolne naprave (kodni čitalci, števne naprave, linijske tehtnice),
- nadzorno-krmilni sistemi (SCADA[2]),
- samostojne programske rešitve za uporabo v proizvodnji (npr. program za tiskanje nalepk),
- mrežne programske rešitve za uporabo v proizvodnji,
- preglednice (excelovi izračuni),
- laboratorijski informacijski sistemi (LIMS[3]),
- proizvodni informacijski sistemi (MES[4]),
- informacijski sistemi za elektronsko dokumentacijo (EDMS[5]),
- informacijski sistemi za materialno poslovanje (MRP[6]).

Za zagotovitev skladnosti računalniških sistemov z nacionalnimi in mednarodnimi predpisi je potrebnih ogromno finančnih in človeških virov. Nujno je izpostaviti sisteme, ki so najbolj kritični. Z ustrezno razvrstitvijo sistemov namreč lahko zmanjšamo nepotrebne stroške. To storimo tako, da zagotovimo skladnost z regulativo pri sistemih, pri katerih je to res potrebno, in jo opustimo pri tistih, pri katerih to ni kritično.

Računalniške sisteme je treba razvrstiti oziroma jim določiti kritičnost glede na funkcijo, namen in uporabo.

Kriteriji za zagotavljanje skladnosti so določeni s predpisi. Poleg skladnosti je treba določiti še t. i. "GXP kritičnost"[7] računalniškega sistema. "GXP kritičnost" določata: vpliv sistema na izdelek in dostop do sistema.

---

[1] PLK - programabilni logični krmilniki
[2] SCADA - Supervisory Control And Data Acquisition
[3] LIMS - Laboratory Information Management System
[4] MES - Manufacturing Execution System
[5] EDMS - Electronic Document Management System
[6] MRP - Material Resource Planning
[7] GXP kritičnost - kritičnost sistema glede na dobre prakse (Good Practices): dobro proizvodno prakso (GMP), dobro laboratorijsko prakso (GLP) in dobro klinično prakso (GCP); označujemo jih s skupno kratico GXP.

Glede na veliko število kriterijev, medsebojnih povezav med njimi in različno pomembnost kriterijev se zdi primeren pristop večparametrskega odločanja. Večparametrsko odločanje temelji na razgradnji odločitvenega problema na manjše podprobleme. Variante razgradimo na posamezne parametre (kriterije ali atribute) in jih ločeno ocenimo glede na vsak parameter. Končno oceno variante dobimo z nekim postopkom združevanja. Tako izpeljana vrednost je potem osnova za izbiro najustreznejše variante (Bohanec, Rajkovič, 1995, str. 428).

1.2 Cilj in namen

Splošen cilj raziskave je ugotoviti vpliv različnih dejavnikov na kritičnost računalniškega sistema in predvideti aktivnosti, ki so potrebne za zagotavljanje skladnosti računalniških sistemov z regulativo o elektronskih zapisih in elektronskih podpisih.

Namen raziskave je:
- opredeliti kriterije (kvantitativne in kvalitativne), ki vplivajo na kritičnost računalniškega sistema;
- določiti funkcijo in vpliv kriterijev;
- izdelati večkriterijski odločitveni model za vrednotenje kritičnosti računalniških sistemov;
- določiti, kako uporabiti odločitveni model pri ugotavljanju kritičnosti računalniškega sistema;
- na podlagi uporabe odločitvenega modela določiti potrebne aktivnosti za zagotovitev ustreznosti posameznega računalniškega sistema.

1.3 Odločitvena skupina

V našem primeru smo se odločili za razvrstitev računalniških sistemov glede na kritičnost pri zagotavljanju skladnosti z regulativo.

Odločitveni problem je kritičen za ustrezno porazdelitev virov (finančnih in človeških). Odgovorni za odločitev so nosilci upravljanja kakovosti v podjetju. Odločitev pa ni pomembna samo za nosilce upravljanja kakovosti, ampak neposredno tudi za uporabnike sistemov.

V odločitveno skupino je torej treba poleg nosilcev zagotavljanja kakovosti vključiti tudi uporabnike in strokovnjake za informacijsko tehnologijo oziroma dobavitelje sistemov.

1.4 Metode dela

Večparametrske odločitvene modele uporabljamo za reševanje kompleksnih odločitvenih problemov. Problem najprej ustrezno opredelimo. Poznati moramo njegovo vsebino in na osnovi znanih dejstev zbrati kriterije, ki vplivajo na vedenje o nekem problemu. Zbranim kriterijem določimo zalogo vrednosti (vsa možna stanja). Tako določene kriterije nato združujemo v kriterije višjega reda, t. i. sestavljene ali agregirane kriterije. Združevanje nadaljujemo toliko časa, da dosežemo najvišji osnovni kriterij. Na osnovi tako izdelanega modela lahko za vsako posamezno varianto določamo vrednosti kriterijev in z agregiranimi kriteriji tudi vrednost celotnega modela (Bohanec, 1990, str. 2).

Za zbiranje podatkov o možnih kriterijih, ki jih lahko vključimo v neki model, in njihovi zalogi vrednosti, lahko uporabimo metode, kot so anketa, viharjenje možganov, študij literature ipd.

Na osnovi kriterijev, zbranih in opredeljenih v prvi fazi, določimo tudi zalogo vrednosti za posamezen kriterij. Običajno določimo negativno in pozitivno vrednost, vendar je priporočljivo, da opredelimo tudi srednjo vrednost. Težimo k temu, da kriterijev ni preveč. Primer za običajno zalogo vrednosti kriterijev je: slabo, povprečno, dobro ali 1, 3, 5 ipd. Merske lestvice so večinoma urejene od slabih (manj zaželenih) proti boljšim vrednostim. Pri metodi DEX (**D**ecision **EX**pert) to sicer ni nujno, je pa dobrodošlo, saj se uporablja v naslednji stopnji pri kontroli konsistentnosti odločitvenih pravil in lahko bistveno pospeši postopek zajemanja funkcij koristnosti (Bohanec, Rajkovič, 1995, str. 432).

Za izvedbo večparametrskega modela smo v magistrskem delu uporabili programski paket DEXi. Osnovne značilnosti programa DEXi, s katerim je bil izdelan prototip, so strukturiranje problema v drevesno strukturo, v kateri so vozlišča drevesa agregirani kriteriji, listi drevesa so bazični kriteriji. Za vse kriterije moramo podati zalogo vrednosti, za agregirane pa še funkcije koristnosti – pravila, kako se iz kombinacij vrednosti podrejenih kriterijev izračuna vrednost agregiranega kriterija. Delo s programom DEXi je zelo enostavno, omogoča pregledno sledenje procesa, vrednotenja posamezne opcije in s tem razumevanje odločitve ter različne "kaj-če" analize. Ob koncu lahko z njim ustvarimo poljubno obsežno dokumentacijo (Bitenc, 2000, str. 494).

1.5 Vsebina poglavij

V uvodu smo že podali osnovne opredelitve problema, cilj in namen raziskave, odločitveno skupino ter metode raziskovalnega dela za večparametrsko odločanje.

V naslednjem poglavju so navedeni bistveni elementi teorije odločanja. Podrobneje smo opisali večparametrsko odločanje in teoretično opredelili funkcijo koristnosti. Prikazali smo proces odločanja in upravljanja poslovnega sistema. V tem poglavju spoznamo tudi faze odločitvenega procesa: določitev problema in kriterijev, kako si pomagamo s funkcijo koristnosti, kako opišemo variante in jih ovrednotimo ter kako analiziramo in razložimo odločitev.

Tretje poglavje opisuje regulativo o elektronskih zapisih in elektronskih podpisih. Preučili smo tako nacionalno kot tudi mednarodno regulativo na tem področju. Predstavljen je pristop zagotavljanja skladnosti z regulativo pri obstoječih in novih sistemih.

V četrtem poglavju smo določili nabor kriterijev in njihovih vrednosti za naš odločitveni problem. Za zbiranje podatkov o možnih kriterijih, ki smo jih vključili v naš model, in njihovih zalogah vrednosti smo uporabili metodo ankete, viharjenja možganov in študija literature. V tem poglavju smo predstavili tudi drevo kriterijev, ki nam določa strukturo modela, in osnovna odločitvena pravila, kako združujemo posamezne nižje kriterije v višje, t. i. sestavljene kriterije.

V petem poglavju analiziramo in testiramo naš odločitveni model. Preverjamo delovanje samega modela sistema, ustreznost drevesne strukture in funkcij koristnosti ter opisujemo rezultate vrednotenja posameznih variant. V okviru vrednotenja variant na kratko opisujemo variante, jih analiziramo glede na naš model, predlagamo možne izboljšave variant in podamo končno oceno.

V zadnjem poglavju predlagamo možnosti za uporabo našega modela v praksi, razpravljamo o programskem orodju za obvladovanje številnih analiz, predvidevamo različne zahteve za različne tipe sistemov in razmišljamo o ekspertnem sistemu za lažjo izvedbo analiz sistemov ter določanje korektivnih ukrepov.

2. Teorija odločanja

Odločamo pravzaprav vsi, saj je odločanje v našem življenju prisotno vsak dan, naj gre za zasebno ali poslovno odločanje. Odločanje je del splošnega reševanja problemov in je pomembna umska aktivnost na vseh področjih človekovega delovanja (Bohanec, Rajkovič, 1995, str. 427).

Definicij odločanja je več. Navedimo nekaj najpogosteje uporabljanih:

"Odločanje je umska aktivnost, ki obsega opredelitev problema in izbiro ene izmed alternativnih smeri dejavnosti za njegovo rešitev" (Možina et al. 1994, str. 213).

"Odločanje pomeni v svoji najpreprostejši in splošni opredelitvi izbiro med možnostmi" (Rozman, Kovač, Koletnik, 1993, str. 25).

"Odločanje je izbira alternative iz množice možnih, ki najbolj zadovoljuje cilje okolja" (Efstathiou, Rajkovič, 1979, str. 326).

"Odločanje je izbiranje med alternativami, med različnimi usmeritvami v zaznanem položaju, ob zaznani zadevi - priložnosti, problemu" (Možina et al. 1994, str. 132).

Povzamemo lahko, da je odločanje umska aktivnost, pri kateri ob natančno določenih pogojih v okolju izberemo tisto izmed več možnih alternativ, ki najbolj zadovoljuje zastavljene cilje.

Odločitev pomeni izbrati med možnostmi. Ljudje nenehno izbiramo, ne da bi se tega zavedali. Preučevanje odločitev vodi k iskanju čimveč rešitev, omogoča možnost izbiranja med njimi; pri tem iščemo razloge za odločitev in preučujemo kriterije, na podlagi katerih se bomo odločali (Rozman, Kovač, Koletnik, 1993, str. 25).

Za proces odločanja so potrebni vsaj:
- potrebe in razlogi za odločitev,
- različne rešitve,
- kriteriji, na podlagi katerih izbiramo (Rozman, Kovač, Koletnik, 1993, str. 25).

Pri odločanju velikokrat nastanejo težave in napake. Problemi, ki se pojavijo pri odločanju, izvirajo iz velikega števila dejavnikov, ki vplivajo na odločitev, nepoznavanja posameznih variant, velike količine variant, nepoznavanja odločitvenega problema in ciljev odločitve,

sodelovanja več ljudi, ki imajo različna mnenja in cilje, omejenih sredstev in omejenega časa za sprejem odločitve (Clemen, 1996, str. 2-3; Bohanec, Rajkovič, 1995, str. 428).

S problemi odločanja se ukvarja vrsta znanstvenih disciplin in področij. Pri tem je najpomembnejše vprašanje, kako pomagati odločevalcu, da bo na sistematičen, organiziran in čim lažji način prišel do kakovostne odločitve. V ta namen je bilo razvitih mnogo metod in računalniških programov za podporo odločanju (angl. Decision Support Systems - DSS). Ena izmed metod je tudi metoda večparametrskega odločanja, ki je teoretično osnovana v okviru odločitvene teorije in teorije koristnosti, v praksi pa se uporablja za podporo pri zahtevnih odločitvenih problemih (Bohanec, Rajkovič, 1995, str. 428).

Primeri odločanja so zelo različni, od vsakodnevnih nakupov do strateškega načrtovanja, izbire poslovnih partnerjev ali kadrov, naložb ipd.

Za podporo odločanju se uporabljajo ekspertni sistemi, za katere lahko trdimo, da temeljijo na znanju, saj omogočajo shranjevanje ekspertnega in ustvarjanje novega znanja. Njihova značilnost sta zato preglednost in interdisciplinarnost zbranega znanja. Uporabni so pri odločevalskih nalogah, kot so sestavljanje projektne skupine, interdisciplinarno reševanje problemov, upravljanje in vodenje projektov (Pivec, Rajkovič, 1999, str. 449).

V tem magistrskem delu smo za analizo kritičnosti računalniških sistemov v farmacevtski industriji glede na regulativo o elektronskih podpisih in elektronskih zapisih uporabili lupino ekspertnega sistema (programsko orodje) DEXi, razvitega na Institutu Jožef Stefan v Ljubljani.

2.1 Večparametrsko odločanje

Večparametrsko odločanje temelji na razgradnji odločitvenega problema na manjše podprobleme. Variante razgradimo na posamezne parametre (kriterije ali atribute) in jih ločeno ocenimo glede na vsak parameter. Končno oceno variante dobimo s postopkom združevanja. Dobljena vrednost je osnova za izbiro najustreznejše variante (Bohanec, Rajkovič, 1995, str. 428).

V nadaljevanju so predstavljeni elementi odločitvenega procesa (Rajkovič, Bohanec, Bitenc, 2001, str. 15):

– množica variant $\boldsymbol{A} = \{a_1, a_2, a_3,...,a_n\}$; odvisno od problema je $\boldsymbol{A}$ lahko končna ali tudi neskončna množica;

– preferenčna relacija $\boldsymbol{P} \in \boldsymbol{A}\times\boldsymbol{A}$; *a* $\boldsymbol{P}$ *b* pomeni, da imamo varianto *a* rajši kot varianto *b*;

– funkcija koristnosti *F(a)*; funkcija *F(a)* izmeri stopnjo zaželenosti variante *a*, tako da za vsak par $a,b \in \boldsymbol{A}$ velja:

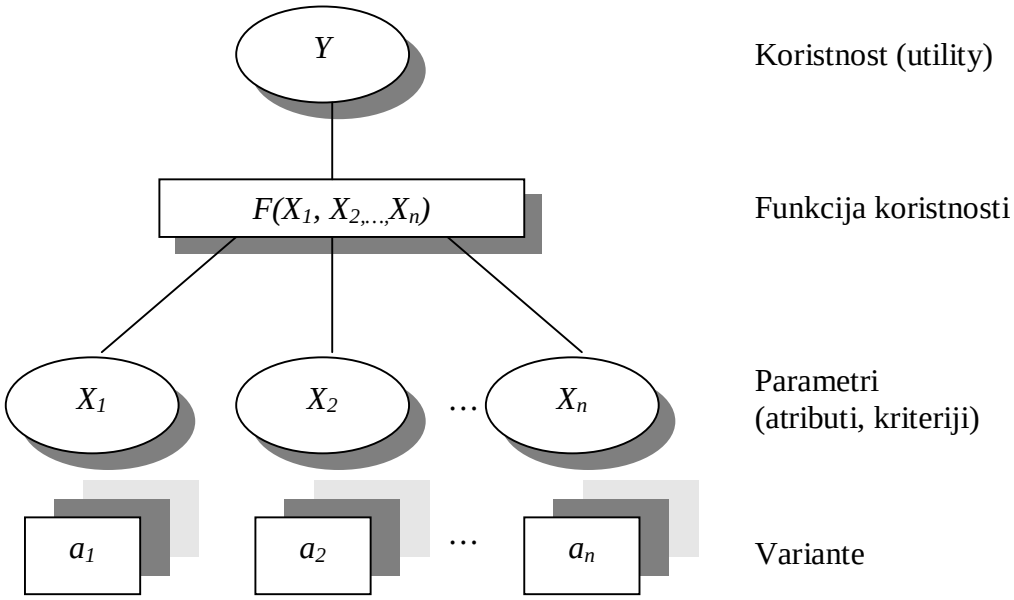
$$a\ P\ b \Leftrightarrow F(a) > F(b).$$

– racionalna odločitev je izbira variante *a**, tako da je

$$F(a^*) = \max_{a \in \boldsymbol{A}} F(a)$$

Relacija ***P*** uredi množico ***A*** po zaželenosti, ustreznosti oziroma koristnosti. Racionalna odločitev pomeni izbiro tiste variante $a \in \boldsymbol{A}$, ki je najbolj zaželena. Takih variant je lahko tudi več. V primeru neskončne množice ***A*** se v praksi omejimo na neko končno podmnožico.
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 odloča na podlagi izkušenj in znanja (Rajkovič, Bohanec, Bitenc, 2001, str. 24).

Slika 1: Večparametrski odločitveni model



Vir: Bohanec, Rajkovič, 1995, str. 428.

Pri večparametrskem odločanju imamo množico parametrov ***X:*** $x_1,x_2,x_3,...,x_n$ (Rajkovič, Bohanec, Bitenc, 2001, str. 17-18).

$$x_i : \boldsymbol{A} \rightarrow \boldsymbol{D}_{i,}$$

kjer so $\boldsymbol{D}_{i,}$ zaloge vrednosti posameznih parametrov.

Vsako varianto *a* iz množice ***A*** opišemo z zalogo (vektorjem) vrednosti parametrov:

$$a = x_1\,(a),\ x_2\,(a),\ x_3\,(a),\ldots\ ,\ x_n\,(a).$$

Preferenčna relacija P, ki uredi množico ***A*** po zaželenosti oziroma koristnosti, sedaj deluje med temi vektorji.

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

$$F(a)=F^*(x_1(a),\ x_2(a),\ x_3(a),\ \ldots,\ x_n(a)).$$

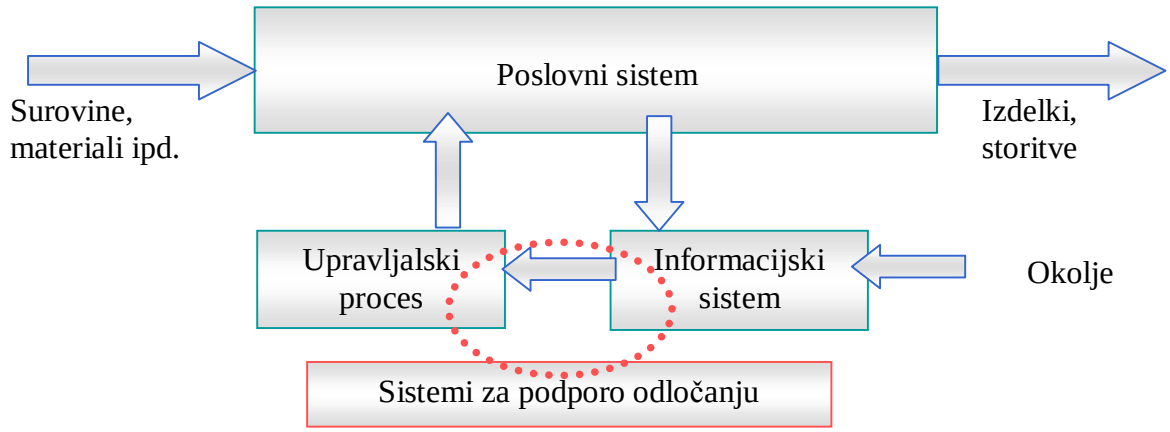
Opisani pristop je smiseln, če imamo opravka s kompleksnimi sistemi s številnimi vplivnimi dejavniki, ki so med seboj povezani. Pri večparametrskem odločanju najprej zgradimo hierarhični model, ki ga prikazuje slika 1. Vhod v model predstavljajo parametri, ki so spremenljivke in predstavljajo podprobleme glavnega odločitvenega problema. Urejeni so v hierarhično strukturo (drevo), ki ponazarja medsebojne odvisnosti med njimi. Glede na položaj v strukturi parametre ločimo na osnovne in izpeljane. Za vsak izpeljani parameter je določena funkcija koristnosti *F*, ki opredeljuje odvisnost tega parametra od njegovih neposrednih naslednikov v strukturi (Bohanec, Zupan, Rajkovič, 1997, str. 3) in tako predstavlja predpis, po katerem se vrednosti posameznih parametrov združujejo v spremenljivko *Y*, ki ponazarja končno oceno ali koristnost variante (Bohanec, Rajkovič, 1995, str. 428).

2.2 Proces odločanja

Proces odločanja in upravljanja je socio-tehnični proces, v katerem sta najpomembnejša odločevalec in problem. Odločevalec je oseba, ki postavi osnovne teze problema in ga razrešuje. Problem opredelimo kot oviro, ki onemogoča normalno delovanje poslovnega sistema in življenjski ciklus poslovnega sistema. Odločevalec mora dobro poznati problem in tehnologijo, ki jo uporablja kot pomoč pri delu. Informacije, ki jih upoštevamo pri odločanju, črpamo iz poslovnega sistema in njegove okolice. Na podlagi informacij lahko ustrezno vplivamo na upravljanje poslovnega sistema (Rajkovič, Bohanec, Bitenc, 2001, str. 11).

Človek se lahko zelo dobro odloča, če upošteva samo en pogled – en parameter. Mnogo težje se odločamo v primeru, ko imamo na voljo več parametrov. Pri takem odločanju potrebujemo pomoč, ki nam jo ponuja informacijska tehnologija. Slika 2 prikazuje opisani proces odločanja in upravljanja poslovnega sistema.

Slika 2: Proces odločanja in upravljanja poslovnega sistema.



Vir: Rajkovič, Bohanec, Bitenc, 2001, str. 11.

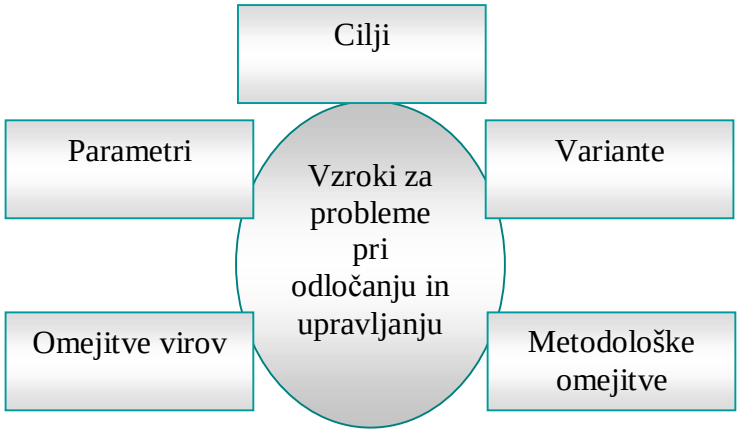
Poslovni sistem mora za svoj obstoj izpolnjevati tele cilje:

- izvajati kakovostne storitve in izdelovati kakovostne izdelke,
- upoštevati roke za izvedbe nalog,
- biti fleksibilen,
- zagotavljati finančno uspešnost opravljenih projektov in celotnega sistema,

– razvijati sistem v skladu z razvojem okolja.

Pri odločanju se srečamo s problemi, ki so lahko posledica različnih vzrokov in so shematsko prikazani na sliki 3.

Slika 3: Problemi pri odločanju in upravljanju



Vir: Rajkovič, Bohanec, Bitenc, 2001, str. 9-10.

Cilji so lahko zapleteni, nepopolni, negotovi, protislovni ali neusklajeni.

Če so variante slabo ali nepopolno opredeljene, nastanejo problemi. Odločitev otežuje tudi veliko število variant.

Parametri, ki vplivajo na odločitev, so lahko slabo določeni, neznani, spregledani ali težko merljivi (npr. uspešnost, sposobnost). Lahko imamo veliko število parametrov in se težko odločamo, saj jih moramo upoštevati glede na pomembnost.

Omejitve virov so lahko časovne, kadrovske in druge. Velikokrat se pojavijo zaradi pomanjkljivega poznavanja problema.

Metodološke omejitve se pojavijo pri ocenjevanju kakovosti odločitve.

Okolje se ves čas spreminja; s tem se spreminjajo tudi njegove potrebe in zahteve do poslovnega sistema. Le-ta se mora ves čas prilagajati potrebam okolja. Poleg avtomatizacije procesov je pomemben del tudi človek, ki s svojo intuicijo, domišljijo, kreativnostjo in fleksibilnostjo upravlja poslovni sistem (Rajkovič, Bohanec, Bitenc, 2001, str. 11).

2.3 Odločitveni proces

V odločitvenem procesu znanje sistematično zbiramo in urejamo. Zagotovil naj bi dovolj informacij za primerno odločitev, zmanjšal možnost, da bi kaj spregledali, pospešil in pocenil proces odločanja ter dvignil kakovost odločitve. Proces poteka po spodaj navedenih fazah, ki se lahko med seboj tudi prepletajo in ponavljajo (Bohanec, Rajkovič, 1995, str. 429-430):

– identifikacija problema,

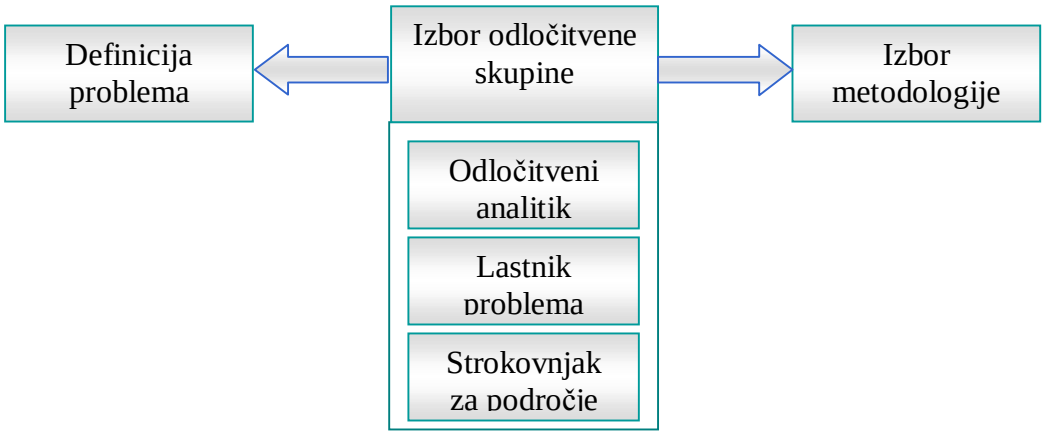
– identifikacija kriterijev,
– določitev funkcij koristnosti,
– opis variant,
– vrednotenje variant,
– analiza in razlaga,
– zaključek.

V nadaljevanju opisujemo bistvene značilnosti posameznih faz odločitvenega procesa.

2.3.1 Identifikacija problema

V prvi fazi odločitvenega procesa moramo problem predvsem opredeliti in ga opisati, zbrati informacije, ki so lahko pomembne za sprejemanje odločitve, ter izbrati ljudi, ki bodo pri odločitvi sodelovali. To so lastniki problema, strokovnjaki za to področje, analitiki in ostali, na katere odločitev vpliva (Zornada, Bohanec, Rajkovič, 2000, str. 519).

Slika 4: Identifikacija problema



Vir: Bohanec, Rajkovič, 1995, str. 430.

V okviru definicije problema opredelimo predmet odločanja, cilje, ki jih želimo doseči z odločitvijo, kakšnim zahtevam mora ustrezati izbrana varianta in težavnost problema. Pri izbiri metode določimo način, kako se bomo lotili problema in kakšne oziroma katere pripomočke bomo pri tem uporabili. Slika 4 prikazuje definicijo problema in izbiro metodologije, ki ju opredeli odločitvena skupina (Bohanec, Rajkovič, 1995, str. 430).

2.3.2 Identifikacija kriterijev

V tej fazi določimo kriterije in zasnujemo strukturo odločitvenega modela. Pomembno je, da pri tem ne spregledamo kriterijev, ki bistveno vplivajo na odločitev. Izpolniti je treba tudi zahteve, kot so strukturiranost, neredundantnost in merljivost kriterijev. Za vsak kriterij moramo podati pomen oziroma kratek opis. Kriterijem določimo tudi merske lestvice, to je zalogo vrednosti, ki jih lahko dobijo pri vrednotenju (Bohanec, Rajkovič, 1995, str. 430; Bohanec, Zupan, Rajkovič, 1997, str. 4).

2.3.3 Definicija funkcij koristnosti

Funkcije koristnosti opredeljujejo vpliv posameznega kriterija na celotno odločitev in izražajo odločitveno moč posameznega kriterija.

Funkcije koristnosti so lahko (Bohanec, Rajkovič, 1995, str. 430):

- utežena vsota,
- povprečja,
- funkcije zvezne logike,
- funkcije na osnovi Bayesovega pravila ali mehkih množic,
- odločitvena pravila.

Računalniško podprte metode omogočajo:

- neposredno analitično izražanje funkcij,
- parametrizacijo vnaprej pripravljenih funkcij,
- določitev funkcij po točkah,
- zajemanje v grafični obliki.

Pri oblikovanju te faze odločitvenega procesa določimo funkcije koristnosti in način njihovega določanja. Določimo, kateri kriteriji so pomembnejši in zakaj, določimo tudi morebitne izločilne kriterije (Bohanec, Rajkovič, 1995, str. 430).

2.3.4 Opis variant

Variante opišemo tako, da jim določimo vrednosti po posameznih kriterijih. To nam uspe po natančni preučitvi posamezne variante. Pri tem moramo biti pozorni na zanesljivost virov informacij o posamezni varianti in popolnost podatkov. Kadar se pri problemu srečamo z manj natančnimi podatki, nam nekatere metode omogočajo opis v obliki intervalov ali verjetnostnih porazdelitev. Pri oblikovanju te faze odločitvenega procesa kratko opišemo variante, med katerimi izbiramo, in način njihovega merjenja (morebitni viri) (Bohanec, Rajkovič, 1995, str. 430).

2.3.5 Vrednotenje variant

Končno oceno variant dobimo po vrednotenju na osnovi njihovega opisa po osnovnih kriterijih. Vrednotenje postavimo od listov do korena drevesa kriterijev, v skladu s strukturo drevesa in z določenimi funkcijami koristnosti.

Vrednost, ki jo na ta način dobimo v korenu drevesa, je končna ocena variante. Varianta z najvišjo oceno je praviloma najboljša. Rezultate vrednotenja variant primerno opišemo. Opredelimo, kako so bile ocenjene variante, katera med njimi je najboljša in zakaj ter primerjamo najboljšo varianto z nekaj najbolje ocenjenimi preostalimi variantami (Bohanec, Rajkovič, 1995, str. 430).

2.3.6 Analiza in razlaga odločitev

Dobljeno odločitev logično utemeljimo v fazi analize in razlage odločitev.

Ponovno preverimo in utemeljimo ustreznost vrednosti kriterijev ter funkcij koristnosti. Utemeljimo, zakaj je ocena takšna, kot je, in opredelimo kateri kriteriji so najbolj vplivali na rezultat. Ugotovimo, v čem se variante bistveno razlikujejo med seboj. Preverimo bistvene prednosti in pomanjkljivosti posameznih variant ter kakšna je občutljivost odločitve oziroma katere spremembe kriterijev vplivajo na končno oceno. Preverimo možnosti za izboljšanje posameznih variant in ugotovimo, kateri kriteriji vplivajo na bistveno poslabšanje ocen variant (Bohanec, Rajkovič, 1995, str. 430).

Na koncu opredelimo, ali je ocena v skladu s pričakovanji ali pa odstopa od pričakovanj in zakaj odstopa.

2.3.7 Zaključek

Pri oblikovanju zaključka odločitvenega procesa ugotovimo končni rezultat odločitve. Določimo in ustrezno utemeljimo najboljšo varianto. Preverimo, ali so bili doseženi cilji odločitvenega procesa oziroma kaj bi bilo še treba ukreniti, da jih dosežemo. Izpostavimo morebitne napotke za uresničitev končne odločitve. Na primer, pri izbrani varianti opišemo kritične lastnosti, ki jim je treba pri uresničitvi posvetiti posebno pozornost. Ko smo utemeljili vse navedeno, smo prišli do končne rešitve odločitvenega procesa (Bohanec, Rajkovič, 1995, str. 430).

Pri tem nam lahko zelo pomagajo računalniška orodja, ki so prirejena tako, da nam omogočajo natančnejšo analizo in sistematičnost ocenjevanja ter s tem kakovostnejšo in bolj utemeljeno odločitev. Pri odločanju so torej računalniška orodja, ki podpirajo odločitveni proces, nepogrešljiva.

2.4 Programsko orodje DEXi

DEXi (**D**ecision **EX**pert) je lupina ekspertnega sistema za večparametrsko odločanje. Glavni namen tega programskega orodja je podpora odločevalcu pri sprejemanju kompleksnih večparametrskih odločitev, kot so izbira kandidatov, nakup hiše, izbira tehnologije, ocena delovanja kompleksnih sistemov in še mnogo drugih. Takšne odločitve se v vsakdanjem življenju pogosto pojavljajo; pri izbiri imamo na voljo mnogo možnosti, ki imajo svoje dobre in slabe lastnosti, zato jih je treba oceniti, analizirati in primerjati med seboj (Bohanec, 1991, str. 1).

Programsko orodje **DEXi** podpira teorijo, ki temelji na večparametrskem odločanju, pri katerem je v procesu odločanja poudarjena pomembnost odločevalca. Orodje odločevalca spodbuja k učenju in raziskovanju problema odločanja. Odločevalec raziskuje problem z določanjem kriterijev, ki so pomembni, in njihovih vrednosti. Namesto matematičnih formul, ki so običajno vključene v program za izračun različnih možnosti, programsko orodje izlušči znanje o odločanju iz samega uporabnika (Rajkovič et al., 1999, str. 387).

Znanje oblikujemo v preprostih pravilih, ki jim rečemo osnovna odločitvena pravila, na primer:

Če je cena visoka in kakovost slaba,
potem ta možnost ni sprejemljiva.

Takšna metoda zapisa znanja je uporabljena v mnogih ekspertnih sistemih in programskih orodjih v umetni inteligenci. Ob prenosu v programsko orodje DEXi se ta pristop izkaže za zelo fleksibilnega, saj program omogoča uporabniku poglobitev v proces odločanja (Bohanec, 1991, str. 1).

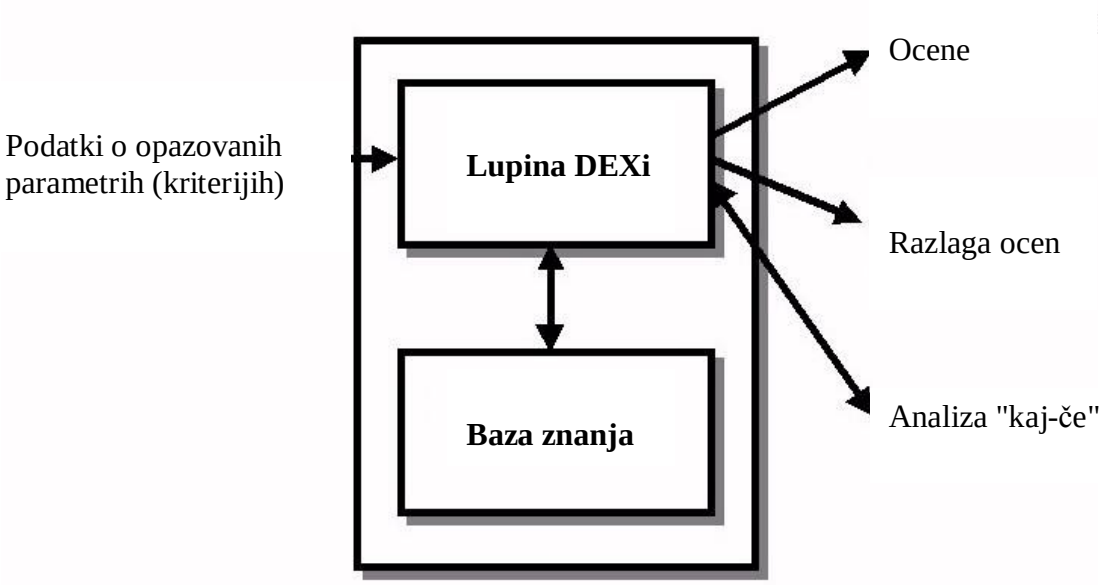
2.4.1 Struktura orodja DEXi

DEXi je v osnovi sestavljen iz dveh delov (Rajkovič et al., 1999, str. 387):

1. *pridobivanja in urejanja znanja*
   Uporabniku pomaga pri oblikovanju drevesa kriterijev in pravil odločanja za obravnavani problem; dejansko je to proces strukturiranja odločitvenega problema in izražanja preferenc, pri čemer se konsistentnost podanih odločitvenih pravil tudi sproti računalniško preverja;

2. *ocene in analize variant*
   Pridobljeno bazo znanja se uporabi za oceno in analizo variant.

Slika 5: Shematični prikaz strukture sistema za ocenjevanje



Vir: Rajkovič et al., 1999, str. 387.

Na začetku je vsaka varianta opisana z vrednostmi kriterijev, ki predstavljajo liste drevesa. DEXi vsako varianto oceni v skladu z bazo znanja, to je drevesom kriterijev in odločitvenimi pravili. Za vsakovarianto tako dobimo oceno primernosti oziroma

ustreznosti. Temu postopku lahko sledi analiza rezultatov, ki je sestavljena iz ene ali več naslednjih aktivnosti (Rajkovič et al., 1999, str. 387-388):

– *razlage ocene*
  DEXi je sposoben razložiti, kako je bila na osnovi kriterijskih vrednosti in uporabljenih odločitvenih pravil pridobljena vsaka posamezna ocena.

– *analize tipa "kaj-če"*
  Izvedena je interaktivno s spremembo opisa variant, njihovo ponovno ocenitvijo in primerjavo dobljenih rezultatov s prvotnimi (referenčnimi) rezultati.

– *selektivne razlage variant*
  DEXi najde tista podkriterijska drevesa, ki odražajo najmočnejše ali najbolj šibke značilnosti posamezne variante, in poroča o njih, s čimer izluščimo samo najbistvenejše informacije.

Opisana struktura programskega orodja DEXi je shematsko prikazana na sliki 5.

Če povzamemo: DEXi nam je v pomoč pri procesu ocenjevanja in odločanja na osnovi modeliranja preferenčnega znanja. S tem pripomoremo k preglednosti odločitvenega postopka. Odločevalec ima na razpolago razlago rezultatov, tako ocenjevanja kot tudi celotnega poteka postopka. Predstavitev znanja je zasnovana na združitvi pristopa večkriterijskega odločanja z ekspertnim sistemom, v DEXi sta vključena tudi strojno učenje in mehka logika (Rajkovič et al., 1999, str. 391; Bohanec, Rajkovič, 1999, str. 73). Uporabniku je s tem omogočeno prijazno in lažje odločanje, saj je znanje o odločanju izraženo preprosto in neposredno z besedami, pravili in hierarhično urejenimi kriteriji.

2.4.2 Faze odločanja s programskim orodjem DEXi

Ob uporabi orodja DEXi gre odločevalec skozi različne faze. Ob tem ima možnost, da se čez nekaj časa, ko je njegovo znanje večje, vrača v prejšnje odločitvene faze in jih spreminja ali jim kaj doda.

Faza 1 – Identifikacija problema

Predvideva se, da je uporabnik že določil problem, ki ga je treba rešiti, npr. nakup avtomobila, kateri investicijski scenarij uporabiti, kako analizirati kritičnost računalniških sistemov ipd. Najprej je treba ugotoviti nekaj najpomembnejših kriterijev problema. Za kritičnost računalniškega sistema, na primer, sta to lahko: "skladnost z regulativo" in "GXP kritičnost sistema".

Pomembno je, da v tej fazi določimo samo najbolj kritične kriterije in se ne obremenjujemo s podrobno listo kriterijev (Bohanec, 1991, str. 4).

Faza 2 – Kriteriji in njihova struktura

Začetne kriterije vnesemo v DEXi. Vsakega od njih je treba nekako opisati, bodisi z besedami bodisi številkami, ki primerno opišejo občutljivost spremenljivke. Tipične vrednosti so lahko: slabo, delno, dobro. Kadar je primerno, spremenljivke lahko opišemo samo s številkami, npr. število avtomobilskih vrat. Spremenljivke strukturiramo v drevo.

DEXi omogoča fleksibilno orodje za izdelavo drevesne strukture (Bohanec, 1991, str. 5).

Faza 3 – Izpeljava pravil

Ta in naslednja faza se lahko večkrat ponavljata in dopolnjujeta, ko uporabnik napreduje skozi fazo učenja. Odločevalec mora v tej fazi postaviti "če–potem" (IF-THEN) pravila (osnovna odločitvena pravila), s katerimi določi, kako se kombinacije kriterijev združujejo.

Programsko orodje že samo ponudi vse možnosti kombinacij kriterijev v tabeli, tako da uporabnik vnese samo končne vrednosti izbranih kombinacij. Še več, na podlagi že vnesenih pravil program sam predlaga ostala pravila. Sistem tudi ves čas nadzoruje konsistentnost pravil. Vse to omogoča hitro in zanesljivo izpeljavo pravil oziroma funkcij koristnosti (Bohanec, 1991, str. 5).

Faza 4 – Opis in ocena variant

Po določitvi kriterijev in izpeljavi pravil določimo vrednosti kriterijev za posamezne variante. Ko so vrednosti vnesene, DEXi oceni variante na podlagi pravil (funkcij koristnosti) in jih razvrsti. V tej fazi se lahko uporabnik zave, da je v prvotnih fazah spregledal kak kriterij in pravilo. Program mu omogoča, da se vrača nazaj v fazo 2 ali 3 in ju dopolnjuje.

Programsko orodje v tej fazi ponuja tudi nekaj funkcij za analizo variant. Vrednotenje vseh variant je prikazano v obliki tabele. Na podlagi vnesenih osnovnih kriterijev s pomočjo funkcij koristnosti ("če-potem" pravil) program določi sestavljene kriterije. Variante lahko analiziramo tudi pri nepopolnih podatkih. Poleg tega je omogočena grafična primerjava med variantami in med kriteriji. Celotno analizo lahko prikažemo z izpisom različnih formatov in elementov poročila (Bohanec, 1991, str. 6).

2.4.3 Uporaba

Programski paket DEXi so praktično uporabili pri mnogih kompleksnih odločitvenih problemih, kot so:

- ocena računalniških sistemov za podjetja in organizacije,
- izbira različnih programskih paketov za podjetja in šole,
- izbira/ocena poslovnih partnerjev,
- izbira ekspertne skupine,
- izbira zaposlitve in kadrov,
- svetovanje otrokom pri izbiri športa,
- ocena uspešnosti poslovnih enot,
- ocena investicijskih scenarijev.

V nadaljevanju bomo uporabili programski paket DEXi za izvedbo večparametrskega odločitvenega modela, s katerim bomo analizirali kritičnost računalniških sistemov glede na regulativo o elektronskih zapisih in elektronskih podpisih.

Problema se bomo lotili z orodjem DEXi po določenih fazah odločanja (*Faza 1 - Faza 4*).

3. Regulativa o elektronskih zapisih in elektronskih podpisih

Pri vzpostavljanju in izvajanju proizvodnih procesov ter kontrolnih postopkov je treba v farmacevtski industriji slediti splošnim standardom in predpisom za proizvajalce zdravil: od smernic dobre proizvodne prakse, ki jih je leta 1968 pripravila Svetovna zdravstvena organizacija, in tovrstnega predpisa ameriške Uprave za hrano in zdravila (FDA[8]) iz leta 1978 do pravil, ki jih je leta 1983 sprejela skupina srednjeevropskih držav ter pravil, ki od leta 1989 veljajo v Evropski skupnosti.

Poleg preverjanja kakovosti vhodnih materialov in končnih izdelkov zahtevajo vsa našteta pravila reden nadzor proizvodnih postopkov ter nadzor distribucije vsake serije izdelka. Bistven element zagotavljanja kakovosti torej vzpostavimo in izvajamo že z upoštevanjem pravil dobre proizvodne, laboratorijske in klinične prakse.

V farmacevtski industriji uporabljajo različne vrste računalniških sistemov, naštete že v uvodu, in sicer so to:

- krmilni sistemi in proizvodna oprema,
- laboratorijska oprema z nadzornim računalniškim sistemom,
- kontrolne naprave (kodni čitalci, številne naprave, linijske tehtnice),
- nadzorno-krmilni sistemi,
- samostojne programske rešitve za uporabo v proizvodnji,
- mrežne programske rešitve za uporabo v proizvodnji,
- preglednice,
- laboratorijski informacijski sistemi,
- proizvodni informacijski sistemi,
- informacijski sistemi za elektronsko dokumentacijo,
- informacijski sistemi za materialno poslovanje.

V vseh teh računalniških sistemih se lahko uporabljajo elektronski zapisi in podpisi.

Medtem ko je v slovenski zakonodaji elektronski podpis določen predvsem v povezavi z elektronskim poslovanjem na daljavo, pa so v mednarodni regulativi določeni tudi kriteriji za elektronske podpise in elektronske zapise, s katerimi se srečujemo tudi pri zgoraj naštetih industrijskih računalniških sistemih.

Predpisi o elektronskih zapisih in podpisih imajo dvojen namen: postaviti kriterije za zagotovitev varnosti, celovitosti in pristnosti elektronskih zapisov v celotni dobi njihovega hranjenja ter zagotoviti, da so elektronski podpisi na elektronskih zapisih zaupni in zanesljivi. Z izpolnjevanjem teh predpisov postanejo elektronski podpisi enakovredni ročnim podpisom (Title 21, Food and Drugs, Part 11, "Electronic Records; Electronic Signatures: Final Rule.", 1997).

Elektronski zapisi so podatki, ki so oblikovani ali shranjeni na elektronski način. To je lahko katerakoli kombinacija besedila, slike ali zvočnega zapisa, ki je ustvarjena, se spreminja, vzdržuje, shranjuje ali pošilja z računalniškim sistemom (Title 21, Food and Drugs, Part 11, "Electronic Records; Electronic Signatures: Final Rule.", 1997).

[8]FDA – Food and Drug Administration

Elektronski podpis je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki in je namenjen preverjanju pristnosti teh podatkov ter identifikaciji podpisnika (Zakon o elektronskem poslovanju in elektronskem podpisu, 2000).

Elektronski podpis je varen, ko izpolnjuje naslednje zahteve (Zakon o elektronskem poslovanju in elektronskem podpisu, 2000):

- povezan je izključno s podpisnikom;
- iz njega je mogoče podpisnika zanesljivo ugotoviti;
- ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki jih nadzoruje izključno podpisnik;
- s podatki, na katere se nanaša, je povezan tako, da je opazna vsaka poznejša sprememba teh podatkov ali povezave z njimi.

Prikaz elektronskega podpisa mora vsebovati najmanj (Title 21, Food and Drugs, Part 11, "Electronic Records; Electronic Signatures: Final Rule.", 1997):

- tiskano ime posameznika,
- časovni žig (datum in čas) podpisa,
- namen podpisa (pregled, odobritev ipd.).

3.1 Slovenska regulativa

Regulativo na področju elektronskih podpisov in elektronskega poslovanja odrejata v Sloveniji Zakon o elektronskem poslovanju in elektronskem podpisu, objavljen v Uradnem listu RS, št.: 57/2000, 23. 6. 2000, in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, Uradni list RS, št. 77/2000 in 2/2001.

Zakon ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki na daljavo z uporabo informacijske in komunikacijske tehnologije, ter uporabo elektronskega podpisa v pravnem prometu. Predpisuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih, če z zakonom ni določeno drugače (Zakon o elektronskem poslovanju in elektronskem podpisu, 2000).

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje določa (Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, 2001):

- kriterije, ki se uporabljajo za presojanje izpolnjevanja zahtev za delovanje overiteljev, ki izdajajo kvalificirana potrdila;
- podrobnejšo vsebino notranjih pravil overiteljev, ki izdajajo kvalificirana potrdila;
- podrobnejše tehnične pogoje za elektronsko podpisovanje in preverjanje varnih elektronskih podpisov;
- časovno veljavnost kvalificiranih potrdil;
- podrobnejše pogoje za uporabo varnih časovnih žigov;
- vrsto in uporabo označbe akreditiranih overiteljev;
- pogoje za elektronsko poslovanje v javni upravi.

3.2 Mednarodna regulativa

Priporočila za farmacevtske proizvajalce v Evropski skupnosti določajo, kako je treba vzdrževati sistema dokumentacije. Dobra dokumentacija je bistveni del zagotavljanja kakovosti. Jasno napisana dokumentacija preprečuje napake, ki bi nastale pri ustnem komuniciranju, in omogoča sledenje zgodovini proizvodne serije. Specifikacije, proizvodni postopki, navodila in zapisi morajo biti brez napak in v pisni obliki. Čitljivost dokumentov je izredno pomembna (The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practices, 1997).

Podatki so lahko zapisani s sistemi za elektronsko procesiranje podatkov, vendar morajo ti izpolnjevati določene kriterije za zaščito (Good Practices for Computerised Systems in Regulated "GXP" Environments, 2002), in sicer:

- dostop je dovoljen samo pooblaščenim uporabnikom,
- zahteva se uporaba gesel,
- izvedena je izdelava varnostnih kopij,
- neodvisno se preverja kritične podatke,
- zagotovljeno je varno hranjenje podatkov za predviden čas.

Takšni sistemi morajo izpolnjevati še dve zahtevi (Good Practices for Computerised Systems in Regulated "GXP" Environments, 2002):

- sistem mora biti validiran (osnovna zahteva),
- zgodovina dogodkov mora biti zanesljivo dokumentirana ter ustrezno zaščitena.

Za računalniške sisteme, ki delujejo v okolju dobrih proizvodnih praks, t. i. "GXP[9] računalniške sisteme", ki elektronsko proizvajajo regulatorne zapise, dovoljujejo zunanji dostop ali sprejemanje glavnih odločitev in akcij preko elektronskih vmesnikov, so postavljene dodatne varnostne zahteve. V glavnem so določene z mednarodnimi pobudami za vzpostavitev elektronskega poslovanja in zahtevami pravila, imenovanega "21CFR Part11", ki ga je pripravila ameriška Uprava za hrano in zdravila (Good Practices for Computerised Systems in Regulated "GXP" Environments, 2002).

Namen priporočil za dobro proizvodno prakso ni ponavljanje zahtev za elektronsko poslovanje; kadar podjetja dostopajo do "GXP računalniških sistemov" preko odprtih sistemov, morajo biti ustrezna zaščita, nadzor in validacija dokumentirani ter na voljo inšpektorjem, ki preverjajo dobre prakse (Good Practices for Computerised Systems in Regulated "GXP" Environments, 2002).

3.2.1 Evropska regulativa

Evropska priporočila za računalniške sisteme določajo način njihove uvedbe v proizvodni proces, ustreznost osebja, obseg validacije in način izvedbe računalniškega sistema. V nadaljevanju so predstavljeni bistveni predpisi s tega področja.

[9]GXP – To je kratica za poimenovanje skupine dobrih praks: dobro proizvodno prakso (GMP), dobro laboratorijsko prakso (GLP) in dobro klinično prakso. (GCP).

3.2.1.1 Princip

Zaradi uvedbe računalniškega sistema v proizvodne sisteme, tudi v distribucijo, skladiščenje in kontrolo kakovosti, se nadzorovanje procesa ne spremeni. Kadar računalniški sistem nadomesti ročno operacijo, to ne sme povzročiti poslabšanja kakovosti izdelka ali zmanjšati zagotavljanje kakovosti v proizvodnem procesu (The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practices, 1997).

3.2.1.2 Osebje

Pomembno je, da so ljudje na odgovornih delovnih mestih ustrezno izobraženi, da lahko uporabljajo računalniški sistem v okviru svojih pristojnosti. Treba je zagotoviti tudi strokovnjake, ki bodo znali svetovati pri načrtovanju, validaciji in delovanju računalniškega sistema (The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practices, 1997).

3.2.1.3 Validacija

Obseg potrebne validacije sistema je odvisen od številnih dejavnikov; upoštevati je treba vrsto validacije (prospektivna[10] ali retrospektivna[11]) in prisotnost novih elementov v sistemu. Življenjski cikel računalniškega sistema je sestavljen iz več faz: načrtovanja, specificiranja, programiranja, testiranja, prevzema, dokumentiranja, uporabe, nadzora in spreminjanja sistema; validirati je treba celoten cikel. (The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practices, 1997).

3.2.1.4 Izvedba sistema

Sistem naj bo izveden v okolju, v katerem se ne morejo pojaviti nepredvideni dejavniki, ki bi lahko vplivali nanj. Priporočila za izvedbo so (The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practices, 1997):

- Pripraviti je treba opis sistema, ga opremiti s primernimi diagrami in sproti dopolnjevati. Opisani naj bodo obseg in namen sistema, varnostni kriteriji, način delovanja in povezave z drugimi sistemi ter procesi.
- Programska oprema je kritični del računalniškega sistema. Uporabnik programske opreme mora na primeren način zagotoviti, da je bila programska oprema izdelana v skladu s sistemom za zagotavljanje kakovosti.
- Sistem naj ima, kjer je to primerno, vgrajene mehanizme za preverjanje ustreznosti vnosov in procesiranje podatkov.
- Preden računalniški sistem uvedemo, naj bo le-ta dobro testiran in potrjen kot primeren za uporabo. Če s sistemom nadomeščamo ročni način dela, naj kot del testiranja določen čas oba procesa potekata vzporedno.

[10] Prospektivna validacija – Validacija, ki se izvaja v celotnem življenjskem ciklu sistema in zajema vse faze validacije, od uporabniških zahtev do specifikacij, izvedbe sistema, kvalifikacij (DQ, IQ, OQ, PQ) in končne validacije procesa. Običajno se izvaja pri novih sistemih.

[11] Retrospektivna validacija – Validacija, ki se izvede na obstoječi opremi ali sistemu (za nazaj). Običajno za takšne sisteme ni uporabniških zahtev in specifikacij. Takšna validacija obsega določitev glavnih komponent in funkcionalnosti sistema ter potrdi ustreznost instalacije in delovanja glede na predvidene parametre.

- Pravico do vnosa in spreminjanja podatkov naj imajo samo pooblaščeni uporabniki. Vnos podatkov nepooblaščenim osebam je treba preprečiti z metodami, kot so: uporaba ključev, kartic in omejen dostop. Določiti je treba postopek za izdajo, preklic in spremembo avtorizacij za vnos podatkov ter način za spreminjanje osebnih gesel. Poskuse nepooblaščenih dostopov do sistema je treba primerno spremljati.
- Kadar se kritični podatki (npr. teža in kontrolna številka pri pripravi surovin) ročno vnašajo, je treba dodatno preveriti točnost zapisa. Dodatno preverjanje lahko izvede bodisi druga oseba bodisi validirani elektronski sistem.
- Sistem naj zapiše identiteto oseb, ki vnašajo in potrjujejo kritične podatke. Spreminjanje vnesenih podatkov naj bo dovoljeno le pooblaščenim osebam. Vsaka sprememba kritičnih podatkov naj bo avtorizirana, podati je treba tudi razlog za spremembo. Smiselna je uporaba zgodovine dogodkov za vse zapise na sistemu.
- Sprememba sistema ali programske opreme se lahko izvede samo v skladu z določenimi postopki, ki vključujejo preverjanje, odobritev, izvedbo in validacijo spremembe.
- Obstajati mora možnost za izpis vseh elektronsko shranjenih podatkov, kar omogoča pregled kakovosti sistema.
- Podatki naj bodo pred naključnimi ali namernimi spremembam zavarovani fizično ali z elektronskimi ukrepi. Dostopnost, točnost in trajnost shranjenih podatkov je treba preveriti. Ob spremembah računalniške ali programske opreme naj pogostost preverjanja zapisov ustreza mediju, na katerem bodo zapisi shranjeni.
- Podatki naj bodo varovani z varnostnimi kopijami, ki naj se shranjujejo v rednih razmakih. Varnostne kopije naj bodo shranjene na ločeni in varni lokaciji, dokler je to potrebno.
- V primeru izpada sistema naj bodo na voljo primerne alternative za izvajanje procesa. Čas, potreben za pripravo alternativnih načinov izvajanja procesov, naj bo odvisen od tega, kako nujna je uporaba sistema.
- Postopki ob izpadu sistema morajo biti vnaprej določeni in validirani. Vsi izpadi in korektivni postopki morajo biti evidentirani.
- Vzpostavljena naj bo procedura za evidentiranje in analizo napak ter izvedbo korektivnih ukrepov.
- Če storitve na računalniških sistemih izvaja zunanji izvajalec, naj obstaja formalni dogovor z jasno izjavo glede odgovornosti zunanjega izvajalca.
- Kadar računalniški sistem dovoljuje sproščanje serij za prodajo ali dobavo, naj sistem omogoča sprostitev serij le pooblaščenemu osebju in naj jasno identificira ter evidentira osebo, ki je sprostila serijo.

3.2.2 Ameriška regulativa

Z vse večjo uporabo informacijske tehnologije in računalniških sistemov v vseh fazah proizvodnje se proizvodni procesi avtomatizirajo. Ključne odločitve in postopki se izvajajo preko elektronskih vmesnikov in zapisi, ki so zahtevani s predpisi, nastajajo elektronsko.

Tveganje za poneverjanje, napačno tolmačenje (interpretacijo) in spremembo brez dokaza je pri elektronskih zapisih veliko večje kot pri ročnih zapisih na papirju. Zato moramo elektronske zapise nadzorovati.

Ameriška Uprava za hrano in zdravila (FDA) je uporabo elektronskih zapisov in elektronskih podpisov opredelila v pravilu "21CFR Part11". Z njim je dovolila, da v proizvodni in regulatorni dokumentaciji ročne zapise in podpise zamenjajo elektronski

zapisi in podpisi, s tem pa je omogočila napredek tehnologije (Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000).

V okolju, kjer se zahtevajo dobre prakse, to pomeni odobritev uporabe proizvodnih informacijskih sistemov, laboratorijskih informacijskih sistemov ter s tem elektronskih zapisov in poročil. Naslednja očitna prednost uporabe elektronskih zapisov in podpisov je možnost elektronske registracije pri razvoju novih zdravil (Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000). Elektronska registracija pomeni, da vso potrebno dokumentacijo za registracijo zdravila na nekem trgu predložimo lahko v elektronski obliki namesto papirni.

Kljub temu, da pravilu "21CFR Part11" priznavajo dolgoročne prednosti in da omogoča tehnološki napredek, se farmacevtska industrija sedaj ukvarja predvsem s tem, kako novosti, ki jih prinaša, uvesti v sedanje sisteme in trenutne projekte. Zato je nujno potrebno pravilo ustrezno razumeti, ga znati tolmačiti in praktično izkoristiti v proizvodnih in laboratorijskih računalniških sistemih (Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000).

Pri proizvodnih in laboratorijskih programskih rešitvah se v glavnem srečujemo z zaprtimi sistemi, ki uporabljajo gesla in druge nebiometrične načine zaščite. Za zaprte sisteme je značilno, da dostop do sistema nadzirajo tiste osebe, ki so odgovorne za vsebino elektronskih zapisov na sistemu (Guidance to Industry on Electronic Records, 2001).

V nadaljevanju so predstavljene zahteve, določene v pravilu "21CFR Part11". Zahteve za nadzor elektronskih zapisov in elektronskih podpisov obsegajo proceduralne zahteve in tehnične funkcionalnosti sistemov.

3.2.2.1 Zahteve za zaprte sisteme

Kadar elektronski zapisi nastajajo, se spreminjajo, vzdržujejo ali prenašajo v zaprtih sistemih, je treba vzpostaviti postopke in mehanizme, s katerimi bomo zagotovili njihovo pristnost, celovitost in, kjer je to primerno, zaupnost. Podpisnik zapisa naj ne bi imel možnosti, da bi podpisan zapis preklical kot nepristen.

S takšnimi procedurami in mehanizmi naj bi zagotovili (Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule.", 1997):

- validacijo sistemov za zagotovitev točnosti, zanesljivosti, stalnega delovanja in zmožnosti prepoznavanja neveljavnih vnosov ali spremenjenih zapisov;
- zmožnost narediti "točne in popolne" kopije zapisov, v elektronski obliki in obliki izpisa, ki bo primeren za inšpekcijo, pregled in kopiranje;
- zaščito zapisov, ki bo omogočala primerno hitro pridobitev točnega zapisa celoten čas hranjenja;
- omejitev dostopa do sistema oziroma dostop samo pooblaščenim uporabnikom;
- varno zgodovino dogodkov, ki jo računalnik ustvari avtomatsko, neodvisno od operaterjev in vsebuje časovni žig; s tem se neodvisno evidentirajo vsi operaterjevi vnosi in dejanja, s katerimi spreminja, ustvarja ali briše elektronske zapise. Spremembe zapisov naj ne bi prikrile prvotne informacije. Takšna zgodovina dogodkov naj se hrani vsaj toliko časa, kot se hrani elektronski zapis, na katerega se zgodovina nanaša, in naj bo na voljo za pregled in kopiranje;

- ustrezno zaporedje operacij in dogodkov procesa;
- ustrezno avtorizacijo, ki dovoljuje, da lahko samo pooblaščeni uporabniki uporabijo sistem, elektronsko podpišejo zapis, dostopajo do operacije ali vhodno-izhodne naprave računalniškega sistema, spremenijo zapis ali izvedejo neko operacijo;
- izvajanje kontrole ustreznosti naprav za zagotovitev ustreznosti izvora vhodnih podatkov;
- da bodo imele osebe, ki razvijajo, vzdržujejo ali uporabljajo sistem z elektronskimi zapisi in elektronskimi podpisi primerno izobrazbo in izkušnje za izvajanje dodeljenih nalog;
- da bodo vzpostavljene in upoštevane procedure, po katerih bo posameznik popolnoma odgovoren za aktivnosti, ki jih bo potrdil z elektronskim podpisom in s katerimi bomo preprečili ponarejanje zapisov in podpisov;
- primeren nadzor nad sistemsko dokumentacijo, ki naj vključuje:
  a) primeren nadzor distribucije, dostopa in uporabe dokumentacije o uporabi in vzdrževanju sistema;
  b) procedure za revizijo in kontrolo sprememb, s katerimi bomo zagotovili zgodovino dogodkov, v kateri bo dokumentirano zaporedje razvoja in sprememb sistemske dokumentacije.

3.2.2.2 Zahteve za odprte sisteme

Pri odprtih sistemih, pri katerih dostopa do sistema ne nadzorujejo osebe, ki so odgovorne za vsebino elektronskih zapisov na sistemu, je treba zagotoviti pristnost, celovitost in, če je primerno, zaupnost elektronskih zapisov od njihovega nastanka do prejema.

Poleg vseh že navedenih funkcionalnosti morajo takšni sistemi izpolnjevati še dodatne zahteve, npr. enkripcijo dokumentov in uporabo primernih standardov za digitalni podpis, s katerimi zagotovimo pristnost, celovitost in zaupnost. Primera takšnih standardov sta enkripcijski standard RSA[12] in NIST[13]-ov DSS[14] (Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule.", 1997).

3.2.2.3 Prikaz elektronskega podpisa

Podpisani elektronski zapis naj vsebuje jasne informacije, in sicer: (Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule.", 1997):

- tiskano ime in priimek podpisnika;
- datum in čas, ko je bil zapis podpisan;
- namen podpisa (npr. izdelava, pregled, odobritev).

Nadzor naštetih informacij o elektronskem podpisu mora biti enak kot za elektronske zapise in naj bo del zapisa pri elektronskem prikazu ali izpisu na papir.

[12]RSA - Rivest Shamir Adleman – enkripcijski standard, poimenovan po treh avtorjih: Rivest, Shamir, Adleman
[13]NIST – National Institute of Standards and Technology
[14]DSS – Digital Signature Standard

3.2.2.4 Povezava med podpisom in zapisom

Elektronski podpisi, izvedeni na elektronskih zapisih, naj bodo povezani s pripadajočim elektronskim zapisom. S tem zagotovimo, da elektronskega podpisa ni mogoče ponarejati na običajen način, npr. izrezati, kopirati ali kako drugače prenašati (Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule.", 1997).

3.2.2.5 Elektronski podpisi

3.2.2.5.1 Splošne zahteve

Splošne zahteve za elektronske podpise so (Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule.", 1997):

- Vsak elektronski podpis naj bo enkraten, lasten enemu posamezniku in naj ne bo ponovno uporabljen ali dodeljen komurkoli drugemu.
- Posameznikovo identiteto je treba preveriti še preden se njegov elektronski podpis ali del podpisa vzpostavi, dodeli, potrdi ali kako drugače spremeni. .
- Pred uporabo elektronskih podpisov ali ob njenem pričetku, je treba pri ameriški Upravi za hrano in zdravila potrditi, da so elektronski podpisi, uporabljeni na sistemu po 20. 8. 1997, pravno enakovredni ročnemu podpisu. To potrdilo mora biti oddano v papirni obliki in ročno podpisano. Če Uprava dodatno zahteva, naj posamezniki, ki uporabljajo elektronski podpis, pripravijo dodatno potrditev ali izjavo, da je specifičen elektronski podpis pravno enakovreden njihovemu ročnemu podpisu.

3.2.2.5.2 Komponente in nadzor elektronskega podpisa

Za nebiometrične elektronske podpise veljajo spodaj našteta pravila (Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule.", 1997):

- *Sestavljeni naj bodo iz vsaj dveh delov (komponent), npr. identifikacijske kode in gesla.*

  Kadar posameznik izvede serijo podpisov med enkratnim, neprekinjenim, nadzorovanim dostopom do sistema, naj vsebuje prvi podpis vse sestavine elektronskega podpisa. Pri naslednjem podpisu lahko uporabi samo tisti del podpisa, ki ga pozna samo ta posameznik.
  Kadar posameznik izvaja enega ali več elektronskih podpisov, ki niso izvedeni pri enkratnem, neprekinjenem, kontroliranem dostopu do sistema, naj bo vsak podpis izveden z uporabo vseh sestavnih delov elektronskega podpisa.

- *Uporabljajo jih lahko samo njihovi lastniki.*

  Bodo administrirani in izvedeni na tak način, da poskus uporabe posameznikovega podpisa s strani nekoga drugega, ni mogoč.

Biometrični elektronski podpisi naj bodo izvedeni tako, da jih lahko uporabi le pravi lastnik elektronskega podpisa.

3.2.2.5.3 Nadzor identifikacijskih kod in gesel

Uporabo elektronskega podpisa, ki temelji na uporabi identifikacijskih kod in gesel, je treba ustrezno nadzorovati, da zagotovimo varnost in celovitost elektronskega podpisa. S takšnim nadzorom moramo poskrbeti (Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule.", 1997):

- da je vsaka kombinacija identifikacijske kode in gesla enkratna, tako da niti dva posameznika nimata enake kombinacije;
- da se izdaja identifikacijskih kod in gesel periodično preverja, pregleda in po potrebi prekliče;
- da so v primeru izgube ali kraje: vzpostavljeni postopki za elektronsko deavtorizacijo žetonov, kartic ali drugih naprav, ki so nosilci informacij o identifikacijski kodi ali geslu, izdaja začasnih ali stalnih zamenjav primerno nadzoruje;
- za uporabo varovalnih mehanizmov, ki nepooblaščenim osebam preprečujejo uporabo identifikacijskih kod in gesel; zagotoviti moramo odkrivanje nepooblaščenih poizkusov uporabe in poročanje o tem (administratorju, vodstvu);
- začetno in periodično testiranje kartic, žetonov in naprav, ki so nosilci informacij o identifikacijski kodi ali geslu; s tem zagotovimo, da ustrezno delujejo in da niso bili spremenjeni na nepooblaščen način.

3.2.3 Doseganje skladnosti z regulativo

V tem poglavju je predstavljen proces, s katerim dosegamo in ohranjamo skladnost računalniških sistemov z regulativo. Farmacevtska industrija priznava, da večina sedanjih programskih rešitev ni popolnoma skladna z regulativo. Skladnost bodočih programskih rešitev je odvisna od funkcionalnosti, ki jih zagotavljajo dobavitelji s svojimi programskimi paketi. Farmacevtska industrija mora skupaj z dobavitelji uvajati nove tehnologije in hkrati zagotavljati skladnost s predpisi. Pri sedanjih sistemih je treba v okviru uporabljenih tehnologij takoj doseči kar največjo možno skladnost. Če obstajajo tehnološke omejitve, je treba skladnost zagotoviti z ustreznimi postopki (Dayton, 2001, str. 1).

Namen v nadaljevanju predstavljenega pristopa k doseganju skladnosti z regulativo je (Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000):

- zagotoviti, da bodo v primeru tehnoloških omejitev takoj vzpostavljeni ustrezni postopki;
- pripraviti terminski plan, v katerem bo prikazano, kdaj bo dosežena popolna skladnost. Vanj so vključene tudi spremembe obstoječe tehnologije računalniških sistemov, za katere bo potrebno več časa. V vsakem trenutku mora biti možen prikaz napredka glede na izdelan plan.

Takšen pristop ima tri glavne elemente (Complying with 21CFR Part11 Electronic Records and Electronic Signatures, Final Draft, 2000):

- začetne korake, ki jih je treba izvesti;
- doseganje skladnosti pri novih sistemih;
- doseganje skladnosti pri obstoječih sistemih.

3.2.3.1 Doseganje skladnosti - začetni koraki

Obstajajo trije začetni koraki, ki naj bi jih izvedli kot osnovo pri doseganju skladnosti z regulativo (Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000).

1. *Določitev ciljev, ki jih je treba uskladiti z višjim vodstvom*

   Cilji pri doseganju skladnosti so: razumevanje regulatornih zahtev, izobraženo osebje, skladnost obstoječih sistemov in mehanizmi za zagotovitev skladnosti novih sistemov.

   Treba je določiti skupino za ugotavljanje in odpravljanje pomanjkljivosti pri obstoječih sistemih in za nadzor nad izvedbo pri novih sistemih. Skupino morajo sestavljati predstavniki enot za upravljanje kakovosti in informacijsko tehnologijo ter uporabniki sistemov.

2. *Komunikacija med vsemi*

   Preden začnemo pri projektu podrobneje delati, si je treba zagotoviti podporo višjega vodstva in z mehanizmi za doseganje skladnosti seznaniti celotno osebje, ki bo sodelovalo pri procesu.

   Razumeti moramo, da se regulativa nanaša na vse, vpletene v proces. Za razrešitev katerihkoli neskladnosti je nujno, da so temu predani vsi zaposleni.

   Da bi dosegli priznavanje elektronskih zapisov in elektronskih podpisov, je treba spremeniti organizacijsko kulturo v podjetju. Nove sisteme lahko uspešno uvedemo in uporabljamo le, če ljudje sprejemajo nov način razmišljanja. Eden največjih izzivov je biti bolj odvisen od elektronskih informacij kot od klasičnih papirnih dokumentov.

   Osebje se mora zavedati varnostnih zahtev in izvajati ustrezne postopke za prijavo in odjavo pri elektronskih sistemih, ki vpeljujejo elektronske podpise.

   Spremembe v organizacijski kulturi je mogoče doseči s programi za izobraževanje, ki so namenjeni ozaveščanju in sprejemanju odgovornosti.

   Ob uvedbi elektronskih podpisov je o tem treba obvestiti tudi ameriško Upravo za hrano in zdravila (FDA) ter jim zagotoviti, da razumemo elektronski podpis kot pravno veljaven in enakovreden ročnemu podpisu.

3. *Določitev interpretacije regulatornih zahtev*

   V organizaciji je treba določiti, kako bomo tolmačili (interpretirali) regulatorne zahteve. Najprimernejši način je, da to stori ekspertna skupina. Interpretacija je lahko različna od organizacije do organizacije, glede na to, kako zahtevni so njihovi elektronski sistemi. Bistveno je, da se interpretacija določi in dokumentira. To interpretacijo je potem mogoče prenesti na celotno organizacijo in tako zagotoviti razumevanje regulative. Ekspertna skupina ima lahko vlogo presojevalca za bodoča vprašanja in interpretacije.

Skupina strokovnjakov mora pri teh sistemih upoštevati znanje in izkušnje iz dobrih praks, pri katerih skladnost pogosto pomeni uporabo dobrega občutka ("common sense"[15]). Ta občutek lahko upoštevamo tudi pri sistemih z elektronskimi zapisi in elektronskimi podpisi. Ko je interpretacija zagotovljena, jo lahko uporabimo za obstoječe in nove sisteme.

V tej fazi je pomembno, da pregledamo in izboljšamo splošne postopke, kot je to potrebno. Preveriti moramo, ali smo upoštevali tudi vse lokalne regulatorne zahteve za uporabo elektronskih podpisov. Tudi v podjetju samem moramo pridobiti potrditev, da je uporaba elektronskega podpisa pravno enakovredna ročnemu podpisu.

3.2.3.2 Doseganje skladnosti - novi sistemi

Kot smo poudarili že v prejšnjem podpoglavju, je takoj po določitvi interpretacije regulative v sami organizaciji bistveno zagotoviti ustrezno izpolnjevanje zahtev na novih sistemih. Pri tem moramo predvideti več korakov (Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000).

1. *Izobraževanje projektnih timov*

   Skladnost trenutnih in predlaganih avtomatiziranih sistemov z regulativo o elektronskih podpisih in elektronskih zapisih je najbolj odvisna od projektnih skupin (timov), odgovornih za razvoj in dobavo teh sistemov. Izjemno pomembno je, da projektne skupine, še posebej njihovo vodstvo, razumejo pomembnost te regulative in se zavedajo svoje odgovornosti za zagotavljanje skladnosti.

   Pomembno je vedeti:

   - da je za skladnost sistemov v celoti odgovorna farmacevtska organizacija in ne dobavitelj sistema;
   - da je vloga dobavitelja pri zagotavljanju potrebnih tehnoloških funkcij in možnosti kritična;
   - da so za doseganje skladnosti uporabniške procedure prav tako kritične;
   - da mora biti zagotovitev skladnosti dokumentirana;.
   - da morajo biti aktivnosti, ki so pomembne za doseganje skladnosti, določene že med pogodbenimi pogajanji in načrtovane ves čas trajanja projekta.

   Dokumentirana interpretacija regulative je osnova za izobraževanje projektnih skupin. Interpretacija mora farmacevtski organizaciji omogočiti jasno opredelitev funkcionalnosti v vsakem novem sistemu, ki mora ustrezati regulativi. Interpretacija naj vključuje tudi zahteve glede validacije teh sistemov, preden se jih uvede v uporabo.

2. *Zagotovitev jasnih zahtev dobaviteljem*

   Avtomatizirani sistemi, ki vplivajo na kakovost produktov v proizvodnji farmacevtskih izdelkov, morajo izpolnjevati pravila dobre proizvodne prakse.

[15]"Common sense" – Občutek, nekaj, kar je pridobljeno na podlagi praktičnih izkušenj, brez posebne študije in ni izrecno navedeno v predpisih.

V uporabniških zahtevah za sisteme, ki vsebujejo elektronske zapise ali elektronske podpise, mora biti jasno določeno, kaj se zahteva od dobavitelja, da bo uporabnik lahko zagotovil skladnost z regulativo.

Pri izdelavi uporabniških zahtev je potrebno jasno določiti uporabo sistema. Opredeljeno naj bo:
- kateri elektronski zapisi bodo obstajali na sistemu in kateri proces jih ustvarja in posodablja,
- kje bodo uporabljeni elektronski podpisi,
- kakšen je namen elektronskih podpisov,
- katere odobritvene aktivnosti bodo potrjene z elektronskimi podpisi,
- kateri zapisi se bodo podpisovali (npr. podatek, ekranski zapis, zaporedje zapisov ipd.).

Predvideti je treba tudi zahteve za izvorne podatke, ki podpirajo elektronske zapise (npr. zgodovina dogodkov, histografija ipd.).

3. Ocena skladnosti predlagane tehnologije

Oceno skladnosti predlagane rešitve je treba izvesti v okviru predpogodbenih pogajanj. Ta ocena je sestavni del skupne ocene dobavitelja in predlagane rešitve. Informacije, potrebne za oceno skladnosti, lahko dobimo na različne načine:
- z oceno dobavitelja, ki jo običajno pridobimo pred izbiro dobavitelja (vključimo tudi oceno glede na regulativo o elektronskih podpisih in zapisih);
- z zahtevo potencialnim dobaviteljem, da se odzovejo na posebne zahteve, ki jih določa regulativa o elektronskih podpisih in elektronskih zapisih;
- z internim pregledom zahtev.

Z izvedeno oceno je pridobljena jasna slika stopnje skladnosti predlaganih rešitev. To je eden izmed dejavnikov, ki vpliva na izbiro rešitve oziroma dobavitelja. Možno je, da nobena izmed rešitev ni popolnoma skladna. V teh primerih imamo na voljo naslednje možnosti:
- zakasnimo ali odpovemo projekt,
- od dobavitelja zahtevamo odpravo pomanjkljivosti,
- predvidimo procese in postopke, s katerimi bomo odpravili pomanjkljivosti,
- projekt spremenimo tako, da izločimo pomanjkljivosti.

Odločitve v okviru ocene skladnosti so izredno pomembne in zagotavljajo bistvene informacije za morebitne potrebne spremembe validacijskega protokola, ki je opisan v nadaljevanju.

4. Ažuriranje in izvedba validacijskega protokola

Z oceno dobavitelja in specifikacij za izvedbo je večina informacij za izdelavo validacijskega protokola na voljo. Validacijski protokol naj vsebuje tudi zaporedje aktivnosti in virov, potrebnih za zagotovitev skladnosti z regulativo o elektronskih zapisih in podpisih. Del aktivnosti naj bo namenjen pridobivanju zagotovitev, da testiranje sistema prikaže skladnost z vsakim pomembnim predpisom v zahtevah. Prav tako je potrebno opredeliti odgovornosti za izvajanje ustreznih procedur za zagotavljanje in vzdrževanje skladnosti.

Navedene aktivnosti in zahteve zaradi dodatnih funkcionalnih zahtev za sistem in testiranja sistema seveda podražijo projekt. Vsekakor je bolje te dodatne aktivnosti in stroške določiti v začetnih fazah projektov kot pozneje, ko so vsake naknadne spremembe in aktivnosti še precej dražje. Pomembno je, da validacijski protokol sproti popravljamo in prilagajamo.

3.2.3.3 Doseganje skladnosti - obstoječi sistemi

Glede na dejstvo, da večina sedanjih računalniških sistemov ni skladna s predpisi o elektronskih zapisih in elektronskih podpisih, moramo izvesti spremembe tudi na teh sistemih (Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000). Ta proces zajema:

1. *Oblikovanje skupine*

   Pred oblikovanjem skupine je treba za predstavnika projekta pridobiti osebo, ki je v podjetju visoko na hierarhični lestvici in ki bo zagovarjala namen in nujnost zagotavljanja skladnosti. To je potrebno, ker so za podrobno oceno skladnosti obstoječih sistemov in potrebne korektivne ukrepe oziroma aktivnosti lahko potrebni veliki viri (finančni in človeški).

   Velikost skupine je odvisna od velikosti in števila računalniških sistemov. Za konkreten računalniški sistem mora biti skupina sestavljena iz:
   - vodje, ki bo razvijal in vodil proces ocenjevanja skladnosti;
   - ocenjevalca, ki bo izvedel oceno (lahko tudi vodja);
   - predstavnika enote za informacijsko tehnologijo oziroma skrbnika sistema, ki bo s svojim znanjem zagotavljal razjasnitev tehničnih podrobnosti;
   - uporabnika oziroma lastnika sistema.

   Vsaj eden od članov skupine mora biti seznanjen z načeli dobrih praks in regulativo o elektronskih zapisih in podpisih.

2. *Oceno stopnje skladnosti za vsak sistem*

   Potem, ko imamo na voljo interpretacijo regulative o elektronskih podpisih in elektronskih zapisih, lahko začnemo z ocenjevanjem trenutne stopnje skladnosti obstoječih sistemov. To najbolje naredimo v dveh fazah:

   - v 1. fazi za vsak sistem ocenimo, ali moramo upoštevati regulativo o elektronskih podpisih in zapisih;
   - v 2. fazi za sisteme, pri katerih je treba regulativo upoštevati, ocenimo, kako obsežna je neskladnost.

1. faza

Pripravimo spisek vseh računalniških sistemov. Ocenimo, ali za posamezen sistem regulativa o elektronskih zapisih in elektronskih podpisih velja. Za pomoč pri ocenjevanju si lahko zastavimo naslednja vprašanja:

- Ali je sistem vključen v "GXP proces"[16]?
- Če je, ali zajema "GXP podatke"[17]?
- Če jih, ali hrani "GXP podatke" na spominskem mediju?
- Ali osebje elektronsko potrjuje izvedbo "GXP akcij" ali to nadomešča ročni podpis, ker je tako določeno v predpisih?

Ključ za odgovor na zgoraj navedena vprašanja je razumevanje, kateri elektronski zapisi in podpisi obstajajo v sistemu. Ravno tako je potrebno upoštevati izvorne podatke, ki podpirajo elektronske zapise. Zapisi tega procesa so osnova za vključitev ali izključitev sistema iz projekta in naj jih podpišejo lastnik sistema, ocenjevalec in predstavnik enote za upravljanje kakovosti.

2. faza

Podrobna analiza je najlaže izvedljiva, če imamo pripravljen vprašalnik, na podlagi katerega ocenjujemo sistem. Smiselno je, da se vprašalnik nanaša neposredno na regulativo. Razdelimo ga lahko v več sekcij:

- postopki in nadzor za zaprte sisteme,
- postopki in nadzor za odprte sisteme,
- elektronski podpisi (splošno, biometrični, nebiometrični),
- nadzor za identifikacijske kode in gesla,
- nadzor za žetone, kartice ali druge naprave, ki so nosilci informacije o identifikacijski kodi ali geslu.

Vprašalnik je lahko pripravljen v obliki tabele, v kateri so tudi stolpci za vpis komentarjev in predlaganih ukrepov v primeru neskladnosti. Za boljši kvantitativni občutek se lahko določi ocenjevalni sistem (%). Popis neskladnosti v tej obliki omogoča presoje in ocene glede na neskladnosti v celotnem podjetju, kar je pomembno za naslednjo fazo.

3. Analiza neskladnosti

Zadnje faze analize vključujejo:

- analizo rezultatov izvedene ocene,
- oceno prioritet,
- odločitev o aktivnostih, ki se bodo izvedle na posameznem sistemu,
- dokumentiranje odločitve.

Za vsak sistem obstaja le pet možnih odločitev:

a.) prenehanje aktivnosti

Možno je, da starejši ali manjši sistemi bistveno ne pripomorejo k zagotavljanju dobrih praks (GXP). Zato se jih ne splača nadgraditi, ampak lahko z aktivnostmi prenehamo.

[16] GXP proces - Proces, ki lahko vpliva na kakovost izdelka.
[17] GXP podatki - Podatki, ki imajo informacije o kakovosti izdelka.

b.) upokojitev sistema in prehod nazaj na ročno vodenje
Ta možnost je lahko primerna za enake sisteme kot pod točko a.). Strošek nadgradnje morda presega vrednost, ki jo prispeva sistem. Vendar, če sistem vsebuje elektronske zapise, je potrebno tudi te upokojiti. Nadaljnji dostop do "upokojenih" zapisov lahko omogočimo s hranjenjem strojne in programske opreme; možnost dostopa naj imajo le pooblaščeni posamezniki, npr. v primeru reklamacij ali odpoklicev izdelka s trga.

c.) vzpostavitev postopkov
To je verjetno najpogosteje uporabljena možnost. Vzpostavijo se procedure in pripravi izobraževanje uporabnikov, da se izognemo neskladnostim sistema z regulativo.

d.) zamenjava sistema
To je najhitrejša in najbolj stroškovno učinkovita možnost, vendar cena in potrebno delo onemogočata izvedbo pri vsakem sistemu.

e.) nadgradnja sistema
To je lahko velika ali majhna naloga. Ocenijo naj jo strokovnjaki za informacijsko tehnologijo.

Primeren ocenjevalni sistem pomaga pri oceni in določitvi prioritet. Dejavniki, ki vplivajo na prioriteto oziroma kritičnost, so:

- "GXP kritičnost" sistema,
- obseg neskladnosti (velika, srednja, mala),
- varnost in celovitost podatkov,
- starost sistema in kdaj se pričakuje upokojitev.

Ob zaključku tega procesa moramo pripraviti:

- spisek sistemov, ki jih je treba uskladiti s predpisi;
- seznam neskladnosti, ki jih je treba odpraviti;
- seznam aktivnosti, ki jih je treba izvesti za vsak sistem;
- vrstni red, po katerem jih bomo uskladili z regulativo.

To so hkrati tudi vhodi v končne faze celotnega procesa.

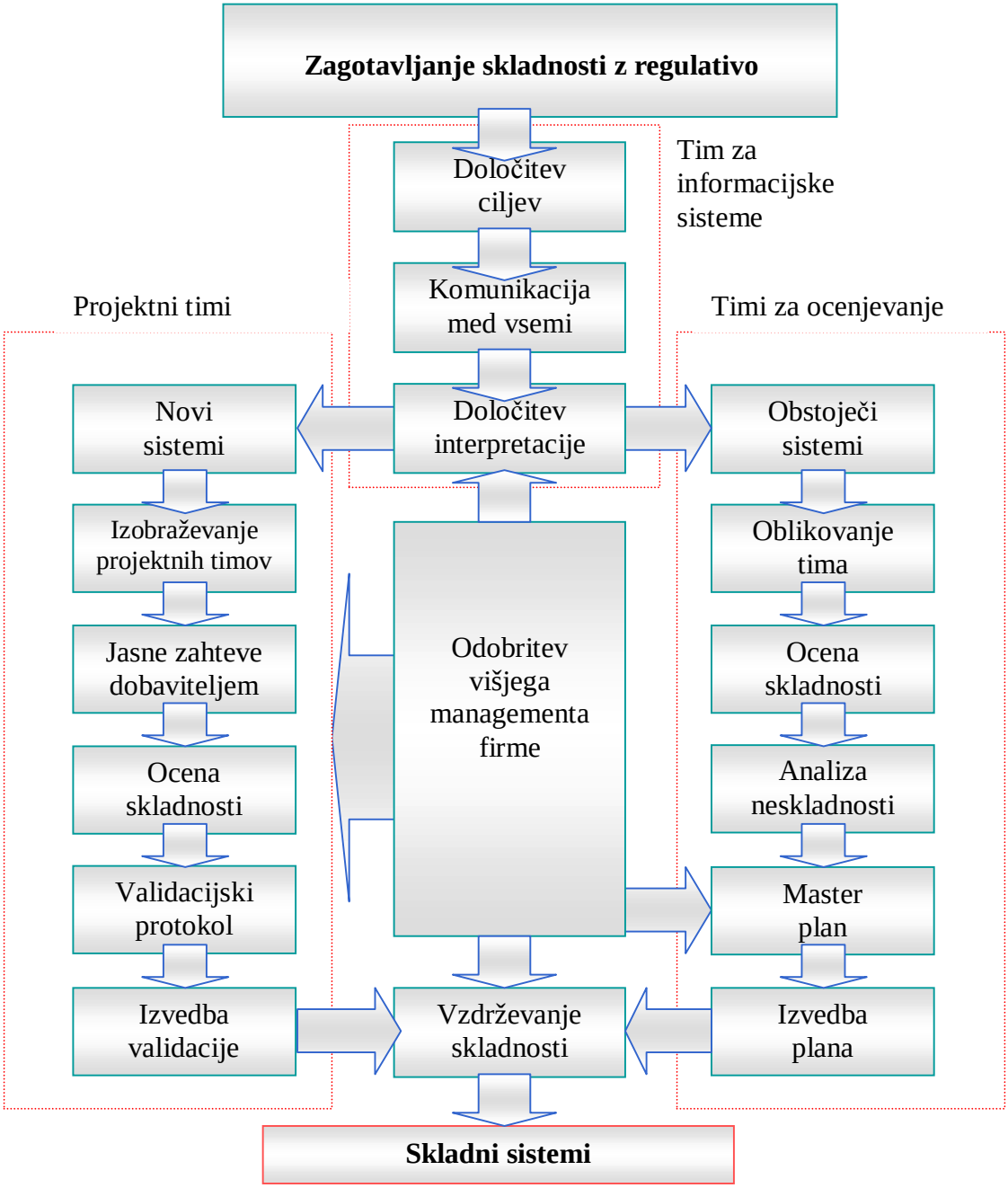
4. Izdelava in izvedba master plana

Večina informacij, ki jih potrebujemo za izdelavo master plana, je že na voljo. Program validacije izdelamo na enak način kot validacijski master plan: z zaporedjem aktivnosti, dogodki in viri, potrebnimi za izvedbo projekta. Vse to omogoča oceno stroškov. Odločitev za pričetek projekta morajo sprejeti višji vodilni (management). V večji tovarni bodo stroški precej veliki; ob njihovi omejitvi bo pred dokončno potrditvijo treba izvesti revizijo programa validacije.

Pomembno je, da program validacije pregledamo in revidiramo, ker se ves čas razvija tudi interpretacija regulative. Sprememba interpretacije lahko pomembno vpliva na program validacije, zato ga je treba primerno popraviti oziroma posodobiti.

Na sliki 6 je še enkrat shematsko prikazan celoten proces zagotavljanja skladnosti z regulativo o elektronskih zapisih in elektronskih podpisih.

Slika 6: Zagotavljanje skladnosti z regulativo



Vir: Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, 2000.

3.2.3.4 Zaključek

Novi predpisi na področju elektronskih podpisov in elektronskih zapisov omogočajo razvoj nove, bolj učinkovite tehnologije v regulirani farmacevtski industriji. Uvedba novih tehnologij in orodij je priložnost, ki jo treba izkoristiti, da bi ohranili konkurenčnost na trgu.

To pomeni, da je treba regulativo ustrezno tolmačiti (interpretirati) in jo upoštevati najprej pri novih sistemih, ki jih še uvajamo, nato pa pri obstoječih sistemih, saj je tudi te treba uskladiti z regulativo na tem področju. To je treba izvesti stroškovno in časovno najbolj optimalno.

V tem poglavju smo predstavili pristop k doseganju in vzdrževanju skladnosti v farmacevtskih podjetjih. Zelo pomembno vlogo v podjetju ima višje vodstvo, ki mora ustrezno odobriti najprej tolmačenje predpisov in nato vse vire (finančne in človeške), ki so potrebni za doseganje skladnosti novih in obstoječih sistemov ter njeno vzdrževanje na vseh sistemih.

4. Večparametrski odločitveni model

Večparametrski odločitveni model nam pomaga pri reševanju kompleksnega odločitvenega problema. Problem najprej ustrezno opredelimo. Poznati moramo njegovo vsebino. Nato na osnovi znanih dejstev zberemo kriterije, ki vplivajo na vedenje o nekem problemu. Zberemo vse kriterije in zanje določimo zalogo vrednosti (vsa možna stanja). Tako določene kriterije nato združujemo v kriterije višjega reda, t. i. sestavljene ali agregirane kriterije. Združevanje nadaljujemo toliko časa, da dosežemo najvišji osnovni kriterij. Na osnovi tako izdelanega modela lahko za vsako posamezno varianto določamo vrednosti kriterijev in z agregiranimi kriteriji tudi vrednost celotnega modela (Bohanec, Urh, Rajkovič, 1992, str. 69).

Za zbiranje podatkov o možnih kriterijih, ki jih lahko vključimo v neki model, in njihovih vrednosti lahko uporabimo različne metode: ankete, viharjenje možganov, študij literature ipd.

4.1 Nabor kriterijev

Na osnovi študija literature, viharjenja možganov in izvedenih posvetovanj smo za nadaljnje raziskovanje izbrali v nadaljevanju navedene kriterije. Opisujemo kriterije in trditve, ki določajo negativne oziroma pozitivne lastnosti kriterija pri ocenjevanem računalniškem sistemu.

Kritičnost računalniškega sistema
├ GXP kritičnost sistema
└ Skladnost z regulativo

Kritičnost računalniških sistemov ocenjujemo glede na oba navedena kriterija. Oba sta ravno tako sestavljena oziroma agregirana kriterija; njune značilnosti so podane v nadaljevanju.

Skladnost z regulativo ima na končno oceno kritičnosti nekoliko večji vpliv kot "GXP kritičnost sistema". Skladnost pomeni oceno sistema glede na zahteve nacionalnih in mednarodnih regulatornih zahtev, "GXP kritičnost sistema" pa vpliv sistema na kakovost izdelka.

Kritičnost računalniškega sistema ovrednotimo z zalogo vrednosti: *zelo kritičen, precej kritičen, srednje kritičen, manj kritičen* in *nekritičen*.

V nadaljevanju podajamo strukturo vseh agregiranih oziroma sestavljenih kriterijev do ravni osnovnih kriterijev. Najprej opišemo osnovne kriterije in način združevanja v višje kriterije.

Določene zaloge vrednosti in odločitvena pravila, kako se na podlagi vrednosti osnovnih kriterijev določa vrednost sestavljenih kriterijev, so podani v dodatku. Razviden je tudi vpliv oziroma utež posameznega kriterija na višje kriterije.

Agregirani oziroma sestavljeni kriteriji so označeni s krepkim tiskom.

4.1.2 "GXP" kritičnost sistema

GXP kritičnost sistema
- Vpliv na kakovost izdelka
- Odprtost sistema

S kriterijem "GXP kritičnost sistema" določimo, v kolikšni meri ima posamezen sistem vpliv na kakovost izdelka. Takšne sisteme inšpekcije tudi najbolj temeljito pregledujejo. Vpliv sistema na kakovost izdelka je lahko neposreden, posreden preko drugih sistemov ali pa vpliva ni.

Drug dejavnik, ki vpliva na kritičnost sistema, je odprtost sistema. Sistem je bolj kritičen, če je bolj odprt. Pod odprtost sistema razumemo tako fizično kot logično dostopnost do njega.

Tu velja omeniti tveganje pri sistemih, ki se uporabljajo prek svetovnega spleta. Za takšne sisteme (zapise, ki se prenašajo prek interneta) je treba zagotoviti dodatne varnostne ukrepe, kot sta: kodiranje in uporaba digitalnih podpisov, ter tako zagotoviti pristnost, celovitost in zaupnost elektronskih zapisov.

4.1.3 Skladnost z regulativo

Skladnost z regulativo
- Klasifikacija sistema
- **Elektronski zapisi**
- **Elektronski podpisi**

Za zagotavljanje skladnosti računalniških sistemov z nacionalnimi in mednarodnimi predpisi so potrebni veliki finančni in človeški viri. Skladnost z regulativo se razdeli na skladnost za elektronske zapise in skladnost za elektronske podpise.

Zalogo vrednosti ovrednotimo z: *neskladni, delno skladni* in *skladni* sistemi.

Elektronski podpisi in elektronski zapisi se ne uporabljajo na vseh sistemih. S kriterijem "klasifikacija sistema" določimo, ali je sistem takšen, da vsebuje le elektronske zapise ali vsebuje elektronske zapise in elektronske podpise. V primeru, da ne vsebuje ne zapisov in ne podpisov, skladnosti ni potrebno zagotavljati.

"Klasifikacija sistema" je tako izločilni kriterij za ostale kriterije v poddrevesu kriterija "skladnost z regulativo". Kriterij "klasifikacija sistema" lahko zavzame vrednosti: *zapisi in podpisi, samo zapisi, ni zapisov ni podpisov*.

4.1.3.1 Elektronski zapisi

Elektronski zapisi
- **Validacija elektronskih zapisov**
- **Zaščita**
- **Zgodovina dogodkov**
- **Sistemska dokumentacija**

Pri skladnosti elektronskih zapisov govorimo o validaciji, zaščiti, zgodovini dogodkov in sistemski dokumentaciji. Vsi ti kriteriji so sestavljeni in opisani v nadaljevanju.

V okviru validacije preverjamo (validiramo) tudi vse ostale kriterije. Pri združevanju vseh kriterijev ima največji vpliv zaščita zapisov. Dobimo lahko vrednosti: *neskladni, delno skladni* in *skladni* elektronski zapisi.

4.1.3.1.1 Validacija elektronskih zapisov

Validacija elektronskih zapisov
- **Validacija glede na industrijske standarde**
- **Validacija glede na regulativo o elektronskih podpisih in zapisih**

Validacijo elektronskih zapisov smo razdelili na dva dela: validacijo glede na industrijske standarde, ki smo jo uporabljali zadnjih nekaj let, in validacijo glede na regulativo o elektronskih podpisih in zapisih. Obseg slednje je določen z opisom regulative s tega področja v prejšnjem poglavju.

Validacija je dokumentiran dokaz, da je sistem razvit, instaliran in operativen v skladu s predhodno postavljenimi specifikacijami oziroma zahtevami. Ne validiramo samo sistema, ampak običajno tudi celoten proces.

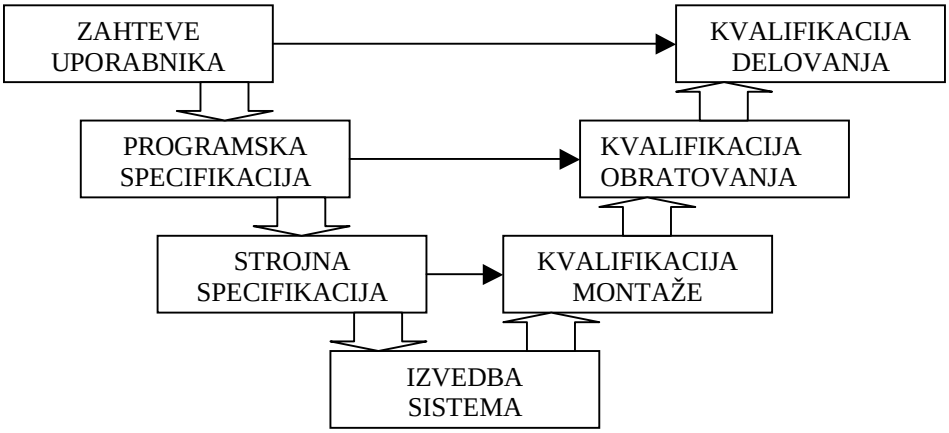
Validacija procesa je dokumentiran program, ki ima visoko stopnjo zanesljivosti, da bo specifičen proces konstantno proizvajal izdelek, ki ustreza predhodno postavljeni specifikaciji in kakovosti (Guidelines on General Principles of Process Validation, 1987).

4.1.3.1.1.1 Validacija glede na industrijske standarde

Validacija glede na industrijske standarde
- **Specifikacije**
- **Kvalifikacija**
- **Postopki**
- **Izobraževanje**

Validacija glede na industrijske standarde se izvaja ves čas življenjskega cikla sistema: od določitve uporabniških zahtev, programskih in strojnih specifikacij do izvajanja kvalifikacij, izdelave postopkov za delo in administracijo ter izvedbe izobraževanja za vse, vključene v sistem. Takšno validacijo imenujemo prospektivna validacija; dobro je predstavljena z V modelom, prikazanim na sliki 7.

Slika 7: V model za prospektivno validacijo



Vir: GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture – Volume2, 1998.

Iz slike 7 je razvidno, da se zahteve uporabnika nanašajo na kvalifikacijo delovanja, programska specifikacija se nanaša na kvalifikacijo obratovanja in strojna specifikacija na kvalifikacijo montaže (GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture – Volume2, 1998).

Na skupni kriterij najbolj vplivata kriterija "kvalifikacija" in "specifikacije". Vsi kriteriji so sestavljeni iz osnovnih kriterijev, ki so opisani v podpoglavjih od 4.1.3.1.1.1.1 do 4.1.3.1.1.1.4.

4.1.3.1.1.1.1 Specifikacije

Specifikacije
- Zahteve uporabnika
- Ocena dobavitelja
- Programska in strojna specifikacija

Specifikacije predstavljajo potrebne dokumente za določitev računalniškega sistema. Ta je določen najprej z zahtevami uporabnika, nato z oceno dobavitelja in seveda s podrobno programsko (funkcijsko) in strojno specifikacijo.

Bistvene za vsako nadaljnje izvajanje kvalifikacij oziroma validacij sistema so ustrezne specifikacije sistema. Na sestavljeni kriterij "specifikacije" najbolj vpliva osnovni kriterij "programska in strojna specifikacija", sledita mu "zahteve uporabnika" in "ocena dobavitelja". V zalogi vrednosti so: *neustrezne, delno ustrezne* in *ustrezne* specifikacije.

Zahteve uporabnika

Zahteve uporabnika določajo, kaj ta pravzaprav želi pri posameznem računalniškem sistemu. V tem dokumentu so običajno opisane funkcijske zahteve za tehnologijo, podatkovne zahteve, zahteve glede arhiviranja in restavriranja, zahteve glede povezljivosti informacijskih sistemov ipd.

V okviru ocenjevanja ocenjujemo ustreznost, delno ustreznost ali neustreznost uporabniških zahtev glede na regulativo in interne splošne postopke podjetja (ti so običajno usklajeni z regulativo).

Ocena dobavitelja

Oceno dobavitelja lahko izvajamo na dva načina: prek referenc ali z izvedbo presoje dobavitelja. Ocenjujemo upoštevanje standardov in vgrajene kontrole kakovosti v proces izdelave ter validacije računalniškega sistema.
Presoja dobavitelja omogoča kupcu, da preveri dobavitelja glede na (GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture – Volume2, 1998):

– tehnične kompetence,
– zmožnost zagotovitve validacijskih zahtev,
– vzpostavitev in skladnost sistema kakovosti,
– razpoložljivost in kakovost izdelkov (strojna oprema, programska oprema, storitve).

Programska in strojna specifikacija

Programska oziroma funkcijska in strojna specifikacija podrobno opisujeta računalniški sistem. V strojni specifikaciji so podane specifikacije za vso strojno opremo, v programski specifikaciji pa za delovanje programske opreme oziroma izvedene programske rešitve. V programski specifikaciji morajo biti poleg navodil za delo in opisa funkcij navedene še druge specifikacije, kot so: arhiviranje, restavriranje podatkov, zaščita sistema, nepričakovani izpadi sistema, diagram poteka, izvorna koda programa ipd.

4.1.3.1.1.1.2 Kvalifikacija

Kvalifikacija
- Kvalifikacija načrtovanja - DQ[18]
- Kvalifikacija montaže - IQ[19]
- Kvalifikacija obratovanja - OQ[20]
- Kvalifikacija delovanja - PQ[21]

[18] DQ - Design Qualification
[19] IQ - Installation Qualification
[20] OQ - Operational Qualification
[21] PQ - Performance Qualification

Kvalifikacija pomeni dokumentiran dokaz, da je sistem zgrajen in da deluje v skladu s specifikacijami. Pri čemer se kvalifikacija montaže nanaša neposredno na strojno specifikacijo, kvalifikacija obratovanja na programsko oziroma funkcijsko specifikacijo in kvalifikacija delovanja na uporabniške zahteve.

Kvalifikacija načrtovanja - DQ

Kvalifikacija načrtovanja poteka ves čas začetnega dela življenjskega cikla sistema. Zajema potrjevanje uporabniških zahtev, projektne naloge, projektov za izvedbo in sistemskih specifikacij (strojne in funkcijske specifikacije). Kvalifikacija načrtovanja potrdi ustreznost načrtovanja sistema predvsem s stališča dobre proizvodne prakse in glede na podane uporabniške zahteve (GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture - Volume1, 1998).

Kvalifikacija montaže - IQ

Kvalifikacija montaže pomeni dokumentiran dokaz, da je sistem montiran, instaliran in povezan v skladu s specifikacijami. V okviru kvalifikacije montaže preverjamo, ali je na voljo vsa zahtevana dokumentacija, ali so pogoji okolja ustrezni, pregledamo karakteristike opreme in preverimo ustreznost montaže. Ustreznost montaže je ločena za mehanski in električni del ter vgrajene komponente (GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture - Volume1, 1998).

Kvalifikacija obratovanja - OQ

Kvalifikacija obratovanja pomeni dokumentiran dokaz, da posamezne funkcije sistema delujejo v skladu s programsko oziroma funkcijsko specifikacijo. V okviru teh aktivnosti preverjamo ustreznost krmilnih funkcij programa, vnos podatkov, prikaz podatkov, stresne situacije, nepričakovane izpade ipd. Posebej preverimo vsako posamezno funkcijo sistema, ki je bistvena za delovanje celotnega sistema (GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture - Volume1, 1998).

Kvalifikacija delovanja - PQ

Kvalifikacija delovanja pomeni dokumentiran dokaz, da celoten sistem (skupek funkcij) deluje v skladu s pričakovanji in zahtevami uporabnika. Sestavni del teh aktivnosti so integracijski testi, pri katerih združimo celoten proces, ki se dejansko izvaja na sistemu. Poleg tega preverimo interakcije in delovanje sistema v okviru povezav z drugimi sistemi ter ustreznost delovanja celote (GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture - Volume1, 1998).

4.1.3.1.1.1.3 Postopki

Postopki
- Validacijski protokol
- Poročilo o validaciji
- **Sistemski splošni postopki**
  - Delovanje sistema
  - **Administracija sistema**
    - Periodični pregled sistema
    - Arhiviranje, varnostno kopiranje, restavracija sistema in zapisov
    - Konfiguracija sistema in zaščit

Za vsak sistem morajo biti izdelani sistemski splošni postopki za delovanje in administracijo sistema ter postopki, ki nastanejo v okviru validacije. To sta validacijski protokol in poročilo o validaciji (Teuchert, 2000, str. 20).
Za vse kriterije, osnovne in sestavljene, tudi za kriterij "postopki", je zaloga vrednosti: *ne, delno* in *da*.

Validacijski protokol

Validacijski protokol je dokument, ki določa način izvajanja validacije, predpiše njen namen, odgovorne osebe za validacijo, nabor testiranj, način izvedbe in kriterije sprejemljivosti (GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture - Volume1, 1998).

Poročilo o validaciji

Poročilo o validaciji je dokument o validaciji, izvedeni po predpisanem validacijskem protokolu. V njem so navedeni potek validacije, vsa odstopanja, ki so se pojavila med postopkom, in končna ocena ustreznosti validacije sistema.

Administracija sistema

Administracija sistema je lahko sestavljena iz enega samega postopka (dokument) ali več postopkov, ki vsebujejo navodila za periodični pregled sistema, varnostno kopiranje, arhiviranje, restavracijo sistema in zapisov ter konfiguracijo sistema in zaščit.

Delovanje sistema

Postopek za delovanje sistema je dokument, ki določa delovanje sistema in navodila za delo s sistemom.

4.1.3.1.1.1.4 Izobraževanje

Izobraževanje
- Uporabniki, sistemski administratorji
- Razvijalci, interni presojevalci, zunanji
- Dokumentiranost

Za postopke, naštete v prejšnjem poglavju, mora biti izvedeno izobraževanje. Izvaja se za uporabnike in sistemske administratorje. Poleg tega morajo biti ustrezno izobraženi vsi, ki so kakorkoli vključeni v posamezen sistem: od razvijalcev sistema, služb za upravljanje kakovosti, ki pregledujejo sisteme, do zunanjih izvajalcev, ki kakorkoli uporabljajo ali vplivajo na sistem.

Pomembno je, da so vsa ta izobraževanja tudi dokumentirana.

4.1.3.1.1.2 Validacija glede na regulativo o elektronskih podpisih in zapisih

Validacija glede na regulativo o elektronskih podpisih in zapisih
- **Neveljavni, spremenjeni zapisi**
- **Generiranje kopij elektronskih zapisov**
- **Ostale zahteve za validacijo elektronskih zapisov**

Validacija, ki se izvaja po industrijskih standardih, v zadnjih letih ni več dovolj dobra. Dodatno je treba izvesti tudi validacijo sistema glede na regulativo o elektronskih zapisih in podpisih. Vsebina te validacije dokazuje, da so elektronski zapisi varni, zanesljivi in ustrezno prikazani ter da so mehanizmi za izvedbo in nadzor elektronskega podpisa ustrezni.

4.1.3.1.1.2.1 Neveljavni, spremenjeni zapisi

Neveljavni, spremenjeni zapisi
- Neveljavni vnosi
- Sposobnost razlikovanja spremenjenih zapisov
- Test razlikovanja spremenjenih zapisov

Sistem mora biti sposoben prepoznavati neveljavne vnose. To pomeni, da pri vsakem vnosu podatkov sistem preverja ustreznost vnosa (npr. znotraj predpisanih mej, samo številčne vrednosti ipd.). Poleg tega mora biti sistem sposoben prepoznavati zapise, ki so bili kakorkoli spremenjeni. Ustrezno prepoznavanje spremenjenih zapisov moramo testirati in ustrezno dokumentirati.

4.1.3.1.1.2.2 Generiranje kopij elektronskih zapisov

Generiranje kopij elektronskih zapisov
- Prikaz v elektronski obliki
- Prikaz v obliki izpisa
- Prenašanje v elektronski obliki

Za potrebe poznejšega pregledovanja zapisov in tudi za potrebe inšpekcij mora biti sistem sposoben ustvariti (generirati) "točne in popolne" kopije zapisov. Te kopije zapisov mora biti možno prikazati v elektronski obliki in v obliki izpisa na papirju. Poleg tega mora biti možno te zapise tudi elektronsko prenašati. V okviru validacije moramo nastajanje kopij elektronskih zapisov testirati in jih tudi ustrezno dokumentirati (Enforcement Policy:

21CFR Part11; Electronic Records; Electronic Signatures, Compliance Policy Guide, 1999).

4.1.3.1.1.2.3 Ostale zahteve za validacijo elektronskih zapisov

Ostale zahteve za validacijo elektronskih zapisov
- Zgodovina dogodkov
- Zaporedje dogodkov
- **Zaščita zapisov in dostopa**
  - Testiranje dostopa in avtorizacij
  - Testiranje arhiviranja in restavracije zapisov
  - Test naprav, ki so vir vhodnih podatkov

Ostale zahteve za ustrezno validacijo elektronskih zapisov vsebujejo testiranja zgodovine dogodkov, zaporedja dogodkov oziroma procesa in testiranje ustreznosti zaščit zapisov ter dostopa.

V zgodovini dogodkov se morajo evidentirati vse spremembe zapisov, od nastanka, spremembe do brisanja zapisov. Iz zgodovine dogodkov morajo biti razvidni: datum in čas, uporabnik (polno tiskano ime), staro in novo stanje zapisa.

Zaporedje dogodkov mora biti vsiljeno s samim procesom in tudi avtomatizirano. Na primer, določenega poročila ne moremo odobriti, če ga prej ni pregledala odgovorna oseba. Sistem mora zahtevati točno določeno zaporedje operacij. Testiranje zaporedja operacij je sestavni del začetne validacije sistema (Abel, LeBlanc, 1999, str. 12).

V vsakem sistemu mora biti dostop zaščiten in avtorizacija dovoljena samo pooblaščenim uporabnikom. V okviru validacije je treba sistem avtorizacij testirati v celoti. To pomeni, da preverimo vse, od načina dodelitve avtorizacij do podrobnega testiranja pravic dostopa posameznih uporabnikov.

Preveriti je treba ustreznost arhiviranja in restavracije zapisov glede na čas in celovitost podatkov.

Naprave, ki so vir vhodnih podatkov, je treba testirati pred pričetkom uporabe in periodično med uporabo naprav ali instrumentov.

4.1.3.1.2 Zaščita

Zaščita
- **Nadzor**
- **Zaščita zapisov**
- **Zaščita dostopa**

Nadzor elektronskih zapisov, zaščita elektronskih zapisov in zaščita dostopa do sistema so kriteriji, s katerimi zagotovimo celotno zaščito za elektronske zapise.

Zaščita elektronskih zapisov je pomembna, za njihovo točnost in celovitost ves čas hranjenja (Keatley, 1999, str. 78).

4.1.3.1.2.1 Nadzor

Nadzor
- **Pregledi zapisov**
- **Zaporedje dogodkov**
- **Preverjanje naprav**

Za zagotovitev ustreznosti in celovitosti zapisov je nad procesom treba imeti ustrezen nadzor. Takšen nadzor zajema preglede zapisov, zaporedje izvajanja dogodkov v procesu in preverjanje naprav, od katerih proces dobiva vhodne podatke.

4.1.3.1.2.1.1 Pregledi zapisov

Pregledi zapisov
- Uporabnika
- Administratorja
- Upravljanja kakovosti

Elektronske zapise morajo periodično pregledovati na različnih ravneh v podjetju. Uporabnik pregleduje zapise s stališča ustreznosti za proces, ki ga izvaja. Administrator pregleda zapise s stališča uporabe informacijskega sistema in ustreznosti delovanja programske rešitve. Predstavniki upravljanja kakovosti pregledujejo zapise s stališča zagotavljanja kakovosti v procesu.

V fazi validacije določenega sistema in izobraževanja je treba določiti način in vrsto pregledov za vse tri skupine uporabnikov. Treba jih je izobraziti, da so sposobni ustrezno izvajati navedene preglede.

4.1.3.1.2.1.2 Zaporedje dogodkov

Zaporedje dogodkov
- Vsiljeno zaporedje dogodkov
- Avtomatski mehanizem sekvenc

Če je možno, mora biti v sistem vgrajeno zaporedje dogodkov oziroma korakov, po katerih določen proces poteka.

Mehanizem sekvenc mora biti v čimbolj avtomatski in neodvisen od operaterja (Keatley, 1999, str. 78).

4.1.3.1.2.1.3 Preverjanje naprav

Preverjanje naprav
- Preverjanje vira vhodnih podatkov
- Periodično testiranje naprav

Vhodni podatki, ki pomenijo navodila za izvajanje procesa, morajo izvirati iz preverjenih naprav (npr. terminali, kodni čitalci ipd).

Tudi naprave, iz katerih prihajajo vhodni podatki, je treba periodično testirati, kar pomeni, da moramo redno preverjati ustreznost delovanja.

4.1.3.1.2.2 Zaščita zapisov

Zaščita zapisov
- Arhiviranje
- **Restavracija**
  - Glede na čas
  - Glede na celovitost podatkov
  - Periodično testiranje restavracije
- **Zaščita zapisov glede na lokacijo**
  - Na sistemu
  - Na arhivskem mediju
  - Perioda arhiviranja

Arhiviranje pomeni, da so elektronski zapisi v ustrezni obliki prevešeni iz sistema na drug arhivski medij in tam primerno hranjeni. Primerno so hranjeni takrat, ko ima dostop do arhivskega medija samo omejeno število ljudi, ko so zapisi zaščiteni pred vplivi okolja (npr. voda, ogenj, mraz) in ko jih je v nekem primerno kratkem času možno pridobiti nazaj (restavrirati).

Restavracija zapisov je pomembna, ker omogoča prenos arhivskih podatkov nazaj na sistem in omogoča njihovo pregledovanje. Pri restavraciji sta pomembna dva kriterija: čas in celovitost podatkov. Še primeren čas za pridobitev podatkov iz arhivskega medija je približno ena ura. Podatki morajo biti po restavraciji popolnoma enaki, kot so bili pred arhiviranjem, sicer postopka arhiviranja in restavracije nista ustrezna.

Poleg tega, da je treba v okviru validacije sistema dokumentirano potrditi ustreznost postopka arhiviranja in restavracije zapisov, moramo testiranje arhiviranja in restavracije zapisov izvajati tudi periodično (npr. enkrat na leto).

Zaščita zapisov mora biti ustrezna povsod, ne glede na to, kje se zapisi trenutno nahajajo. V primeru slabe zaščite na sistemu se težavam lahko izognemo tako, da je čas arhiviranja čim krajši (npr. nekaj minut). Če se arhiviranje sprememb izvaja na nekaj minut, je le malo možnosti, da bi nekdo v tako kratkem času naključno ali namerno poneveril oziroma spremenil zapise.

4.1.3.1.2.3 Zaščita dostopa

Zaščita dostopa
- Fizični dostop
- Arhiv konfiguracije zaščit
- **Logični dostop**

Dostop do elektronskih zapisov najprej najlažje zaščitimo z omejitvijo fizičnega dostopa do sistema. To storimo tako, da lahko samo pooblaščene osebe pridejo v bližino sistema in ga uporabljajo.

Arhiv konfiguracije zaščit je elektronski zapis, zato ga je treba ustrezno zaščititi in hraniti ves čas hranjenja zapisov (10 let ali več). Iz tega zapisa lahko za vsak trenutek v preteklosti razberemo, kdo so bili takratni pooblaščenci za delo s sistemom in kakšne so bile njihove pravice.

Način izvajanja logičnega dostopa do sistema v veliki meri opredeljuje zaščito dostopa do elektronskih zapisov. V naslednjih podpoglavjih opisujemo logični dostop do sistema.

4.1.3.1.2.3.1 Logični dostop

Logični dostop
├ **Avtorizacije**
└ **Dostop do sistema**

Logični dostop je opredeljen z avtorizacijami in z dostopom do sistema. Dostop do sistema je lahko omejen na ravni uporabniškega programa in na ravni operacijskega sistema, poleg tega je možno izvesti še avtomatsko odjavo v primeru neaktivnosti ("Inactivity Timeout"[22]) (Computerized Systems Used in Clinical Trials, Giudance for Industry, 1999, str. 7).

Dostop do sistema je lahko: *neomejen, delno omejen* ali *omejen.*

4.1.3.1.2.3.1.1 Avtorizacije

Avtorizacije
├ Način avtorizacije dostopa
├ Preverjanje avtorizacije za izvedbo podpisa
└ Preverjanje avtorizacije pri uporabi sistema

Avtorizacija je določena z načinom izvedbe dostopa do sistema in preverjanja avtorizacij na sistemu. Za avtorizacijo določenega uporabnika za delo na sistemu mora obstajati določena procedura, s katero se določijo in odobrijo vsi parametri za dostop do sistema (raven dostopa, geslo, uporabniško ime ipd.). Ko odgovorna oseba odobri posamezniku raven dostopa, lahko administrator sistema vnese oziroma avtorizira uporabnika na sistemu.

Pri uporabi sistema in pri izvajanju elektronskega podpisa se mora avtomatsko preveriti raven avtorizacije. To pomeni, da se pri uporabniku preveri, ali je avtoriziran za izvedbo določene funkcije oziroma za izvedbo podpisa na tej ravni (npr. odobritev elektronskega zapisa proizvodnega poročila).

[22] "Inactivity Timeout" - Po nekem določenem kratkem času (npr. po 5 minutah) neaktivnosti na sistemu se izvede avtomatska odjava uporabnika oziroma se pojavi ohranjevalnik zaslona, ki zahteva za nadaljnje delo ponoven vnos gesla uporabnika, ki je bil zadnji prijavljen.

4.1.3.1.2.3.1.2 Dostop do sistema

Dostop do sistema
- Operacijski sistem
- Avtomatska odjava
- **Aplikacija**
  - Večnivojski dostop
  - Prikritost gesel, minimalna dolžina gesel
  - **Uporabniški računi**
    - Potek uporabniškega računa
    - Periodično pregledovanje računov
    - Detekcija nepooblaščenih poizkusov dostopa

Zaščito dostopa do sistema je možno narediti že na ravni operacijskega sistema. Možno je zelo podrobno določiti in izvesti funkcije, ki so dovoljene posameznikom, še posebej, če je to operacijski sistem, kot je Windows NT. Na primer, na posameznem računalniku lahko uporabnikom določimo, da imajo dostop le do uporabniškega programa. S tem smo onemogočili enostavno brisanje ali spreminjanje datotek (elektronskih zapisov) na sistemu.

Avtomatska odjava v primeru, da v določenem času nihče ne dela na sistemu, je lahko narejena na ravni operacijskega sistema ali uporabniškega programa. Takšen primer je ohranjevalnik zaslona, ki zahteva ponoven vnos gesla uporabnika, ki je bil zadnji prijavljen.

Tudi na ravni uporabniškega programa morajo biti narejene ustrezne zaščite za gesla, kot sta prikritost in minimalna dolžina. Uresničen mora biti večnivojski dostop, in to na tak način, da se posameznikom dodeli pravice le do tistih funkcij, ki jih nujno potrebujejo za svoje delo. Pri uporabniških računih je pomemben kriterij "potek uporabniškega računa" (za primere zapustitve ali prehodov med delovnimi mesti). Uporabniške račune je treba periodično pregledovati in sistem mora biti sposoben odkriti in prikazati nepooblaščene poskuse dostopa do sistema.

4.1.3.1.3 Zgodovina dogodkov

Zgodovina dogodkov
- Ročna zgodovina dogodkov
- **Računalniško generirana zgodovina dogodkov**

V zgodovini dogodkov morajo biti zajeti vsi dogodke, ki se tičejo pomembnih elektronskih zapisov (nastanek, sprememba, brisanje).

V primeru, da sistem zgodovine dogodkov ne ustvari avtomatsko, je treba zagotoviti mehanizme za ročno dokumentiranje zgodovine dogodkov.

4.1.3.1.3.1 Računalniško generirana zgodovina dogodkov

Računalniško generirana zgodovina dogodkov
- **Ohranitev zgodovine dogodkov**
- **Časovna značka**
- **Ustreznost zgodovine dogodkov**

Avtomatsko zgodovino dogodkov sestavimo iz kriterijev za ohranitev zgodovine dogodkov, časovne značke in ustreznosti zgodovine dogodkov. Najpomembnejša pri združevanju navedenih kriterijev je ustreznost zgodovine dogodkov.

4.1.3.1.3.1.1 Ohranitev zgodovine dogodkov

Ohranitev zgodovine dogodkov
- Varna povezava med zapisom in zgodovino dogodkov
- Zaščita pred spremembo in brisanjem
- Arhiviranje, restavracija zgodovine dogodkov

Zgodovino dogodkov je treba hraniti vsaj toliko časa, kolikor dolgo se hranijo elektronski zapisi, ki so predmet zgodovine dogodkov. Zgodovino dogodkov mora biti možno pregledovati, kopirati ter elektronsko prenašati.

Za ustreznost zgodovine dogodkov mora biti zagotovljena varna povezava med zgodovino dogodkov in zapisom, ki je predmet zgodovine. Ta povezava se mora ohranjati skozi celotno dobo hranjenja zapisov in zgodovine (Deitz, 2001, str. 48).

Zgodovina dogodkov je elektronski zapis, zato jo moramo primerno zaščititi pred spremembami ali brisanjem. S primernim arhiviranjem in postopkom restavracije zgodovine dogodkov zagotovimo ustreznost hranjenja.

4.1.3.1.3.1.2 Časovna značka

Časovna značka
- Možnost spremembe
- Periodična verifikacija

Za točnost in ustreznost zgodovine dogodkov je treba zagotoviti, da je nastavitev časovne značke (datum in čas) izven uporabnikovega nadzora. Torej, da je uporabnik ne more naključno ali namerno spremeniti.

Za ustreznost časovne značke je primerno, da se le-ta periodično preverja oziroma verificira. Ena od možnosti je, da se sinhronizacija avtomatsko izvaja preko strežnika, druga, da jo preverja uporabnik (Guidance for Industry, 21 CFR Part11; Electronic Records; Electronic Signatures, Time Stamps, 2002).

4.1.3.1.3.1.3 Ustreznost zgodovine dogodkov

Ustreznost zgodovine dogodkov
- **Možnost izklopa zgodovine dogodkov**
  - Operater
  - Administrator
- **Dogodki v zapisu zgodovine**
  - Kreacija
  - Sprememba
  - Brisanje
- **Prikaz zgodovine dogodkov**
  - Elektronski
  - Izpis
  - Prenašanje v elektronski obliki
- **Parametri**
  - Tip sistema
  - Namen spremembe
  - **Industrijski parametri**
    - Datum in čas
    - Tiskano ime posameznika
    - Staro in novo stanje

Za zagotovitev ustreznosti računalniško ustvarjene zgodovine dogodkov, le-te ne sme biti možno izklopiti.

Zapisati se morajo vsi dogodki, ki so povezani z elektronskimi zapisi, ki so predmet vsebine zgodovine dogodkov. To so nastanek (kreacija), sprememba ali brisanje zapisa.

Za pregledovanje zgodovine dogodkov mora biti na voljo ustrezen prikaz, ki je lahko elektronski ali izpisan na papirju. Tudi zgodovino dogodkov mora biti ravno tako kot druge elektronske zapise mogoče prenašati v elektronski obliki.

Parametri v zgodovini dogodkov morajo biti: časovna značka, uporabnik, staro in novo stanje za industrijske sisteme ter za laboratorijske sisteme tudi namen spremembe. S kriterijem "tip sistema" določimo, ali je sistem industrijski ali laboratorijski, in na podlagi tega sprejmemo ali izločimo kriterij "namen spremembe" (Keatley, 1999, str. 82).

4.1.3.1.4 Sistemska dokumentacija

Sistemska dokumentacija
- Nadzor nad uporabo in vzdrževanjem - kontrola dostopa
- **Kontrola sprememb**

Distribucija, dostop in uporaba sistemske dokumentacije za uporabo in vzdrževanje morajo biti primerno nadzorovani ne glede na obliko sistemske dokumentacije (papirna ali elektronska) (Computerized Systems Used in Clinical Trials, Giudance for Industry, 1999, str. 8).

Dostop do zaupne dokumentacije, npr. navodil za modifikacijo sistemskih zaščit, je lahko dovoljen le pooblaščenim posameznikom.

Tudi sistemsko dokumentacijo moramo nadzorovati s kontrolo sprememb.

4.1.3.1.4.1 Kontrola sprememb sistemske dokumentacije

Kontrola sprememb
- Kontrola verzij dokumentov
- Pretečena dokumentacija - odstranitev, arhiviranje
- **Zgodovina dogodkov**
  - Možnost pregledovanja, inšpekcije
  - Ohranitev povezave
  - Povezava zgodovine dogodkov z dokumentacijo
  - **Elementi zgodovine dogodkov**
    - Datum in čas
    - Tiskano ime posameznika
    - Staro in novo stanje

Vsaka sprememba sistema in sistemske dokumentacije mora biti dokumentirana s postopki za kontrolo sprememb.

Kontrolo sprememb zagotavljamo s kontrolo verzij dokumentov, ustreznim arhiviranjem, odstranitvijo dokumentov in zagotovitvijo zgodovine dogodkov.

Zgodovina dogodkov mora spet vsebovati ustrezne parametre (datum, čas, ime, staro stanje, novo stanje), zagotovljena mora biti povezava in ohranitev zgodovine dogodkov z dokumentacijo, ki je predmet zgodovine. Zgodovino dogodkov mora biti možno enako kot vse elektronske zapise izpisati, kopirati in prenašati.

4.1.3.2 Elektronski podpisi

Elektronski podpisi
- **Validacija elektronskega podpisa**
- **Prikaz podpisa**
- **Povezava podpis-zapis**
- **Zahteve in nadzor podpisa**

Skladni z regulativo morajo biti poleg elektronskih zapisov tudi elektronski podpisi. Elektronski podpis je mehanizem, s katerim izvedemo aktivnost, povezano z elektronskim zapisom (pregled, odobritev, verifikacija ipd.).

Za ustreznost z regulativo morajo biti elektronski podpisi ustrezno validirani, prikaz podpisa mora ustrezati zahtevam, zagotovljena mora biti neločljiva povezava med elektronskim podpisom in elektronskim zapisom, zadoščeno mora biti tudi določenim zahtevam in nadzoru podpisa.

4.1.3.2.1 Validacija elektronskega podpisa

Validacija elektronskega podpisa
- Validacija izvedbe in prikaza podpisa
- Validacija povezave podpis-zapis
- Validacija zahtev in nadzora podpisa

Validacija elektronskega podpisa pomeni, da moramo preveriti ustreznost izvedbe in prikaza podpisa, ustreznost povezave med elektronskim zapisom in elektronskim podpisom ter preveriti mehanizme glede zahtev in nadzora podpisa.

Pomembno je, da vsa testiranja in verifikacije ustrezno dokumentiramo.

4.1.3.2.2 Prikaz podpisa

Prikaz podpisa
- **Vsebina prikaza**
  - Datum in čas
  - Tiskano ime posameznika
  - Namen podpisa
- **Zaščita prikaza**
  - Dostop do prikaza podpisa
  - Zgodovina dogodkov pri spremembah prikaza
  - Nadzor prikaza podpisa

Prikaz podpisa mora vsebinsko ustrezati in biti primerno zaščiten.

Vsebina elektronskega podpisa mora biti sestavljena iz časovne značke (datum in čas), tiskanega imena posameznika, ki je izvedel podpis, in namena podpisa (pregledal, overil ipd.). Oseba, ki izvaja podpis, ne sme biti tudi tista, ki nadzoruje časovno značko oziroma ima možnost njenega spreminjanja (Brazier, 2001, str. 287).

Dostop do prikaza podpisa mora biti zaščiten tako, da ga ni možno enostavno brisati, kopirati ali kako drugače prenašati. V primeru spremembe prikaza podpisa mora biti zagotovljena ustrezna zgodovina dogodkov. Prikaz podpisa mora imeti enak nadzor kot vsi ostali pomembni elektronski zapisi.

4.1.3.2.3 Povezava podpis-zapis

Povezava podpis-zapis
- Varnost povezave
- Ukrepi za ohranitev povezave

Izveden elektronski podpis mora biti varno povezan z elektronskim zapisom, ki je podpisan. Ta povezava se mora ohranjati skozi celotno dobo hranjenja zapisov. Ukrepi za ohranitev povezave morajo biti zanesljivi (zaščita, zgodovina dogodkov).

4.1.3.2.4 Zahteve in nadzor podpisa

Zahteve in nadzor podpisa
- **Enkratnost elektronskega podpisa**
- **Nadzor identifikacijskih kod in gesel**
- **Nebiometrični podpis**

Zagotovljena mora biti enkratnost elektronskega podpisa. Še posebej pozorni moramo biti v primerih, ko ima več uporabnikov enako ime in priimek ali ko se spremeni priimek osebe, ki izvaja elektronski podpis, npr. ob poroki.

Za ustreznost elektronskega podpisa je treba zagotoviti ustrezen nadzor uporabniških imen (identifikacijskih kod) in gesel, ki sta osnovni sestavini izvedbe elektronskega podpisa.

Nebiometrični podpis je tisti, pri katerem za overitev posameznika pri izvajanju podpisa niso uporabljene biometrične metode (npr. prstni odtis, zenica očesa, prepoznavanje glasu), temveč so uporabljeni mehanizmi, ki ne temeljijo na biometriki. Primer nebiometričnega podpisa je uporaba uporabniškega imena in gesla. Pri tem lahko uporabljamo tudi različne kartice, žetone, naprave, ki so lahko nosilci informacij o uporabniških imenih in geslih (Brazier, 2001, str. 287).

4.1.3.2.4.1 Enkratnost elektronskega podpisa

Enkratnost elektronskega podpisa
- Enak elektronski podpis
- Poznejša dodelitev enakega elektronskega podpisa
- Ustrezen dokumentiran nadzor dodelitve elektronskega podpisa

Pri elektronskem podpisu mora biti zagotovljeno, da niti dva uporabnika nimata enakega. Še več, tudi poznejša dodelitev elektronskega podpisa nekomu drugemu ni dovoljena.

Za zagotovitev enkratnosti elektronskega podpisa je treba imeti vzpostavljen ustrezen dokumentiran nadzor dodeljevanja elektronskih podpisov.

4.1.3.2.4.2 Nadzor identifikacijskih kod in gesel

Nadzor identifikacijskih kod in gesel
- **Zaščita in integriteta**
- **Kartice, žetoni, naprave**
- **Nepooblaščen dostop**

V okviru izvedbe sistema je treba zagotoviti ustrezen nadzor uporabniških imen in gesel. To zagotovimo s primerno zaščito, ustreznimi napravami, ki jih tudi primerno testiramo (kartice, žetoni ipd.), in s primernimi mehanizmi za odkrivanje in ukrepanje pri poskusih nepooblaščenega dostopa do sistema (Brazier, 2001, str. 287).

4.1.3.2.4.2.1 Zaščita in integriteta

Zaščita in integriteta
- Enkratnost identifikacijskih kod
- Periodično pregledovanje
- Časovni potek gesel

Zagotovljena mora biti enkratnost uporabniških imen, tako da sistem ne dovoli dveh enakih. Če sistem tega ne zagotavlja, je treba uvesti potrebne procedure za zagotovitev enkratnosti uporabniških imen, kar zagotavlja enkratnost elektronskega podpisa.

Uporabniške račune je treba periodično pregledovati glede na veljavnost, ustreznost dodeljenih pravic in poskuse nepooblaščenih dostopov.

Časovni potek gesel je pomemben za ustrezno zaščito in enkratnost podpisa. Uporabniki morajo biti prisiljeni, da časovno revidirajo gesla (običajno na 90 dni). Lahko si sistem tudi zapomni vsa prejšnja gesla in ne dovoli ponovne uporabe enakih gesel.

4.1.3.2.4.2.2 Kartice, žetoni, naprave

Kartice, žetoni, naprave
- Postopki za izdajo
- Začetno testiranje
- Periodično testiranje

Kartice, žetone ali naprave, ki nosijo informacijo o uporabniškem imenu ali geslu, je treba testirati. Testiranja izvedemo in dokumentiramo pred uporabo in nato periodično v določenem časovnem intervalu (npr. enkrat na leto). Testiramo jih glede na funkcijo delovanja in preverimo, da niso bile spremenjene na neavtoriziran način.

4.1.3.2.4.2.3 Nepooblaščen dostop

Nepooblaščen dostop
- Odkrivanje
- Poročanje in ukrepanje
- Avtomatska blokada

Poskuse nepooblaščenega dostopa do sistema je treba odkrivati in o tem poročati vodstvu ter ustrezno ukrepati. V primeru večkratnih poskusov nepooblaščenega dostopa do sistema lahko zagotovimo avtomatsko blokado uporabnika za določen čas ali dokler administrator ne sprosti blokade.

4.1.3.2.4.3 Nebiometrični podpis

Nebiometrični podpis
- **Administracija in izvedba elektronskega podpisa**
- **Postopki in procedure**
- **Neprekinjen dostop**

V nadaljevanju sta opisana način izvedbe in administracija nebiometričnega elektronskega podpisa.

Določeni morajo biti postopki oziroma procedure za uporabo sistema in način izvajanja nebiometričnega elektronskega podpisa.

Pri neprekinjenem dostopu je možno pri zaporednih izvedbah podpisov v nadaljevanju uporabiti samo en del elektronskega podpisa, ki je zaupen (geslo). Prvi podpis je treba izvesti z obema deloma elektronskega podpisa, uporabniškim imenom in geslom (E-Records Technology Gap is Closing, But Implementation Poses Challenges, 2000, str. 21).

4.1.3.2.4.3.1 Administracija in izvedba elektronskega podpisa

Administracija in izvedba
- Zaščita datotek z vsebino podpisa
- Zaščita gesla pred administratorjem
- Minimalna dolžina gesla

Informacije z vsebino podpisa morajo biti na sistemu ustrezno zaščitene. Geslo mora biti zaščiteno tudi pred administratorjem sistema, določena mora biti najmanjša dolžina gesla (npr. 6 znakov).

4.1.3.2.4.3.2 Postopki, procedure

Postopki, procedure
- So napisani
- Izobraženost
- Se izvajajo

Če na sistemu ni avtomatskih kontrol za dostop (avtomatska odjava, ohranjevalnik zaslona), morajo biti predpisani postopki oziroma procedure za uporabo sistema. Takšni postopki opredeljujejo uporabo sistema pri prekinjeni uporabi sistema (npr. če zapustimo prostor, kjer je sistem, se je treba odjaviti s sistema).

Postopke je treba določiti v primeru, ko avtomatske kontrole ne obstajajo. Če so postopki predpisani, je bistveno, da so vsi uporabniki o njih izobraženi in da se postopki ustrezno izvajajo.

4.1.3.2.4.3.2 Neprekinjen dostop

Neprekinjen dostop
- Je definiran
- Uporabniki so izobraženi
- **Uporaba**
  - Oba dela podpisa ob prvem podpisu - prijava
  - Samo geslo ob neprekinjenem dostopu
  - **Tehnične kontrole**
    - Ohranjevalnik zaslona
    - Avtomatska odjava
    - Nivo operacijskega sistema in aplikacije

Če je na sistemu določen in uporabljen neprekinjen dostop, morajo biti uporabniki o tem izobraženi.

Kadar uporabniki med enkratnim, sočasnim dostopom do sistema izvajajo podpis večkrat, morajo prvič (lahko je to prijava, če se uporablja enak mehanizem za prijavo kot za elektronski podpis) uporabiti oba dela elektronskega podpisa (uporabniško ime in geslo), za vsak nadaljnji podpis pa lahko samo tisti del podpisa, ki je zaseben (geslo).

Če dostop uporabnika do sistema ni enkraten in sočasen, mora za vsak podpis uporabiti oba dela elektronskega podpisa.

Izvedba prekinjenega in neprekinjenega dostopa je lahko različna, lahko je to, na primer, ohranjevalnik zaslona ali avtomatska odjava iz sistema.

Tehnični kontroli za nebiometrični elektronski podpis sta: ohranjevalnik zaslona in avtomatska odjava. Kontrola je lahko izvedena na ravni operacijskega sistema, na ravni uporabniškega programa ali obeh.

4.2 Vrednosti kriterijev

Na osnovi podanih kriterijev so bile določene zaloge vrednosti za posamezni kriterij. Vsakemu kriteriju je treba določiti vsaj negativno in pozitivno vrednost, priporoča pa se, da določimo tudi vmesno vrednost. Težiti moramo k temu, da kriterijev ni preveč.

Običajna zaloga vrednosti je: *ne, delno, da* ali *ne ustreza, delno ustreza* in *ustreza*. Merske lestvice so običajno urejene od slabih proti boljšim vrednostim. Pri uporabi programskega orodja DEXi je to dobrodošlo, ker pri kontroli konsistentnosti odločitvenih pravil to lahko bistveno pospeši postopek zajemanja funkcij koristnosti (Bohanec, Rajkovič, 1995, str. 432). DEXi v tem primeru namreč že sam predlaga določene vrednosti funkcij koristnosti.

Za vse kriterije so zaloge vrednosti izpisane v dodatku.

Na vseh sistemih, ki jih ocenjujemo, ne pridejo v poštev vsi kriteriji, po katerih ocenjujemo. Na primer, na preprostih strojih v proizvodnji niso izvedeni elektronski podpisi, temveč le elektronski zapisi (npr. parametri za delovanje stroja). Zato smo pri kriterijih za skladnost z regulativo dodali še izločilni kriterij "klasifikacija sistema", s

katerim na podlagi vrste sistema izločimo določene kriterije, da ne vplivajo na končno oceno.

Kriterij "klasifikacija sistema" lahko zavzame vrednosti: *zapisi in podpisi*, *samo zapisi* in *ni zapisov ni podpisov*. Glede na to s pomočjo funkcije koristnosti ustrezno upoštevamo oba pripadajoča agregirana kriterija "elektronski zapisi" in "elektronski podpisi". Na primer, v funkciji koristnosti za skladnost sistema imamo določene naslednje vrednosti kriterijev:

elektronski zapisi = skladni
elektronski podpisi = neskladni
klasifikacija sistema = samo zapisi

iz tega sledi, da je

skladnost z regulativo = skladen

Čeprav smo pri oceni elektronskih podpisov neskladni, nam kriterij "klasifikacija sistema" pove, da so na sistemu izvedeni le zapisi, zato kriterij "elektronski podpisi" na končno oceno skladnosti ne sme vplivati.

4.3 Izdelava drevesa kriterijev

DEXi, s katerim je bil izdelan prototip drevesa kriterijev, omogoča strukturiranje problema v drevesno strukturo. Vozlišča drevesa so sestavljeni (agregirani) kriteriji, listi pa bazični kriteriji.
Za vse kriterije smo podali zaloge vrednosti, ki jih lahko zavzamejo, funkcije koristnosti in pravila, kako se iz kombinacij vrednosti podrejenih kriterijev izračuna vrednost agregiranega.

V naši raziskavi je drevo zgrajeno iz 183 kriterijev, od tega je 120 osnovnih.

4.3.1 Drevo kriterijev

Na osnovi vseh podanih kriterijev in načina združevanja kriterijev v drevesu je bilo izdelano naslednje drevo:

Kritičnost računalniškega sistema
├ **GXP kritičnost sistema**
│ ├ Vpliv na kvaliteto izdelka
│ └ Odprtost sistema
└ **Skladnost z regulativo**
  ├ Klasifikacija sistema
  ├ **Elektronski zapisi**
  │ ├ **Validacija elektronskih zapisov**
  │ │ ├ **Validacija glede na industrijske standarde**
  │ │ │ ├ **Specifikacije**
  │ │ │ │ ├ Zahteve uporabnika
  │ │ │ │ ├ Ocena dobavitelja
  │ │ │ │ └ Programska in strojna specifikacija

- **Kvalifikacija**
  - Kvalifikacija načrtovanja - DQ
  - Kvalifikacija montaže - IQ
  - Kvalifikacija obratovanja - OQ
  - Kvalifikacija delovanja - PQ
- **Postopki**
  - Validacijski protokol
  - Poročilo o validaciji
  - **Sistemski splošni postopki**
    - Delovanje sistema
    - **Administracija sistema**
      - Periodični pregled sistema
      - Arhiviranje, varnostno kopiranje, restavracija sistema in zapisov
      - Konfiguracija sistema in zaščit
- **Izobraževanje**
  - Uporabniki, sistemski administratorji
  - Razvijalci, interni presojevalci, zunanji
  - Dokumentiranost

Validacija glede na regulativo o elektronskih podpisih in zapisih

- **Neveljavni, spremenjeni zapisi**
  - Neveljavni vnosi
  - Sposobnost razlikovanja spremenjenih zapisov
  - Test razlikovanja spremenjenih zapisov
- **Generiranje kopij elektronskih zapisov**
  - Prikaz v elektronski obliki
  - Prikaz v obliki izpisa
  - Prenašanje v elektronski obliki
- **Ostale zahteve za validacijo elektronskih zapisov**
  - Zgodovina dogodkov
  - Zaporedje dogodkov
  - **Zaščita zapisov in dostopa**
    - Testiranje dostopa in avtorizacij
    - Testiranje arhiviranja in restavracije zapisov
    - Test naprav, ki so vir vhodnih podatkov

Zaščita

- **Nadzor**
  - **Pregledi zapisov**
    - Uporabnika
    - Administratorja
    - Upravljanja kakovosti
  - **Zaporedje dogodkov**
    - Vsiljeno zaporedje dogodkov
    - Avtomatski mehanizem sekvenc
  - **Preverjanje naprav**
    - Preverjanje vira vhodnih podatkov
    - Periodično testiranje naprav
- **Zaščita zapisov**
  - Arhiviranje
  - **Restavracija**
    - Glede na čas
    - Glede na celovitost podatkov
    - Periodično testiranje restavracije
  - **Zaščita zapisov glede na lokacijo**
    - Na sistemu
    - Na arhivskem mediju
    - Perioda arhiviranja

- **Zaščita dostopa**
  - Fizični dostop
  - Arhiv konfiguracije zaščit
  - **Logični dostop**
    - **Avtorizacije**
      - Način avtorizacije dostopa
      - Preverjanje avtorizacije za izvedbo podpisa
      - Preverjanje avtorizacije pri uporabi sistema
    - **Dostop do sistema**
      - Operacijski sistem
      - Avtomatska odjava
      - **Aplikacija**
        - Večnivojski dostop
        - Prikritost gesel, minimalna dolžina gesel
        - **Uporabniški računi**
          - Potek uporabniškega računa
          - Periodično pregledovanje računov
          - Detekcija nepooblaščenih poizkusov dostopa
- **Zgodovina dogodkov**
  - Ročna zgodovina dogodkov
  - **Računalniško generirana zgodovina dogodkov**
    - **Ohranitev zgodovine dogodkov**
      - Varna povezava med zapisom in zgodovino dogodkov
      - Zaščita pred spremembo in brisanjem
      - Arhiviranje, restavracija zgodovine dogodkov
    - **Časovna značka**
      - Možnost spremembe
      - Periodična verifikacija
    - **Ustreznost zgodovine dogodkov**
      - **Možnost izklopa zgodovine dogodkov**
        - Operater
        - Administrator
      - **Dogodki v zapisu zgodovine**
        - Kreacija
        - Sprememba
        - Brisanje
      - **Prikaz zgodovine dogodkov**
        - Elektronski
        - Izpis
        - Prenašanje v elektronski obliki
      - **Parametri**
        - Tip sistema
        - Namen spremembe
        - **Industrijski parametri**
          - Datum in čas
          - Tiskano ime posameznika
          - Staro in novo stanje
- **Sistemska dokumentacija**
  - Nadzor nad uporabo in vzdrževanjem - kontrola dostopa
  - **Kontrola sprememb**
    - Kontrola verzij dokumentov
    - Pretečena dokumentacija - odstranitev, arhiviranje
    - **Zgodovina dogodkov**
      - Možnost pregledovanja, inšpekcije
      - Ohranitev povezave
      - Povezava zgodovine dogodkov z dokumentacijo

- **Elementi zgodovine dogodkov**
  - Datum in čas
  - Tiskano ime posameznika
  - Staro in novo stanje
- **Elektronski podpisi**
  - **Validacija elektronskega podpisa**
    - Validacija izvedbe in prikaza podpisa
    - Validacija povezave podpis/zapis
    - Validacija zahtev in nadzora podpisa
  - **Prikaz podpisa**
    - **Vsebina prikaza**
      - Datum in čas
      - Tiskano ime posameznika
      - Namen podpisa
    - **Zaščita prikaza**
      - Dostop do prikaza podpisa
      - Zgodovina dogodkov pri spremembah prikaza
      - Nadzor prikaza podpisa
  - **Povezava podpis/zapis**
    - Varnost povezave
    - Ukrepi za ohranitev povezave
  - **Zahteve in nadzor podpisa**
    - **Enkratnost elektronskega podpisa**
      - Enak elektronski podpis
      - Kasnejša dodelitev enakega elektronskega podpisa
      - Ustrezen dokumentiran nadzor dodelitve elektronskega podpisa
    - **Nadzor identifikacijskih kod in gesel**
      - **Zaščita in integriteta**
        - Enkratnost identifikacijskih kod
        - Periodično pregledovanje
        - Časovni potek gesel
      - **Kartice, žetoni, naprave**
        - Postopki za izdajo
        - Začetno testiranje
        - Periodično testiranje
      - **Nepooblaščen dostop**
        - Odkrivanje
        - Poročanje in ukrepanje
        - Avtomatska blokada
    - **Nebiometrični podpis**
      - **Administracija in izvedba elektronskega podpisa**
        - Zaščita datotek z vsebino podpisa
        - Zaščita gesla pred administratorjem
        - Minimalna dolžina gesla
      - **Postopki, procedure**
        - So napisani
        - Izobraženost
        - Se izvajajo
      - **Neprekinjen dostop**
        - Je definiran
        - Uporabniki so izobraženi
        - **Uporaba**
          - Obe komponenti podpisa ob prvem podpisu - prijava
          - Samo geslo ob neprekinjenem dostopu
          - **Tehnične kontrole**
            - Ohranjevalnik zaslona
            - Avtomatska odjava
            - Nivo operacijskega sistema in aplikacije

4.3.2 Osnovna odločitvena pravila

Kot smo določili že v poglavju 2.4, so funkcije koristnosti pri programskem orodju DEXi predstavljene s preprostimi odločitvenimi pravili tipa "če-potem" (IF-THEN).

Določimo jih v obliki tabele. Postopek določitve odločitvenih pravil s programskim orodjem DEXi je zelo preprost. Za posamezen sestavljen kriterij DEXi že pripravi celotno tabelo možnih kombinacij vrednosti odvisnih spremenljivk. Izpolnimo zadnji stolpec v tabeli kombinacij, v katerem podamo vrednost sestavljenega kriterija za posamezno kombinacijo vrednosti odvisnih spremenljivk (podrejenih kriterijev). Pri tem nas DEXi sproti opozarja na morebitne nekonsistentnosti oziroma na podlagi do takrat že podanih pravil sam predlaga določene vrednosti v tabeli.

Za naš model na tem mestu podajamo funkcijo koristnosti za najvišji kriterij "kritičnost računalniškega sistema". Vse ostale tabele so prikazane v dodatku.

Iz tabele 1 je razvidno, da so vsi sistemi, ki so popolnoma skladni z regulativo, nekritični.

Pri precej skladnih sistemih je pri veliki "GXP kritičnosti" sistem manj kritičen, sicer je nekritičen.

Sistemi, ki so srednje skladni s predpisi, so lahko precej kritični, če je "GXP kritičnost" sistema velika, srednje kritični, ko je "GXP kritičnost" srednja, in manj kritični, ko je "GXP kritičnost" majhna.

V primeru manj skladnih sistemov je sistem precej kritičen za veliko "GXP kritičnost", srednje kritičen za srednjo "GXP kritičnost" in manj kritičen za majhno "GXP kritičnost" sistema.

Pri neskladnih sistemih je sistem zelo kritičen za veliko, precej kritičen za srednjo in srednje kritičen za majhno "GXP kritičnost" sistema.

V praksi pri obstoječih računalniških sistemih pričakujemo največ sistemov, ki so neskladni, manj ali srednje skladni s predpisi in imajo veliko ali srednjo »GXP kritičnost«. To pomeni, da so po našem modelu zelo, precej ali srednje kritični.

Tabela 1 - Funkcija koristnosti za najvišji kriterij "kritičnost računalniškega sistema"

"GXP kritičnost" sistema	Skladnost z regulativo	Kritičnost računalniškega sistema
velika	neskladen	zelo kritičen
velika	manj skladen	precej kritičen
velika	srednje skladen	srednje kritičen
velika	precej skladen	manj kritičen
velika	popolno skladen	nekritičen
srednja	neskladen	precej kritičen
srednja	manj skladen	srednje kritičen
srednja	srednje skladen	manj kritičen
srednja	precej skladen	nekritičen
srednja	popolno skladen	nekritičen
majhna	neskladen	srednje kritičen
majhna	manj skladen	manj kritičen
majhna	srednje skladen	nekritičen
majhna	precej skladen	nekritičen
majhna	popolno skladen	nekritičen

Vir: Lastna ocena.

5. Kritična analiza in testiranje odločitvenega modela

Če želimo preveriti ustrezno delovanje modela, moramo poskusno oceniti nekaj računalniških sistemov in preveriti ustreznost njihovega delovanja. Pri analizi in testiranju odločitvenega modela moramo upoštevati:

– delovanje samega modela sistema,
– ustreznost drevesne strukture kriterijev in funkcij koristnosti,
– opis in rezultate vrednotenja variant računalniških sistemov.

5.1 Delovanje modela sistema

Pri preverjanju delovanja samega sistema ugotavljamo, ali sistem posamezne kriterije na podlagi določenih odločitvenih pravil pravilno združuje v višje kriterije. Sistem mora na podlagi določenih vrednosti kriterijev na nižji ravni pravilno prikazati vrednost višjega kriterija. Glede na to, da smo uporabili že mnogokrat preizkušeno orodje (DEXi), pri tem preizkusu nismo pričakovali nobenih posebnosti oziroma odstopov.

Za nekaj pomembnejših kriterijev smo vzorčno preverili ustreznost združevanja kriterijev v višje kriterije.

Celoten izpis vrednotenja variant je podan v dodatku.

Pri preverjanju nismo ugotovili nobenih odstopov. Sistem združuje nižje kriterije v višje na podlagi določenih odločitvenih pravil.

5.2 Ustreznost drevesne strukture in funkcij koristnosti

Ustreznost drevesne strukture in odločitvenih funkcij (funkcij koristnosti) smo preverili s podrobnim pregledom drevesne strukture vseh odločitvenih funkcij in razmerja uteži pri posamezni odločitveni funkciji.

Pri oceni je sodelovala odgovorna oseba za skladnost računalniških sistemov z regulativo o elektronskih podpisih in zapisih v podjetju.

Nabor osnovnih kriterijev za oceno smo izbrali v okviru priprav na ocenjevanje vseh sistemov. Določili smo jih na podlagi študija regulative, viharjenja možganov, raznih posvetovanj strokovnjakov, obiskov konferenc o elektronskih zapisih in podpisih ter dokončno izbrali v okviru skupine za informacijske sisteme v podjetju.

Na podlagi navedenega menimo, da je nabor osnovnih kriterijev ustrezen, zato nas na tem mestu bolj zanima ustreznost združevanja osnovnih kriterijev v višje kriterije. Preverjamo in utemeljujemo torej osnovne odločitvene funkcije (pravila, uteži) in samo strukturo, kako se nižji kriteriji združujejo v višje kriterije.

Pri oceni in analizi ustreznosti modela nam je programsko orodje DEXi v veliko pomoč, ker nam omogoča različne oblike izpisov modela, na podlagi katerih lahko ocenjujemo ustreznost samega modela. DEXi omogoča izpis drevesa kriterijev, zalog vrednosti kriterijev, opisa zalog vrednosti, tabele odločitvenih pravil, uteži, rezultatov vrednotenja variant in grafikonov.

Drevesna struktura je bila podana že v poglavju 4.3.1 in je tudi del dodatka, tudi vse odločitvene funkcije so izpisane v dodatku, zato jih tu ne navajamo še enkrat, temveč jih samo utemeljujemo. Utemeljujemo nekaj najbolj pomembnih kriterijev oziroma tiste, ki najbolj vplivajo na končno oceno sistema.

Kritičnost računalniškega sistema

Odločitvena funkcija za ta najvišji kriterij je bila predstavljena že v poglavju 4.3.2. Tu je bolj pomemben kriterij skladnosti, saj nas v primeru skladnosti načeloma "GXP kritičnost" sploh ne zanima, saj smo tako ali tako skladni z regulativo. V primeru neskladnosti to še vseeno ni tako kritično, če sistem ni oziroma je manj "GXP kritičen". Razdelitev uteži na 52 % za skladnost in 48 % za "GXP kritičnost" se zdi primerna.

"GXP kritičnost" sistema

"GXP kritičnost" sistema je rezultat vpliva na kakovost izdelka in odprtosti sistema. Kadar je vpliv sistema na kakovost izdelka velik, je v vsakem primeru "GXP kritičnost" velika in če je vpliv majhen, je "GXP kritičnost" majhna, ne glede na odprtost oziroma dostopnost do sistema. V primeru posrednega vpliva sistema na kakovost izdelka je kritičnost odvisna od odprtosti sistema. Najbolj (75 %) torej "GXP kritičnost" vpliva na kakovost izdelka.

Skladnost z regulativo

Regulativa določa kriterije in zahteve za elektronske zapise in elektronske podpise. Pri združevanju teh dveh kriterijev smo dodali še tretji, izločilni kriterij "klasifikacija sistema".

Na nekaterih sistemih elektronski podpisi niso uporabljeni in tako lahko s kriterijem "klasifikacija sistema" izločimo kriterij "elektronski podpisi". Na končno oceno skladnosti z regulativo v tem primeru vpliva le del poddrevesa za elektronske zapise.

Elektronski zapisi

Skladnost elektronskih zapisov z regulativo ocenjujemo na podlagi naslednjih kriterijev: "validacija elektronskih zapisov", "zaščita", "zgodovina dogodkov" in "sistemska dokumentacija".
Pomembnejši kriteriji so: "zaščita" (30 %), "validacija elektronskih zapisov" (25 %) in "zgodovina dogodkov" (24 %), malo manj pomemben je kriterij "sistemska dokumentacija" (21 %).

Že v sami regulativi (gl. poglavje 3.2.2.1) je poudarjeno, da je treba vzpostaviti procedure in mehanizme za zagotovitev pristnosti, celovitosti in, kjer je to primerno, zaupnosti elektronskih zapisov. Zato se zdi logično, da je kriterij "zaščita" eden najpomembnejših oziroma najbolj uteženih kriterijev.

Validacija elektronskih zapisov

Ločimo klasično validacijo glede na industrijske standarde, ki se uporablja v zadnjih nekaj letih, in validacijo glede na predpise o elektronskih zapisih in podpisih. Upoštevati je treba oba vidika, sicer sistem ni ustrezno validiran. V naši odločitveni funkciji imata oba kriterija enako težo (50 %).

Validacija sistema glede na industrijske standarde

Validacija sistema zajema celoten življenjski cikel sistema, od uporabniških zahtev, določitve specifikacij do izvedbe sistema, izvedbe kvalifikacij, izdelavo potrebnih postopkov in izobraževanja vseh, ki delajo s sistemom.

Glede na odločitveno funkcijo sta najbolj utežena kriterija "specifikacije" (36 %) in "kvalifikacije" (36 %) ter nekoliko manj "postopki" (18 %) in "izobraževanje" (10 %). To se zdi logično, saj sta ustreznost specifikacij in ustreznost kvalifikacij osnovna pogoja za ustreznost in validacijo računalniškega sistema.

Validacija sistema glede na regulativo o elektronskih podpisih in zapisih

Najpomembnejše pri validaciji sistema glede na regulativo o elektronskih zapisih in podpisih je testiranje neveljavnih in spremenjenih zapisov (52 %). Pomembno vlogo ima še testiranje zmožnosti ustvarjanja kopij elektronskih zapisov (24 %) in ostale zahteve (24 %) , ki vključujejo testiranje zgodovine dogodkov, zaporedja dogodkov, zaščite zapisov in dostopa.

Taka razporeditev uteži je primerna zaradi zagotavljanja pristnosti, celovitosti in zaupnosti elektronskih zapisov. Z validacijo ustrezno pokažemo, da sistem prepoznava in preprečuje neveljavne vnose ter prepoznava spremenjene zapise.

Zaščita

Kriterija "zaščita zapisov" in "zaščita dostopa" sta nekoliko bolj utežena (38 % in 37%) kot kriterij "nadzor" (25 %). Zaščita zapisov vsebuje arhiviranje, restavracijo in zaščito zapisov glede na lokacijo. Zaščita dostopa pomeni fizični in logični dostop do sistema. Nadzor nad elektronskimi zapisi zajema pregledovanje zapisov, zaporedje dogodkov in preverjanje naprav oziroma vira vhodnih podatkov.

Pri zaščiti dostopa ima nekoliko večjo utež kriterij "logični dostop" (63 %) kot kriterija "arhiv konfiguracije zaščit (25 %) in "fizični dostop" (12 %).

Zaščita elektronskih zapisov je eden najvplivnejših kriterijev za končno oceno kritičnosti računalniških sistemov. Povsem logično je, da je temeljni pogoj za ustrezne elektronske zapise ustrezna zaščita tako na sistemu kot na arhivskem mediju.

Zgodovina dogodkov

V regulativi je zgodovina dogodkov za elektronske zapise zahtevana. Če sistem ne omogoča izdelave zgodovine dogodkov računalniško (avtomatsko), jo je treba zagotoviti ročno. To izvedemo z ustreznimi postopki, s katerimi ročno zapišemo vse spremembe elektronskih zapisov.

Ker vsi računalniški sistemi zgodovine dogodkov ne zagotavljajo avtomatsko, jo moramo ponekod zagotoviti s postopki oziroma procedurami. Na primer, nastavitveni parametri na nekem proizvodnem stroju so v obliki elektronskih zapisov in lahko vplivajo na kakovost izdelka. V primeru spremembe parametra se v samem sistemu ne zapišejo vsi podatki, ki so pomembni za zgodovino dogodkov (datum, čas, staro stanje, novo stanje, ime posameznika, ki je izvedel spremembo), zato je nujno potrebno zagotoviti ročno vpisovanje sprememb.

Regulativa zahteva možnost rekonstrukcije vseh zapisov, pomembnih za dobre prakse, za vsak trenutek v preteklosti. Primeri takih zapisov so: tehnološki parametri, strojni parametri, histografija fizikalnih parametrov, proizvodna poročila, konfiguracija zaščit. Tudi zgodovina dogodkov je zapis, ki je s stališča dobrih praks pomemben, zato je treba njeno elektronsko obliko nadzorovati enako kot vse druge zapise, ki so pomembni za dobre prakse.

V našem drevesu smo enakovredno utežili kriterija "računalniško generirana zgodovina dogodkov" in "ročna zgodovina dogodkov" (50 %). Zgodovina dogodkov je pomemben kriterij in ima velik vpliv na končno oceno kritičnosti računalniškega sistema.

Ustreznost zgodovine dogodkov

Pri računalniško ustvarjeni zgodovini dogodkov ima največji vpliv kriterij "ustreznost zgodovine dogodkov" (52 %). Seveda je logično pričakovati, da mora biti računalniško izdelana zgodovina dogodkov ustrezna. Prvi nižji kriterij, ki najbolj vpliva na ustreznost zgodovine dogodkov, je "parametri" (35 %).

V okviru kriterijev za parametre je izločilni kriterij "tip sistema", ki lahko izloči kriterij "namen spremembe" pri parametrih za zgodovino dogodkov. Kriterij "namen spremembe" mora obstajati pri dobri laboratorijski praksi, ni pa zahtevan za dobro proizvodno prakso.

Če imamo torej laboratorijski sistem, je treba pri spremembi zapisa v zgodovini dogodkov opredeliti tudi namen oziroma vzrok spremembe.

Sistemska dokumentacija

Uveden mora biti ustrezen nadzor nad uporabo, vzdrževanjem in kontrolo sprememb sistemske dokumentacije. Sistemska dokumentacija je lahko v papirni ali elektronski obliki in ima lahko avtomatsko računalniško ustvarjeno zgodovino dogodkov ali ročno pripravljeno.

Kriterija "kontrola sprememb" in "nadzor nad uporabo in vzdrževanjem" imata enak vpliv na višji kriterij "sistemska dokumentacija".

Tudi kriterij "sistemska dokumentacija" vpliva na višji kriterij "elektronski zapisi", vendar nekoliko manj kot kriteriji "zaščita", "zgodovina dogodkov" ali "validacija elektronskih zapisov".

Elektronski podpisi

Praktično pomeni elektronski podpis pregled, odobritev ali overitev nekega elektronskega zapisa ali neke aktivnosti. Za elektronski podpis sta pomembna sama izvedba in prikaz ter seveda tudi povezava med zapisom in podpisom. Podpis se lahko izvede z biometričnimi (npr. prstni odtis, zenica očesa, prepoznavanje govora) ali z nebiometričnimi metodami (kombinacija uporabniškega imena in gesla).

Kriterij "elektronski podpisi" opredeljujejo naslednji nižji kriteriji: "validacija elektronskega podpisa", "prikaz podpisa", "povezava podpis-zapis" in "zahteve in nadzor podpisa". Največ vpliva ima kriterij "zahteve in nadzor podpisa" (31%), nekoliko manj ostali trije kriteriji (23 %).

Validacija elektronskega podpisa

Tako kot vse ostalo, je treba validirati tudi elektronski podpis, in sicer izvedbo in prikaz podpisa, povezavo med podpisom in zapisom ter zahteve za nadzor podpisa. Z validacijo dokumentirano zagotovimo ustreznost elektronskega podpisa. Kriterij "validacija elektronskega podpisa" ima pomemben vpliv (23 %) na višji kriterij "elektronski podpisi".

Prikaz podpisa

Za prikaz podpisa sta enako pomembna nižja kriterija "vsebina prikaza" in "zaščita prikaza". Vsak elektronski podpis mora biti ustrezno prikazan na elektronskem zapisu. Pomembno je, da se za prikaz podpisa ravno tako ustvarja zgodovina dogodkov, s katero lahko pregledujemo morebitne spremembe. Kriterij "prikaz podpisa" pomembno vpliva (23 %) na višji kriterij "elektronski podpisi".

Povezava podpis-zapis

Vsak podpis mora biti ustrezno povezan s podpisanim elektronskim zapisom. Zagotovljena mora biti varnost povezave in določeni ukrepi za ohranitev povezave. Kriterij "povezava podpis-zapis" je pomemben in ima precejšen vpliv (22 %) na višji kriterij "elektronski podpisi".

Zahteve in nadzor podpisa

Ta kriterij je določen z nižjimi kriteriji: "enkratnost elektronskega podpisa", "nadzor ID kod in gesel" in "nebiometrični podpis". V našem odločitvenem drevesu nismo upoštevali biometričnih metod za izvedbo elektronskega podpisa, ker praktično nikjer še niso v uporabi.

Na kriterij "zahteve in nadzor podpisa" najbolj vpliva kriterij "nadzor ID kod in gesel" (60 %). Kriterija "enkratnost podpisa" in "nebiometrični podpis" prispevata po 20 odstotkov k višjemu kriteriju.

Bistven za nadzor elektronskega podpisa, ki ga izvajamo s pomočjo uporabniških kod in gesel, je seveda nadzor le-teh.

5.3 Opis in rezultati vrednotenja variant

Ekspertna skupina je ocenila tri računalniške sisteme in jih primerjala med seboj. Skupina je bila sestavljena iz uporabnikov (lastnikov) sistema, strokovnjakov za zagotavljanje kakovosti (poznavanje regulative) in strokovnjakov za informacijsko tehnologijo (proizvodni inženiring ali dobavitelj sistema).

Ocenjevanje se je izvajalo po vprašalniku, ki vsebuje kriterije iz našega modela in je podan v dodatku. Na podlagi izvedenih ocen smo lahko osnovne kriterije vnesli v naš model.

5.3.1 Opis variant

Za boljše ovrednotenje modela smo izbrali variante računalniških sistemov približno enakega obsega (velikostnega razreda) z različnih področij v podjetju. Tri variante so opisane v naslednjih podpoglavjih.

5.3.1.1 Nadzorno-krmilni sistem v proizvodnji

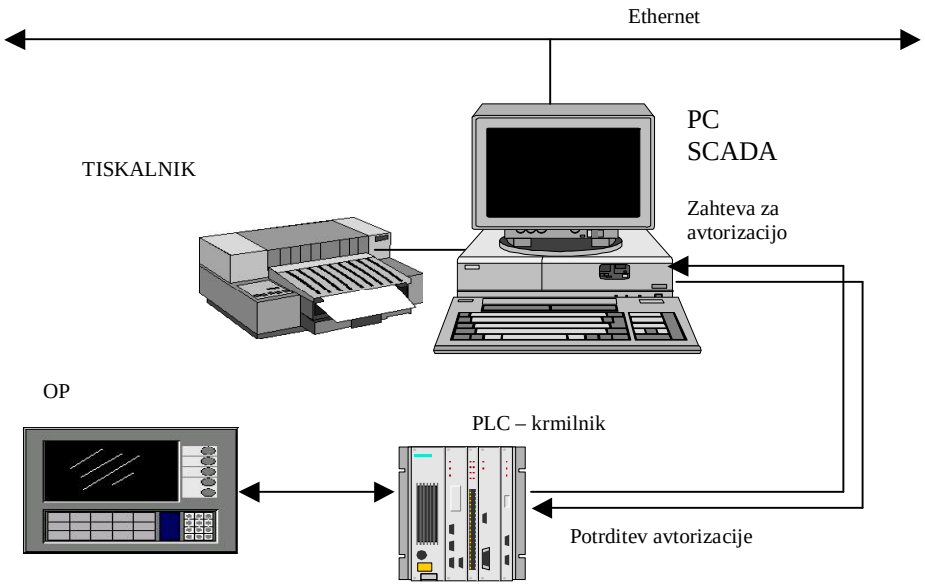
Nadzorno-krmilni sistem je sestavljen iz nadzornega dela in krmilnega dela sistema. Nadzorni del sistema (SCADA[23]) skrbi za nadzor in zbiranje podatkov, krmilni del sistema (PLC[24]) neposredno krmili opremo ali naprave (Avtomatika, 2001).

Slika 7 predstavlja klasični nadzorno-krmilni sistem. Operater upravlja krmilnik preko terminala (OP[25]). Avtorizacija operaterja se pri vnosu uporabniškega imena in gesla na spodnji ravni prenaša na nadzorni sistem, kjer se preverja ustreznost operaterja. Če je operater vnesel ustrezno uporabniško ime in geslo, se avtorizacija potrdi in krmilnik operaterju omogoči vodenje procesa.

[23]SCADA – Supervisory Control and Data Acquisistion
[24]PLC – Programmable Logical Controler
[25]OP – Operating Panel

Iz nadzornega sistema se lahko avtorizacija prenaša in preverja na višji, centralni ravni avtorizacij. Če je nadzorni sistem lokalnega značaja, je treba uporabniška imena in gesla vzdrževati lokalno na nadzornem sistemu.

Slika 7: Klasični krmilno-nadzorni sistem



Vir: Avtomatika, 2001.

Nadzorno-krmilni sistem je namenjen vodenju procesa in zbiranju podatkov o procesu. Proces poteka tako, da tehnik proizvodnje pred začetkom na nadzornem sistemu načrtuje proizvodni proces. Potem ga operater na proizvodni liniji izvede v skladu z načrtovanimi recepturami.

Načrtovanje poteka tako, da vpiše pomembne proizvodne podatke (naziv izdelka, šifra izdelka, kontrolna številka, delovni nalog, serija) in parametre (posoda, v kateri se izvaja proces) oziroma izbere že prej določeno recepturo za vodenje procesa.

Proces na sami strojni opremi vodijo operaterji po načrtovani recepturi.

Med procesom se shranjujejo vsi historični podatki fizikalnih veličin, morebitni alarmi, zgodovina dogodkov in posegi na sistemu.

Ob koncu procesa se izdela proizvodno poročilo in stiska na tiskalniku nato pa ga tehnik proizvodnje ročno podpiše.

Nadzorni sistem pokriva celotno proizvodno linijo, ki je sestavljena iz več strojev. Nekateri stroji so samostojni in imajo svoje nadzorno-krmilne sisteme. Tako naš sistem nekatere sisteme krmili neposredno, iz drugih sistemov, ki so samostojni, pa samo zbira podatke in jih shranjuje.

Programski paket omogoča vse pomembne funkcije: alarmiranje, histografijo, ekranske prikaze, načrtovanje, izdelavo receptur, vodenje procesa, konfiguracijo zaščit in zgodovino dogodkov.

Končno poročilo je izdelano v programu Excel, izpiše se na tiskalnik in shrani na trdem disku računalnika. Trdi disk računalnika se varnostno kopira in arhivira. Na tem sistemu so s stališča dobrih praks pomembni tile elektronski zapisi:

- proizvodna poročila (Excelove datoteke),
- histografija procesnih veličin,
- recepture,
- alarmne datoteke,
- zgodovina dogodkov,
- konfiguracija zaščit.

Ta sistem je t. i. hibridni sistem, pri katerem elektronski zapis (proizvodno poročilo) izpišemo in ročno podpišemo. Elektronski podpis na sistemu ni izvedljiv.

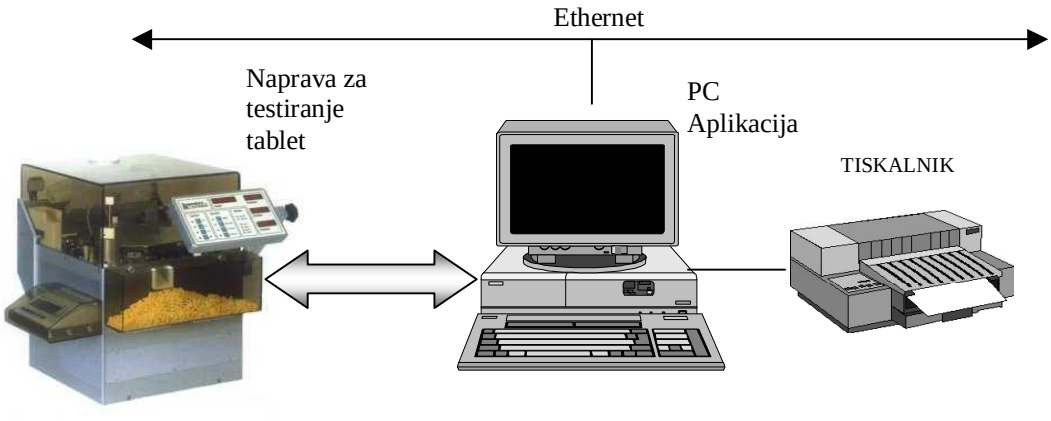
5.3.1.2 Sistem za medprocesno kontrolo tablet

Sistem za medprocesno kontrolo tablet je sestavljen iz naprave za testiranje tablet in iz računalnika, na katerem je nameščena programska rešitev za vodenje naprave, zbiranje in obdelavo rezultatov testiranja. Na računalnik je priključen še tiskalnik za izpis obdelanih rezultatov testiranja. Sestavo sistema prikazuje slika 8.

Sistem za testiranje tablet je naprava za določanje mase, debeline, premera oziroma dolžine in trdnosti tablet, jeder, lakiranih tablet ali dražejev.

Pri testiranju posamezna tableta preko dozirnega sistema pade v zarezo zvezdastega krožnika, ki jo pomakne do tehtnice, merila za debelino, merila za premer in merila za trdnost. Po končanem testiranju padejo zdrobljene tablete v odpadno posodo, nezdrobljene tablete pa v zbiralni lonček.

Slika 8: Sistem za testiranje tablet



Vir: Tablet Testing System, 2001.

Računalnik zbere podatke, dobljene s testiranjem, jih obdela in shrani, tiskalnik jih izpiše.

Ob vklopu računalnika se je najprej treba prijaviti na računalnik in v omrežje. Pri tem geslo ni zahtevano. Nato se izvede zagonska procedura, v sklopu katere se avtomatsko naloži tudi program za testiranje fizikalnih lastnosti tablet oziroma dražejev.

Vsak dan se pred testiranjem izvede testiranje ustreznosti merilnih veličin z referenčnimi merili. Enkrat na leto se izvede kalibracija merilnih senzorjev na napravi..

Teste izvajamo na osnovi predhodno vstavljenih podatkov. Izberemo že prednastavljeno vrsto preparata, ki ga bomo testirali (tablete, jedra, lakirane tablete, draženji). Za preparate, ki jih bomo testirali, so na sistemu že shranjene specifikacije. Določimo vrsto testiranja, izmet in mesto testirane tablete za avtomatsko odmerjanje. Z mestom tablete je določena točna pozicija posamezne tablete.

Izvajanje testa lahko operater prekine. Po prekinitvi testa lahko nato postopek normalno nadaljujemo. Pri ustavljenem testu pa sistem izvrže preostale tablete. Med izvajanjem testa se na nadzornem računalniku izpisujejo rezultati in barvne indikacije o rezultatih testiranja. Zelena barva pomeni, da je rezultat v določenih mejah specifikacije, in rdeča, da je izven mej.

Ko je test končan, se avtomatično izpiše poročilo o testiranju. Natisnjeni izpis testiranja se pregleda in podpiše. Hkrati se izpis shrani tudi na trdem disku računalnika.

Na tem sistemu so za dobre prakse pomembni tile elektronski zapisi:

- testne specifikacije produktov,
- prednastavljeni testi,
- poročila,
- nastavitveni parametri,
- konfiguracija zaščit,
- zgodovina dogodkov.

Tudi ta sistem je t. i. hibridni sistem, pri katerem elektronski zapis (proizvodno poročilo) izpišemo in ročno podpišemo. Elektronski podpis na sistemu ni izvedljiv.

5.3.1.3 Nadzorni sistem za termostatirano shranjevanje vzorcev

Nadzorni sistem je namenjen nadzorovanju temperature in vlage v termostatiranih komorah za shranjevanje vzorcev.

Sistem je povsem samostojen in ni povezan na mrežo. Izvedena je povezava računalnika na hladilno komoro preko serijskega (RS232) vmesnika. Hladilna komora pošilja podatke na nadzorni računalnik, kjer se shranjujejo in v primeru odstopa fizikalnih vrednosti izven določenih meja sprožijo alarm.

Na nadzorni računalnik je vezan še tiskalnik, s katerim lahko po potrebi izpišemo podatke o temperaturi in vlagi ter nastavitvah.

Operacijski sistem nadzornega računalnika je Linux. Sistem omogoča prikaze in izpise vrednosti temperature in relativne vlage.

Na tem sistemu so za dobre prakse pomembni tile elektronski zapisi:

- histografija temperature in vlage,
- nastavitveni parametri,
- konfiguracija zaščit.

Tudi ta sistem je t. i. hibridni sistem, pri katerem elektronski zapis (proizvodno poročilo) izpišemo in ročno podpišemo. Elektronski podpis na sistemu ni izvedljiv.

5.3.2 Rezultati vrednotenja variant

Na podlagi ocene računalniških sistemov, ki jo je ekspertna skupina izvedla po pripravljenem vprašalniku, smo v model ustrezno vnesli ocene za kriterije. Končna ocena variant je predstavljena v tabeli 2.

Tabela 2: Končna ocena kritičnosti računalniškega sistema izbranih variant

Sistem	**Ocena**
NADZORNO-KRMILNI SISTEM	srednje kritičen
TESTIRANJE TABLET	precej kritičen
NADZOR KOMOR	zelo kritičen

Vir: Interne ocene računalniških sistemov, LEK, 2001.

Ocena je pravilna in predstavlja odraz dejanskega stanja sistemov. Kot je razvidno, je kot najbolj kritičen ocenjen sistem za nadzor termostatiranih komor za shranjevanje vzorcev.

Glede na to, da so vsi izbrani sistemi brez elektronskih podpisov, smo v kriteriju "klasifikacija sistema" izbrali vrednost *samo zapisi*. Na ta način smo izločili vse kriterije za elektronske podpise. Torej kriterij "elektronski podpisi" ni imel nikakršnega vpliva na končno oceno kritičnosti.

Na oceno pa so bistveno vplivali kriteriji za elektronske zapise, in sicer so to: "validacija elektronskih zapisov", "zaščita", "zgodovina dogodkov" in "sistemska dokumentacija".

Tabela 3 prikazuje vrednosti kriterijev za elektronske zapise, ki bistveno vplivajo na končno oceno kritičnosti.

Tabela 3: Vpliv kriterijev na končno oceno za izbrane variante

	Vrednosti sestavljenih kriterijev			
Sistem	Validacija el. zapisov	Zaščita	Zgodovina dogodkov	Sistemska dokumentacija
NADZORNO-KRMILNI SISTEM	delno	povprečno	dobro	povprečno
TESTIRANJE TABLET	delno	slabo	povprečno	povprečno
NADZOR KOMOR	Slabo	Slabo	slabo	povprečno

Vir: Interne ocene računalniških sistemov, LEK, 2001.

5.3.2.1 Nadzorno-krmilni sistem v proizvodnji

Iz obeh tabel je razvidno, da je varianta "NADZORNO-KRMILNI SISTEM" med izbranimi variantami najmanj kritična.

Skupna ocena kritičnosti sistema je srednje kritičen. Ta ocena sledi iz ocene skladnosti za elektronske zapise, ki je pri tem sistemu srednje skladna.

5.3.2.1.1 Analiza

V nadaljevanju opisujemo kriterije, ki bistveno vplivajo na končno oceno kritičnosti sistema.

– Validacija elektronskih zapisov, ocena kriterija: *delno*

  Pri ocenjevanju kriterijev smo ugotovili, da je validacija sistema glede na industrijske standarde večinoma izvedena, čeprav manjkajo uporabniške zahteve, kvalifikacija načrtovanja in nekateri postopki.

  Ravno tako je delno izvedena že validacija glede na regulativo o elektronskih zapisih in elektronskih podpisih. Delno so bili testirani neveljavni vnosi, testirana je bila zaščita dostopov in avtorizacij.

– Zaščita, ocena kriterija: *povprečno*

  Skupna ocena kriterija je povprečno, ker so vsi podkriteriji ocenjeni z enako oceno povprečno.

  Nadzor je povprečen, ker ni periodičnega pregledovanja zapisov in ker je zaporedje dogodkov vsiljeno le delno.

  Tudi zaščita zapisov je povprečna. Arhiviranje se izvaja centralno preko mreže. Restavracija se ne izvaja periodično in ni bila preverjena niti v okviru validacije sistema. Perioda arhiviranja podatkov iz sistema je en dan.

V okviru zaščite dostopa do sistema avtorizacija dostopa ni dobro nadzirana, manjka arhiv konfiguracije zaščit. Poleg tega se uporabniški računi periodično ne pregledujejo in časovno ne pretečejo.

- Zgodovina dogodkov, ocena kriterija: *dobro urejeno*

  Izvedeno imamo računalniško zgodovino dogodkov, zato ročna ni potrebna. V okviru kriterijev je slabo ocenjen le del parametrov zgodovine dogodkov, ker se v zgodovini ne izpiše tiskano ime posameznika, temveč njegova koda za uporabniško ime. Vendar je ta koda enoznačna in je sledljiva do posameznika.

- Sistemska dokumentacija, ocena kriterija: *povprečno*

  Nadzor nad uporabo in vzdrževanjem je ustrezen, manjka ustrezna kontrola sprememb, ker ni kontrole verzij in zgodovine dogodkov za sistemsko dokumentacijo.

5.3.2.1.2 Možnosti izboljšav

S krajšo analizo odločitvenega modela lahko ugotovimo, da že s povišanjem ocene enega izmed podkriterijev za skladnost dobimo precej skladen sistem, če povišamo dva kriterija pa že popolno skladen sistem.

Glede na izvedbo sistema bi bilo najbolj smiselno izboljšati zaščito sistema in ustrezno urediti sistemsko dokumentacijo.

Validacijo sicer lahko izboljšamo, vendar nekaterih kriterijev, ki jih nismo izpolnili v začetni fazi življenjskega cikla sistema, kot so: uporabniške zahteve, ocena dobavitelja in kvalifikacija načrtovanja, ne moremo izvesti za nazaj. Smiselno je izvesti nekatere izboljšave, testirati zgodovino dogodkov, arhiviranje in restavracijo, vendar s tem ne bomo bistveno vplivali na končno oceno validacije sistema.
Če želimo doseči popolno ustreznost validacije, nam trenutni sistem tega ne omogoča. Potrebna bi bila nadgradnja sistema, s katero bi dodali tudi nekatere funkcije za zagotavljanje skladnosti (neveljavni vnosi, avtomatski mehanizem sekvenc).

Zaščito sistema lahko izboljšamo z ustrezno zaščito zapisov in zaščito dostopa. To bi dosegli z boljšo zaščito zapisov na sistemu in ustrezno ureditvijo celotnega arhiviranja in restavracije, ki vključuje tudi periodično verifikacijo ustreznosti. Poleg tega je potrebno vpeljati nekatere postopke, ker sistem nekaterih zahtev avtomatsko ne more izpolniti. Urediti je potrebno arhiv konfiguracije zaščit (ročno vodenje sprememb), način avtorizacije dostopa in periodično pregledovanje uporabniških računov.

Zgodovina dogodkov je že dobro urejena. Kot izboljšavo bi lahko za uporabniška imena namesto številk uporabljali tiskano ime posameznika. Tako bi se tudi v zgodovini dogodkov za parametre pri nekem dogodku izpisalo tiskano ime posameznika.

Pri sistemski dokumentaciji je potrebno urediti kontrolo sprememb, vpeljati procedure za kontrolo sprememb oziroma uvesti zgodovino dogodkov. Če želimo dobro urejenost kriterija "sistemska dokumentacija" in je kriterij "nadzor nad uporabo in vzdrževanjem - kontrola dostopa" dobro urejen, mora biti kriterij "kontrola sprememb" vsaj povprečno dobro urejen.

Elektronski podpisi na obstoječem sistemu niso izvedeni. Elektronski zapis (proizvodno poročilo) se ob koncu procesa izpiše in se ga ročno podpiše. Zahteva regulative v tem primeru je zagotoviti sledljivost podpisanega zapisa z originalnim elektronskim zapisom. Tu je to zagotovljeno s časovno značko in drugimi podatki (naziv izdelka, kontrolna številka serije, delovni nalog) na elektronskem zapisu poročila. Potrebno je le zagotoviti primerno zaščito elektronskih zapisov.

5.3.2.1.3 Končna ocena sistema

Trenutna ocena sistema je srednje kritičen. Z uvedbo nekaterih postopkov, kot so:

- pregled elektronskih zapisov na sistemu,
- arhiv konfiguracije zaščit,
- način avtorizacije dostopa,
- periodično pregledovanje uporabniških računov in menjava gesel ter
- kontrolo sprememb sistemske dokumentacije,

in z ustrezno zaščito dostopa do operacijskega sistema lahko sistem potrdimo kot popolnoma skladen z regulativo. V primeru popolne skladnosti računalniški sistem ni več kritičen.

Druga možnost je nadgradnja obstoječega sistema z novim sistemom. Z novim sistemom bi lahko določene postopke, navedene zgoraj, zagotovili avtomatsko, poleg tega bi bila možna vpeljava elektronskega podpisa v pravi obliki (ne hibridni) in ne bi bilo več potrebno izpisovati in ročno podpisovati poročil. Nov sistem seveda zahteva celotno načrtovanje, izvedbo in validacijo.

Ne glede na možnost nadgradnje sistema je v vsakem primeru potrebno postopke za zagotavljanje skladnosti vpeljati takoj.

5.3.2.2 Sistem za medprocesno kontrolo tablet

Skupna ocena kritičnosti sistema za testiranje tablet je precej kritičen. Ta ocena sledi iz ocene skladnosti za elektronske zapise, ki je v tem primeru manj skladna.

5.3.2.2.1 Analiza

V nadaljevanju utemeljujemo oceno na podlagi kriterijev, ki bistveno vplivajo na končno oceno.

- Validacija elektronskih zapisov, ocena kriterija: *delno*

  Ugotovili smo, da je validacija sistema glede na industrijske standarde večinoma izvedena, čeprav ni bila izvedena ocena dobavitelja, kvalifikacija načrtovanja ni popolnoma ustrezna in manjkajo nekateri postopki za administracijo sistema.

Ravno tako je delno že izvedena validacija glede na regulativo o elektronskih zapisih in elektronskih podpisih. Delno so bili testirani neveljavni vnosi, testirana je bila zaščita dostopov in avtorizacij.

– Zaščita, ocena kriterija: *slabo urejeno*

  Povprečen nadzor, povprečna zaščita zapisov in slabo urejena zaščita dostopa dajejo kriteriju "zaščita" skupno oceno slabo urejeno.

  Nadzor je povprečen, ker ni periodičnega pregledovanja zapisov in je zaporedje dogodkov vsiljeno le delno.

  Tudi zaščita zapisov je povprečna. Arhiviranje in restavracija se izvajata lokalno na zahtevo operaterja. Perioda arhiviranja podatkov je predpisana na en teden. Verifikacija ustreznosti arhiviranja in restavracije se ne izvaja periodično. Preverjena je bila v okviru validacije sistema.

  Problem pri zaščiti dostopa je slaba urejenost logičnega dostopa do programa. Uporabniški računi so slabo urejeni, gesla so skupna in niso prikrita in tudi minimalna dolžina gesel ni določena.

  Dostop do operacijskega sistema sicer ni omejen, vendar je zaščiten dostop do vseh drugih programov razen tistega za nadzor testiranja tablet.

– Zgodovina dogodkov, ocena kriterija: *povprečno*

  Izvedeno imamo računalniško zgodovino dogodkov, zato ročna ni potrebna. Računalniško ustvarjena zgodovina dogodkov je delno ustrezna, ker ni ustrezno arhivirana, operaterji imajo možnost spreminjanja časovne značke in med parametri ni izpisano tiskano ime posameznika, ampak njegovo uporabniško ime, ki je skupno za več uporabnikov.
  Sprememba časovne značke lahko bistveno vpliva na verodostojnost zgodovine. Zgodovina dogodkov tudi ni sledljiva do posameznika, temveč samo do skupine posameznikov (operaterji, tehniki).

– Sistemska dokumentacija, ocena kriterija: *povprečno*

  Nadzor nad uporabo in vzdrževanjem je ustrezen, manjka ustrezna kontrola sprememb, ker ni kontrole verzij in zgodovine dogodkov za sistemsko dokumentacijo.

5.3.2.2.2 Možnosti izboljšav

S krajšo "če-potem" analizo odločitvenega modela lahko ugotovimo, da največ pridobimo z ureditvijo zaščite dostopa in zaščite zapisov na sistemu. Če vsaj povprečno uredimo zaščito na sistemu, se končna ocena kritičnosti že zniža na vrednost srednje kritičen. Če dobro uredimo zaščito in nato na dobro urejenost povišamo še enega od ostalih kriterijev za elektronske zapise ("validacija elektronskih zapisov", "zgodovina dogodkov", "sistemska dokumentacija"), je sistem že manj kritičen. Če dobro uredimo zaščito in še dva od ostalih kriterijev, imamo popolnoma skladen sistem, ki ni kritičen.

Po podrobnem pregledu sistema in tehnične dokumentacije o sistemu je bilo ugotovljeno, da sistem omogoča primerne zaščite in zgodovino dogodkov ter celo elektronske podpise. Poleg tega je možno za vsako aktivnost, ki jo izvedemo, predpisati raven zaščite. Ugotovili smo, da je sistem popolnoma konfigurabilen. Potrebno je določiti le kritičnost funkcij in operacij za sam proces ter na podlagi tega ustrezno konfigurirati sistem.

Poleg tega je potrebno določiti uporabniške račune za vsakega posameznika posebej. Na sistemu je možno določiti tudi minimalno število znakov za gesla.

Validacijo enako kot v primeru proizvodnega nadzornega sistema lahko nekoliko izboljšamo, vendar nekaterih aktivnosti ne moremo izvesti za nazaj (ocena dobavitelja, kvalifikacija načrtovanja). Validacijo glede na regulativo o elektronskih zapisih in podpisih lahko izboljšamo tako, da preverimo, ali sistem prepoznava neveljavne ali spremenjene zapise in jih primerno testiramo, preverimo ustreznost zgodovine dogodkov in testiramo ustreznost arhiviranja in restavracije zapisov.

Na tem sistemu je nujno potrebno izboljšati zaščito zapisov in dostopa do sistema. Treba je poskrbeti, da bodo elektronske zapise pregledovali uporabnik, administrator in predstavnik upravljanja kakovosti. Pri zaščiti zapisov je potrebno ustrezno urediti arhiviranje (krajši časovni interval - vsaj dnevno) in restavracijo ter izvajati periodično testiranje. Potrebna je tudi boljša zaščita zapisov, dokler so na sistemu.

Logični dostop je zelo slabo urejen in ga je potrebno izboljšati. Uporabniške račune je treba določiti za vsakega posameznika posebej (do sedaj skupna gesla uporabnikov) in jih periodično pregledovati ter odkrivati poskuse nepooblaščenih dostopov do sistema. Večnivojske dostope je potrebno na novo preveriti in ustrezno določiti. Prav tako je potrebno določiti minimalno število znakov za gesla (priporočeno število je šest). Za nekatere funkcije, kot so: arhiv konfiguracije zaščit, periodična menjava gesel in način avtorizacije dostopa, ki niso izvedljive avtomatsko, je potrebno zagotoviti ročne procedure oziroma postopke.

Priporoča se nabava in uvedba dodatnega programskega modula, ki omogoča funkcionalnosti glede uporabniških računov in gesel z namenom zagotovitve skladnosti z regulativo. Te funkcionalnosti so: periodična menjava gesel, časovni potek uporabniških računov, blokada uporabniškega računa v primeru več poskusov nepooblaščenega dostopa, določitev minimalnega števila znakov za gesla in pomnjenje že uporabljenih gesel. Z vsem navedenim lahko uredimo zaščito tako, da bo končna ocena kriterija "zaščita" dobro urejeno.

Zgodovina dogodkov je že povprečno urejena. Za dobro urejeno zgodovino dogodkov moramo zgodovino dogodkov tako kot ostale "GXP elektronske zapise" primerno arhivirati in zaščititi na sistemu. Preprečiti je treba možnost spremembe časovne značke, saj to lahko bistveno vpliva na verodostojnost zgodovine dogodkov. Poleg tega je z ureditvijo uporabniških računov potrebno zagotoviti, da se med parametri zgodovine dogodkov izpisuje tiskano ime posameznika in ne uporabniško ime skupine kot sedaj.

Pri sistemski dokumentaciji moramo urediti kontrolo sprememb. Potrebno je vpeljati procedure za kontrolo sprememb oziroma uvesti zgodovino dogodkov. Za dobro urejenost kriterija "sistemska dokumentacija" in v primeru, da je kriterij "nadzor nad uporabo in vzdrževanjem - kontrola dostopa" dobro urejen, mora biti kriterij "kontrola sprememb" vsaj povprečno dobro urejen.

Na sistemu je možno dodatno določiti elektronsko podpisovanje za vsako aktivnost, ki jo izvedemo. V okviru procesa je potrebno določiti kritične aktivnosti in jih primerno zaščititi z dodatnim elektronskim podpisom. Takšne aktivnosti so: ustvarjanje, shranjevanje ali brisanje pomembnih zapisov na sistemu (poročil, alarmov, produktov, testnih specifikacij). Takšen elektronski podpis mora seveda ustrezati vsem kriterijem za elektronske podpise. V primeru ustreznih elektronskih podpisov ni več nujen izpis končnih poročil in dodaten ročni podpis poročila. Sicer se poročilo lahko izpiše, vendar že prikaz elektronskega podpisa, ki se izpiše hkrati s poročilom, zadošča, ker je pravno enakovreden ročnemu podpisu.

5.3.2.2.3 Končna ocena sistema

Trenutna ocena sistema je precej kritičen. Z ustrezno konfiguracijo obstoječega sistema in vpeljavo nekaterih postopkov, kot so:

- pregled elektronskih zapisov na sistemu,
- arhiv konfiguracije zaščit,
- način avtorizacije dostopa,
- periodično pregledovanje uporabniških računov in menjavo gesel,
- kontrolo sprememb sistemske dokumentacije,

in z ustrezno zaščito zapisov ter dostopa do sistema lahko sistem potrdimo kot popolnoma skladen z regulativo. V primeru popolne skladnosti seveda računalniški sistem ni več kritičen.

Priporoča se nadgradnja sistema s programskim modulom za uporabniške račune in gesla, ki posebej zagotavlja funkcionalnosti za skladnost z regulativo. Sicer je tudi za ta del aktivnosti (menjava gesel, pregledovanje nepooblaščenih poizkusov dostopa, minimalno število karakterjev) potrebno vpeljati ročne procedure.

Poleg elektronskih zapisov sistem omogoča tudi določanje in konfiguracijo elektronskih podpisov. V primeru elektronskih podpisov moramo seveda zadostiti tudi vsem kriterijem za elektronske podpise, tako pri izvedbi, prikazu, povezavi podpisa z zapisom kot pri zahtevah za nadzor elektronskega podpisa.

5.3.2.3 Nadzorni sistem za termostatirano shranjevanje vzorcev

Skupna ocena kritičnosti sistema za termostatirano shranjevanje vzorcev je zelo kritičen. Ta ocena sledi iz ocene skladnosti za elektronske zapise, ki je za ta primer neskladna.

5.3.2.3.1 Analiza

V nadaljevanju opisujemo kriterije, ki bistveno vplivajo na končno oceno kritičnosti sistema.

– Validacija elektronskih zapisov, ocena kriterija: *ne*

  Iz ocene sistema je razvidno, da validacija sistema ni bila ustrezno izvedena. Na začetku življenjskega cikla sistema aktivnosti niso bile ustrezno izvajane. Sicer so postopki za delo s sistemom izdelani, vendar je to mnogo premalo za potrditev ustreznosti validacije.

  Prav tako je neustrezna validacija glede na elektronske zapise. Od vseh zahtev je zadoščeno le zahtevam za izdelavo kopij elektronskih zapisov.

  Izpostavimo lahko kar nekaj slabosti validacije: ni uporabniških zahtev, ni izvedenih kvalifikacij (DQ, IQ, OQ izveden le delno, PQ), ni postopkov za administracijo, arhiviranje, sistem ne prepoznava neveljavnih vnosov oziroma spremenjenih zapisov, zaščite zapisov na sistemu niso izvedene in tudi ne testirane.

– Zaščita, ocena kriterija: *slabo urejeno*

  Povprečno dobro sta urejena nadzor in zaščita dostopa do sistema. V okviru nadzora lahko kot ustrezno potrdimo zaporedje dogodkov. Na sistemu nobenih aktivnosti in zapisovanje fizikalnih parametrov se izvaja avtomatsko. Delno lahko potrdimo preverjanje naprav, ker sistem komunicira s termostatiranimi komorami po posebnem protokolu. Če bi priključili kakšno drugo komoro, komunikacija ne bi delovala.

  Zaščita zapisov ni urejena, ker vsakdo lahko dostopa do elektronskih zapisov in jih naključno ali namerno spremeni. Prav tako se ne izvaja arhiviranje zapisov.

  Zaščita dostopa do sistema je urejena povprečno dobro z omejenim fizičnim dostopom, brez arhiva konfiguracije zaščit in z delno urejenim logičnim dostopom. Omejen je dostop do operacijskega sistema in na ravni programa je uresničena tudi večnivojska zaščita. Manjka ustrezna kontrola uporabniških računov, kot so: časovni potek, periodično pregledovanje in odkrivanje nepooblaščenih poskusov dostopa do sistema.

– Zgodovina dogodkov, ocena kriterija: *slabo urejeno*

  Sistem nima izvedene avtomatske zgodovine dogodkov. Izvedbo katerekoli aktivnosti ali spremembe na sistemu bi bilo treba ustrezno evidentirati. Če sistem tega ne zagotavlja avtomatsko, neodvisno od operaterja, moramo za vodenje zgodovine dogodkov na sistemu zagotoviti ročne procedure.

– Sistemska dokumentacija, ocena kriterija: *povprečno*

  Nadzor nad uporabo in vzdrževanjem je ustrezen, manjka ustrezna kontrola sprememb, ker ni kontrole verzij in zgodovine dogodkov za sistemsko dokumentacijo.

5.3.2.3.2 Možnosti izboljšav

Največ k skladnosti sistema doprineseta kriterija "zaščita" in "zgodovina dogodkov". Z izboljšavo vsaj enega od teh dveh kriterijev na povprečno že dobimo iz popolnoma neskladnega sistema manj skladen sistem.

Validacija elektronskih zapisov ni bila izvedena in jo za nazaj lahko izvedemo le delno. Na obstoječem sistemu tako lahko ustrezno uredimo in popišemo programske in strojne specifikacije ter na podlagi tega izvedemo ustrezno kvalifikacijo montaže in obratovanja. Smiselna je tudi izdelava in uvedba postopkov za administracijo sistema.

V okviru validacije glede na regulativo o elektronskih zapisih in podpisih je potrebno ustrezno testirati avtorizacije in uporabniške ravni, izvesti in testirati arhiviranje in restavracijo zapisov.

Zaščita je slabo izvedena predvsem zaradi slabe zaščite elektronskih zapisov. Elektronske zapise je potrebno ustrezno zaščititi. Poleg omejitve dostopa in omejitve možnosti spreminjanja to lahko dosežemo tudi z ustreznim arhiviranjem. Potrebno je urediti tudi zaščito dostopa z vodenjem arhiva konfiguracije zaščit in večjim nadzorom uporabniških računov.

Avtomatska zgodovina dogodkov na sistemu ni izvedena, prav tako ni uvedena ročna zgodovina dogodkov. Nujno potrebno je takoj uvesti procedure za zgodovino dogodkov (evidentiranje kakršnihkoli sprememb na sistemu). Vendar z ročno zgodovino dogodkov le delno lahko zagotavljamo ustreznost zgodovine dogodkov.

Pri sistemski dokumentaciji je treba urediti kontrolo sprememb. Uvesti moramo procedure za kontrolo sprememb oziroma zgodovino dogodkov. Za dobro urejenost kriterija "sistemska dokumentacija" in v primeru, da je kriterij "nadzor nad uporabo in vzdrževanjem - kontrola dostopa" dobro urejen, mora biti kriterij "kontrola sprememb" vsaj povprečno dobro urejen.

Elektronski podpisi na obstoječem sistemu niso izvedeni. Elektronski zapis, podatki o temperaturi in relativni vlagi se lahko izpišejo in ročno podpišejo. Zahteva regulative v tem primeru je zagotoviti sledljivost podpisanega zapisa z originalnim elektronskim zapisom. Tu je to zagotovljeno s časovno značko na elektronskem zapisu poročila. Ker je potrebno zagotoviti primerno zaščito elektronskih zapisov, mora biti spreminjanje časovne značke onemogočeno.

5.3.2.3.3 Končna ocena sistema

Trenutna ocena sistema je zelo kritičen. Z ustrezno konfiguracijo obstoječega sistema in vpeljavo nekaterih postopkov, kot so:

- zgodovina dogodkov,
- arhiviranje,
- pregled elektronskih zapisov na sistemu,
- arhiv konfiguracije zaščit,
- način avtorizacije dostopa,
- periodično pregledovanje uporabniških računov in menjavo gesel,
- kontrolo sprememb sistemske dokumentacije,

in z ustrezno zaščito zapisov na sistemu lahko sistem potrdimo kot precej skladen z regulativo. V primeru precejšnje skladnosti postane računalniški sistem manj kritičen.

Za zagotovitev popolne skladnosti se priporoča nadgradnja sistema, ki zagotavlja funkcionalnosti za skladnost z regulativo. Te funkcionalnosti obsegajo zgodovino dogodkov, arhiviranje, kodiranje in zaščito elektronskih zapisov ter funkcionalnosti za uporabniška imena in gesla.

5.3.3 Rezultati vrednotenja izboljšanih variant

Ocene izboljšanih variant glede na naš model so izpisane v dodatku D.

5.3.3.1 Začetne ocene sistemov

Prvotna ocena kritičnosti računalniškega sistema izbranih variant je razvidna iz tabele 2 na strani 66.

Zelo kritičen je sistem za nadzor termostatiranih komor, ker ni ustrezne validacije sistema, ni primerne zaščite dostopa in zapisov, ni zgodovine dogodkov in tudi ni kontrole sprememb sistemske dokumentacije. Sistem za testiranje tablet smo ocenili kot precej kritičen in nadzorni sistem za vodenje proizvodnje kot srednje kritičen.

Na podlagi analize in možnosti izboljšav lahko ugotovimo, da z določenimi procedurami in nastavitvami sistemov lahko bistveno izboljšamo sistem za testiranje tablet in nadzorni sistem za vodenje proizvodnje, medtem ko je sistem za nadzor termostatiranih komor treba nadgraditi z dodatnimi funkcijami, če želimo zagotavljati popolno skladnost sistema.

5.3.3.2 Izboljšane ocene sistemov

V okviru aktivnosti za izvedbo skladnosti sistemov se za tri izbrane variante izvede naslednje:

- **Nadzorno-krmilni sistem**
  Uvede se predlagane procedure iz poglavja 5.3.2.1.3. Izvede se ponovno oceno prej neustreznih kriterijev in vnese ustrezne vrednosti v model za oceno kritičnosti.

- **Testiranje tablet**
  Kupi se nova verzija programske opreme, ki ima dodatne funkcionalnosti za zaščite, za administracijo gesel in za elektronske podpise. Oceni se proces in predvidi ustrezno konfiguracijo aplikativnega dela programske opreme (konfiguracija sistema, večnivojska zaščita funkcij, uvedba elektronskega podpisa) in instalacija ter zagotovitev varnostnega kopiranja podatkov. Po instalaciji in nastavitvi konfiguracije sistema se izvede validacija glede na pripravljene protokole (IQ, OQ, PQ). Poleg tega se uvedejo potrebne dodatne procedure, kot so: način avtorizacije dostopa in dodelitve elektronskega podpisa, kontrola sprememb sistemske dokumentacije ter periodično pregledovanje sistema in zapisov, ki ga izvajajo uporabnik, administrator in predstavnik upravljanja kakovosti.

  Analiza kriterijev za elektronske podpise je podana v nadaljevanju.

- **Nadzor termostatiranih komor**
  Kupi se nova verzija programske opreme, ki ima dodatne funkcionalnosti za zaščite, uporabniške račune, gesla, zgodovino dogodkov, varnostno kopiranje in prepoznavanje neveljavnih oziroma spremenjenih zapisov. Po izvedeni namestitvi in kvalifikacijah se uvedejo še potrebne procedure za zagotavljanje skladnosti: način avtorizacije dostopa, periodično pregledovanje sistema, zapisov, uporabniških računov in arhiv konfiguracije zaščit. Ustrezno se zaščitijo tudi elektronski zapisi na sistemu.

5.3.3.3 Analiza kriterijev za elektronske podpise

V nadaljevanju analiziramo še bistvene kriterije v okviru kriterija "elektronski podpisi", ki smo jih uvedli z novo verzijo programske rešitve za testiranje tablet.

- Validacija elektronskega podpisa, ocena kriterija: *dobra*

  V okviru validacije elektronskega podpisa smo preverili izvedbo in prikaz podpisa, povezavo podpis-zapis in zahteve za nadzor podpisa. Validacija vseh navedenih kriterijev je bila ustrezna in je bila dobro izvedena.

- Prikaz podpisa, ocena kriterija: *dobro urejeno*

  Vsebina prikaza elektronskega podpisa je ustrezna, ker vsebuje vse zahtevane parametre. Prav tako je ustrezno urejena zaščita prikaza elektronskega podpisa.

- Povezava podpis - zapis, ocena kriterija: *dobro urejeno*

  Elektronski podpis je sestavni del elektronskega zapisa, ki ga podpišemo (proizvodno poročilo). Tako je zagotovljeno, da sta elektronski zapis in elektronski podpis neločljivo povezana oziroma združena v eno.

- Zahteve in nadzor podpisa, ocena kriterija: *dobro urejeno*

  S procedurami je vzpostavljen ustrezen nadzor za dodelitev in enkratnost elektronskega podpisa. Nadzor uporabniških kod in gesel je dobro urejen. Izmed vseh zahtevanih kriterijev ni uresničen le ohranjevalnik zaslona, sistem ima avtomatsko odjavo po določenem času neaktivnosti (trenutna nastavitev na 10 minut), s čimer onemogočimo, da bi naključni posamezniki uporabljali sistem.

5.3.4 Zaključek

S samim modelom, izbiro variant, njihovo oceno in analizo smo zadostili ciljem raziskave:

1. Opredelili smo kriterije (kvantitativne in kvalitativne), ki vplivajo na kritičnost računalniškega sistema. Nabor osnovnih kriterijev je bil izbran v okviru priprav na ocenjevanje vseh sistemov. Izbrani kriteriji so rezultat študija regulative, viharjenja možganov, raznih posvetovanj mednarodnih ekspertov, obiskov konferenc na temo elektronskih podpisov in zapisov ter končne izbire v okviru skupine za informacijske sisteme v podjetju.

2. Določili smo funkcijo in vpliv posameznih kriterijev, ki nižje kriterije združujejo v višje kriterije. Pri tem smo upoštevali tudi uteži posameznih kriterijev. Vplivi posameznega kriterija na višji kriterij se namreč lahko med seboj razlikujejo. Značilen primer kriterija z velikim vplivom na ostale kriterije je kriterij "zaščita" elektronskih zapisov. Sistem je lahko izvrstno validiran, zagotovljena je lahko zgodovina dogodkov in ustrezna sistemska dokumentacija, vendar če ne zagotavlja ustrezne zaščite dostopa in elektronskih zapisov, potem ne more biti skladen z regulativo.

3. Na podlagi določenih kriterijev in odločitvenih pravil je nastal večkriterijski odločitveni model za vrednotenje kritičnosti računalniških sistemov, ki smo ga nato preizkusili na praktičnih variantah.

4. Določili smo, kako uporabiti odločitveni model pri ugotavljanju kritičnosti računalniškega sistema. Z uporabo modela in preizkušanjem raznih variant smo lahko določili vrstni red kritičnosti le-teh. Model omogoča objektivno primerjanje več računalniških sistemov med seboj. Do sedaj so sisteme med seboj primerjali na podlagi nepopolnih oziroma neobjektivnih in napačno uteženih kriterijev. S takšnim odločanjem lahko dobimo netočne ocene in posledično slabe odločitve.

5. Na podlagi uporabe odločitvenega modela smo določili potrebne aktivnosti za zagotovitev ustreznosti posameznega računalniškega sistema. Z izvedbo ocene in vnosom osnovnih kriterijev v naš model dobimo končni rezultat kritičnosti računalniškega sistema. Vpliv posameznega kriterija lahko takoj prikažemo na modelu (spreminjanje vrednosti). Uporaba modela tako skrajšuje čas od ocene posameznega sistema do načrtovanja ukrepov za izboljšanje skladnosti sistema.

Pri preizkušanju in uporabi modela smo ugotovili, da je model razumljiv vsem udeležencem odločitvene skupine, da jim omogoča lažje odločanje in končno oceno kritičnosti računalniških sistemov ter lažje načrtovanje ukrepov za odpravljanje neskladnosti sistemov.

6. Zaključki in napotki za nadaljnje delo

V magistrski nalogi smo izvedli večparametrski odločitveni model za analizo kritičnosti računalniških sistemov glede na regulativo o elektronskih zapisih in elektronskih podpisih.

V nadaljevanju bomo spregovorili o možnostih praktične uporabe modela.

6.1 Uporaba sistema v praksi

Na podlagi prvih izkušenj pri uporabi sistema lahko potrdimo možnosti uporabe modela v praksi.

Uporaba modela pri načrtovanju investicijskih projektov

Glede na obseg neskladnosti računalniških sistemov bodo pri nekaterih sistemih potrebna velika investicijska vlaganja. Nemogoče je zagotoviti nadgradnje vseh sistemov naenkrat. Z modelom lahko pomagamo k ustreznemu odločanju in razporeditvi sredstev tja, kjer je to

najbolj potrebno. Najprej je namreč potrebno zagotoviti sredstva za najbolj kritične sisteme.

Uporaba modela pri presoji skladnosti obstoječih in novih sistemov

Z modelom lahko objektivno ocenimo skladnost nekega računalniškega sistema. Kriteriji, na podlagi katerih izvajamo oceno, so primerno uteženi glede na pomembnost. Z uporabo istega modela lahko več različnih uporabnikov enako oceni isti sistem. Brez uporabe istega modela so lahko končne ocene sistema popolnoma različne, če jih ocenjujejo različni uporabniki.

Enako, kot lahko ocenjujemo obstoječe, lahko ocenimo tudi nove, še nedobavljene sisteme, in sicer na podlagi specifikacij potencialnih dobaviteljev. Na podlagi večje skladnosti posameznih sistemov se lažje odločamo za neki sistem in s tem izberemo dobavitelja.

Uporaba modela za izobraževanje

Model lahko zelo dobro služi tudi za izobraževalne namene. Odgovornost in zavedanje, da je potrebna skladnost z regulativo, je pomembno na vseh ravneh zaposlenih v podjetju. S pomočjo modela, uporabo praktičnih variant in "če-potem" analizo, ki jo omogoča model, lahko pregledno prikažemo zahteve za računalniške sisteme vsem ravnem zaposlenih.

Z modelom lahko dobro predstavimo tudi interpretacijo regulative v praksi. S kriteriji in odločitvenimi pravili ter utežmi smo določili, kako se posamezne zahteve regulative odražajo v praksi.

Uporaba modela za definiranje načina dela z računalniškim sistemom

Nenazadnje nam model pomaga tudi pri določanju načina dela in postopkov z računalniškimi sistemi. Poleg funkcionalnosti, ki jih omogočajo računalniški sistemi, bo vedno potrebno vzpostaviti tudi nekatere procedure za zagotovitev skladnosti. Primeri takšnih procedur so lahko pregledovanje elektronskih zapisov na sistemu, način avtorizacije dostopa, periodično pregledovanje uporabniških računov in še bi lahko naštevali. Procedure nam lahko služijo tudi kot nadomestilo tehničnih funkcionalnosti sistema. Na primer, periodično menjavo gesla lahko zahteva sistem avtomatično, sicer je potrebno predpisati postopek, po katerem se gesla periodično menjajo.

6.2 Programsko orodje za obvladovanje analiz

Število računalniških sistemov, ki morajo ustrezati regulativi za elektronske zapise in elektronske podpise, je v vsakem farmacevtskem podjetju zelo veliko. Glede na veliko število računalniških sistemov in veliko podatkov pri sami analizi in oceni posameznega sistema se zdi nujno potrebno programsko orodje za obvladovanje analiz.

Takšno programsko orodje naj omogoča vsaj naslednje funkcionalnosti: vnos podatkov o analizi oziroma oceni številnih sistemov, možnost načrtovanja korektivnih ukrepov s terminskimi plani in nosilci za izvedbo ter spremljanje in analizo izvajanja ukrepov glede na terminske plane.

6.3 Ocena sistemov glede na tip sistema

Zavedati se moramo, da različne tipe sistemov lahko obravnavamo različno. Smiseln se zdi pristop, ki nam opredeli oziroma že določi zahteve za posamezne tipe sistemov glede na našo interpretacijo regulative. Določen stroj v proizvodnji, ki vsebuje krmilnik in krmilni tablo, s katerim nastavljamo določene parametre za proizvodnjo, bomo verjetno obravnavali drugače kot neki računalniški sistem za materialno poslovanja ali vodenje proizvodnega procesa.

Za posamezne tipe sistemov je potrebno določiti minimalne potrebne zahteve. Na primer, za stroje v proizvodnji verjetno ne bomo zahtevali avtomatske zgodovine dogodkov, ker praktično niso nikjer izvedene. Zato je potrebno uvesti druge mehanizme za zaščito zapisov. Zaščita dostopa s ključem in ročna zgodovina dogodkov se zdita primerni za takšne sisteme. Nadaljnje aktivnosti za zagotavljanje skladnosti lahko torej vodimo v tej smeri, da za posamezne tipe sistemov določimo minimalni obseg funkcionalnosti in postopkov, katerim mora takšen tip sistema ustrezati.

6.4 Ekspertni sistem za ocenjevanje računalniških sistemov

Še bolj drzno razmišljanje nas pripelje do ekspertnega sistema, ki bi nam ocenil kritičnost računalniškega sistema.

Ekspertni sistemi so inteligentni informacijski sistemi, ki s svojim delovanjem poizkušajo posnemati delovanje eksperta pri analiziranju, reševanju in utemeljevanju odločitev v problemski domeni (Bratko, 1984; Zimmerman, 1987, str. 261; Mallach, 1994, str. 463; Bohanec, Rajkovič, 1990).

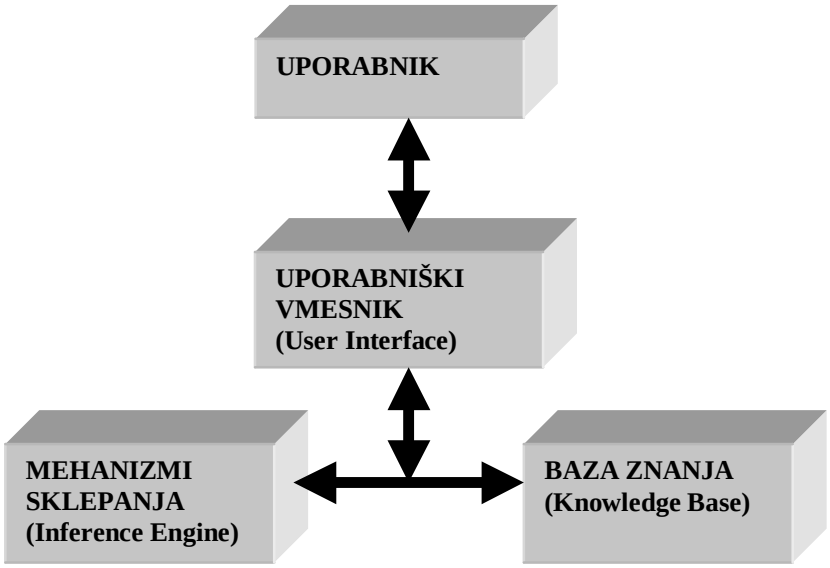
Zgradbo ekspertnega sistema lahko opredelimo z bazo znanja, mehanizmi sklepanja in uporabniškim vmesnikom (Sprague, Watson, 1996, str. 376). Lupino ekspertnega sistema pa sestavljajo mehanizmi sklepanja in uporabniški vmesnik, medtem ko je baza znanja prazna. S pomočjo uporabniškega vmesnika jo napolnimo z znanjem, ki je na voljo za rešitev konkretnega odločitvenega problema (Rajkovič, Bohanec, 1988, str. 132).

Naš model nam praktično predstavlja že prototip takšnega ekspertnega sistema. V ekspertni sistem bi lahko nato vključili še minimalne zahteve za posamezne tipe sistemov, o katerih govorimo v prejšnjem podpoglavju.

Glede na vnos minimalnih zahtev o sistemih in vnos dotedanjih informacij v sistem bi nas ekspertni sistem preko uporabniškega vmesnika selektivno spraševal in s tem povečeval svojo bazo znanja o skladnosti posameznega sistema.

Na podlagi vnosov informacij v sistem bi takšen ekspertni sistem predlagal potrebne korektivne aktivnosti za zagotovitev skladnosti.

Slika 9: Shema ekspertnega sistema



Vir: Sprague, Watson,1996, str. 376.

Osnovni gradniki ekspertnega sistema so prikazani na sliki 9.

6.5 Sklep

Večparametrski odločitveni model, ki smo ga izdelali za analizo kritičnosti računalniških sistemov glede na regulativo o elektronskih zapisih in elektronskih podpisih, nam omogoča hitro, učinkovito in objektivno oceno računalniških sistemov.

Z oceno lahko v kratkem času objektivno ocenimo neskladnosti sistema in na podlagi tega ustrezno načrtujemo korektivne ukrepe. Model omogoča hitro in učinkovito odpravljanje neskladnosti, kjer je to najbolj potrebno.

Možna je izpostavitev kritičnih sistemov in s tem ustrezna razporeditev človeških in finančnih virov.

7. Literatura

1. Abel J., LeBlanc L.: Specifying a Batch Management System for Electronic Records and Signatures – A Checklist for Compliance with 21CFR Part11, Pharmaceutical Engineering, July/August 1999, str. 8-22.
2. Bitenc I., Mayer J., Rajkovič V.: Ugotavljanje primernosti za vodenje s pomočjo ekspertnega sistema. Zbornik 19. posvetovanja organizatorjev dela. Kranj : Moderna organizacija, 2000, str. 493-497.
3. Bohanec M.: DEX: An Expert System Shell for Multi-Attribute Decision Making, User's Manual (Software version 1.00ITR). Report DP-5896. Jožef Stefan Institute, 1990.
4. Bohanec M.: Introduction to DEX - An Expert System Shell for Multi - Attribute Decision Making. Report DP-6420. Jožef Stefan Institute, 1991.
5. Bohanec M., Rajkovič V.: DEX: An Expert System Shell for Decision Support. Sistematica 1, 1990, str. 145-157.
6. Bohanec M., Rajkovič V.: Večparameterski odločitveni modeli. Organizacija in kadri 7/95, str. 427-439.
7. Bohanec M., Rajkovič V.: Multi-attribute decision modeling: Industrial applications of DEX. Informatica 23, 1999, str. 487-491.
8. Bohanec M., Urh B., Rajkovič V.: DEX: Evaluating options by combined qualitative and quantitative methods. Acta Psychologica 80, North-Holland, 1992, str. 67-89.
9. Bohanec M., Zupan B., Rajkovič V.: Hierarhični odločitveni modeli in njihova uporaba v zdravstvu. CADAM-97. Bled, 12. november 1997.
10. Bratko I.: Inteligentni informacijski sistemi. 4. izdaja. Fakulteta za elektrotehniko, Ljubljana, 1984, 106 str.
11. Brazier M.: Electronic Records & Signatures. Regulatory Affairs Journals Ltd 2001, 2001, str. 284-295.
12. Clemen R. T.: Making Hard Decisions. An Introduction to Decision Analysis. 2nd Edition. Pacific Groove: Brooks/Cole Publishing Company - A Division of the International Thomson Publishing Inc., 1996, 664 str.
13. Dayton N. A.: A Practical Approach to Compliance for 21CFR Part11 - Electronic records/Electronic Signatures. [URL: http://www.ivthome.com/free/21cfr.htm], 01.09.2001.
14. Deitz D.: Addresing 21CFR Part11 Requirements with an Automated Configuration Audit Trail and Version Management System. Pharmaceutical Engineering, March/April 2001, str. 38-48.
15. Efstathiou J., Rajkovič V.: Multiattribute Decisionmaking Using a Fuzzy Heuristic Approach. IEEE Transaction on Systems, Man and Cybernetics, Vol. SMC-9, No. 6, June 1979, str. 326-333.
16. Keatley L. K.: A Review of US and FDA Requirements for Electronic records, Electronic Signatures, and Electronic Submissions. Quality Assurance, 7, 1999, str. 77-89.
17. Mallach E. G.: Understanding Decision Support Systems and Expert Systems. Richard D. Irwin Inc., 1994, 695 str.
18. Možina S. et al.: Management. Radovljica : Didakta, 1994, str. 212-264.
19. Pivec M., Rajkovič V.: Obvladovanje znanja z metodami umetne inteligence. Organizacija, št. 8-9, oktober-november 1999, str. 449-452.
20. Rajkovič V. et al.: Kako storiti več za kakovost zdravstva in šolstva? Modra knjiga: Civilna družba v Sloveniji in Evropi. Ljubljana : Društvo občanski forum, Služba vlade RS za evropske zadeve, 1999, str. 386-395.

21. Rajkovič V., Bohanec M., Bitenc I.: Sistemi za podporo odločanju. [URL: ftp://lopes1.fov.uni-mb.si/pub/odlocanje/SPO.zip], 13. 6. 2001.
22. Rozman R., Kovač J., Koletnik F.: Management. Gospodarski vestnik, Ljubljana, 1993, str. 25-37.
23. Sprague R. H. Jr., Watson H. J.: Decison Support for Management. New Jersey : Prentice Hall Inc., 1996, 490 str.
24. Teuchert V.: Operation and Maintenance of Process Control Systems in the Pharmaceutical Industry – Standard Operating Procedures According to VDI/VDE 3517. Part 4. Pharmaceutical Engineering, November/December 2000, str. 18-32.
25. Zimmerman H. J.: Fuzzy Sets, Decision Making and Expert Systems. Boston : Kluwer Academic Publishers, 1987, 335 str.
26. Zornada L., Bohanec M., Rajkovič V.: Model lupine ekspertnega sistema za podporo odločanju. Zbornik 19. posvetovanja organizatorjev dela. Kranj : Moderna organizacija, 2000, str. 516-525.

8. Viri

1. Avtomatika. Metronikova izdaja revije o avtomatizaciji procesov. Junij, 2001.
2. Complying with 21CFR Part 11 Electronic Records and Electronic Signatures, Final Draft, GAMP Special Interest Group, 1 september 2000.
3. Computerized Systems Used in Clinical Trials. Giudance for Industry. FDA. [http:// www.fda.gov/ora/compliance_ref/bimo/ffinalcct.htm], 01.09.2001.
4. E-Records Technology Gap is Closing, But Implementation Poses Challenges, "The Gold Sheet". Pharmaceutical & Biotechnology Quality Control, Vol. 34, No. 10, October 2000, str. 1-24.
5. Enforcement Policy: 21CFR Part11; Electronic Records; Electronic Signatures, Compliance Policy Guide. Section 160.850. FDA. [http://www.fda.gov/ora/compliance_ref/cpg/ cpggenl/cpg160-850.htm], 01.09.2001.
6. GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture. Version: V3.0, Volume 1, GAMP Forum, ISPE, March 1998.
7. GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture, Version: V3.0, Volume2, GAMP Forum, ISPE, March 1998.
8. Good Practices for Computerised Systems in Regulated "GXP" Environments, Pharmaceutical Inspection Convention, 14 January 2002.
9. Guidance to Industry on Electronic Records, Food and Drug Administration, International Pharmaceutical Regulatory Monitor, October 2001
10. Guidance for Industry, 21 CFR Part11; Electronic Records; Electronic Signatures, Time Stamps, Food and Drug Administration, February 2002.
11. Guidelines on General Principles of Process Validation, Food and Drug Administration, May 1987.
12. Tablet Testing System, Kraemer Electronic, [URL: http://www.advpr.com/products/ process/km0001_compulab_01.html], 01.02.2002.
13. The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practices, European Commission, Directorate General III, Edition 1997.
14. Title 21, Food and Drugs, Part11, "Electronic Records; Electronic Signatures: Final Rule." Food and Drug Administration, Code of Federal Regulations, FDA Federal Register 62 (54), 13429-66, 1997.

15. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001).
16. Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št.: 57/2000).

9. Slovar izrazov

C		
CFR	Code of Federal Regulation	Ameriška zvezna regulativa
D		
DSS	Digital Signature Standard	Standard za digitalni podpis
DEX	Decision Expert	Inf. sistem za podporo odločanju
E		
EDMS	Electronic Document Management System	Inf. sistem za upravljanje z dokumenti
F		
FDA	Food and Drug Adminstration	(Ameriška) uprava za hrano in zdravila
G		
GMP	Good Manufacturing Practice	Dobra proizvodna praksa
GLP	Good Laboratory Practice	Dobra laboratorijska praksa
GCP	Good Clinical Practice	Dobra klinična praksa
GXP	Good Practices	Dobre prakse
L		
LIMS	Laboratory Information Management System	Informacijski sistem za vodenje laboratorijev
M		
MRP	Material Resource Planning	Inf. sistem za materialno poslovanje
MES	Manufacturing Execution System	Inf. sistem za vodenje proizvodnje
N		
NIST	National Institute of Standards and Technology	Ameriški nacionalni inštitut za standarde in tehnologijo
O		
OP	Operating Panel	Krmilni tablo
P		
PLC	Programmable Logical Controller	Programabilni logični krmilnik
S		
SCADA	Supervisory Control And Data Aquisition	Inf. sistem za nadzor sistemov in zbiranje podatkov

Dodatki

A. Zaloga vrednosti kriterijev

Kriterij	Zaloga vrednosti
Kritičnost računalniškega sistema	zelo kritičen; precej kritičen; srednje kritičen; manj kritičen; nekritičen
├ GXP kritičnost sistema	visoka; srednja; mala
│ ├ Vpliv na kvaliteto izdelka	neposredni; posredni; ni vpliva
│ └ Odprtost sistema	dostopen; delno dostopen; nedostopen
└ Skladnost z regulativo	neskladen; manj skladen; srednje skladen; precej skladen; popolno skladen
├ Klasifikacija sistema	zapisi in podpisi; samo zapisi; ni zapisov ni podpisov
├ Elektronski zapisi	neskladen; manj skladen; srednje skladen; precej skladen; popolno skladen
│ ├ Validacija elektronskih zapisov	Ne; Delno; Da
│ │ ├ Validacija sistema glede na industrijske standarde	Slaba; Delna; Dobra
│ │ │ ├ Specifikacije	Neustrezne; Povprečne; Ustrezne
│ │ │ │ ├ Zahteve uporabnika	Neustrezne; Povprečne; Ustrezne
│ │ │ │ ├ Ocena dobavitelja	Slaba; Delna; Dobra
│ │ │ │ └ Programska in strojna specifikacija	Slaba; Delna; Dobra
│ │ │ ├ Kvalifikacija	Slaba; Delna; Dobra
│ │ │ │ ├ Kvalifikacija načrtovanja - DQ	Slaba; Delna; Dobra
│ │ │ │ ├ Kvalifikacija montaže - IQ	Slaba; Delna; Dobra
│ │ │ │ ├ Kvalifikacija obratovanja - OQ	Slaba; Delna; Dobra
│ │ │ │ └ Kvalifikacija delovanja - PQ	Slaba; Delna; Dobra
│ │ │ ├ Postopki	Ne; Delno; Da
│ │ │ │ ├ Validacijski protokol	Ne; Delno; Da
│ │ │ │ ├ Poročilo o validaciji	Ne; Delno; Da
│ │ │ │ └ Sistemski splošni postopki	Ne; Delno; Da
│ │ │ │ ├ Delovanje sistema	Ne; Delno; Da
│ │ │ │ └ Administracija sistema	Ne; Delno; Da
│ │ │ │ ├ Periodični pregled sistema	Ne; Delno; Da
│ │ │ │ ├ Arhiviranje, varnostno kopiranje, restavracija sistema in zapisov	Ne; Delno; Da
│ │ │ │ └ Konfiguracija sistema in zaščit	Ne; Delno; Da
│ │ │ └ Izobraževanje	Ne; Delno; Da
│ │ │ ├ Uporabniki, sistemski administratorji	Ni izvedeno; Izvedeno
│ │ │ ├ Razvijalci, interni presojevalci, zunanji	Ni izvedeno; Izvedeno
│ │ │ └ Dokumentiranost	Ni; Je
│ │ └ Validacija glede na regulativo o elektronskih podpisih in zapisih	Ne; Delno; Da
│ │ ├ Neveljavni, spremenjeni zapisi	Ne; Delno; Da
│ │ │ ├ Neveljavni vnosi	Ne; Delno; Da
│ │ │ ├ Sposobnost razlikovanja spremenjenih zapisov	Ne; Da
│ │ │ └ Test razlikovanja spremenjenih zapisov	Ne; Da

├ Generiranje kopij elektronskih zapisov	Ne; Delno; Da
│ ├ Prikaz v elektronski obliki	Ni; Je
│ ├ Prikaz v obliki izpisa	Ni; Je
│ └ Prenašanje v elektronski obliki	Ni; Je
└ Ostale zahteve za validacijo elektronskih zapisov	Ne; Delno; Da
├ Zgodovina dogodkov	Ne; Delno; Da
├ Zaporedje dogodkov	Ne; Delno; Da
└ Zaščita zapisov in dostopa	ni izvedeno; delno izvedeno; izvedeno
├ Testiranje dostopa in avtorizacij	ni izvedeno; delno izvedeno; izvedeno
├ Testiranje arhiviranja in restavracije zapisov	ni izvedeno; delno izvedeno; izvedeno
└ Test naprav, ki so vir vhodnih podatkov	ni izvedeno; delno izvedeno; izvedeno
├ Zaščita	slabo urejeno; povprečno; dobro urejeno
├ Nadzor	slab; povprečen; dober
├ Pregledi zapisov	nikoli; včasih; redno
├ Uporabnika	nikoli; včasih; redno
├ Administratorja	nikoli; včasih; redno
└ Upravljanja kakovosti	nikoli; včasih; redno
├ Zaporedje dogodkov	Ne; Delno; Da
├ Vsiljeno zaporedje dogodkov	Ne; Delno; Da
└ Avtomatski mehanizem sekvenc	Ne; Delno; Da
└ Preverjanje naprav	ni izvedeno; delno izvedeno; izvedeno
├ Preverjanje vira vhodnih podatkov	Ne; Delno; Da
└ Periodično testiranje naprav	ni izvedeno; delno izvedeno; izvedeno
├ Zaščita zapisov	slabo urejeno; povprečno; dobro urejeno
├ Arhiviranje	slabo urejeno; povprečno; dobro urejeno
├ Restavracija	slabo urejeno; povprečno; dobro urejeno
├ Glede na čas	Več kot 1 dan; 15 minut-1 dan; manj kot 15 minut
├ Glede na celovitost podatkov	neustrezno; ustrezno
└ Periodično testiranje restavracije	ni izvedeno; delno izvedeno; izvedeno
└ Zaščita zapisov glede na lokacijo	Slaba; Delna; Dobra
├ Na sistemu	Slaba; Delna; Dobra
├ Na arhivskem mediju	Slaba; Delna; Dobra
└ Perioda arhiviranja	več kot 1 dan; 5 minut - 1 dan; manj kot 5 minut
└ Zaščita dostopa	slabo urejeno; povprečno; dobro urejeno
├ Fizični dostop	neomejen; delno omejen; omejen
├ Arhiv konfiguracije zaščit	Ni; Je
└ Logični dostop	slabo urejeno; povprečno; dobro urejeno
├ Avtorizacije	slabo urejeno; povprečno; dobro urejeno
│ ├ Način avtorizacije dostopa	nekontroliran; delno kontroliran ; kontroliran
│ ├ Preverjanje avtorizacije za izvedbo podpisa	Ne; Da
│ └ Preverjanje avtorizacije pri uporabi sistema	Ne; Delno; Da

└ Dostop do sistema	neomejen; delno omejen; omejen
├ Operacijski sistem	Ne; Da
├ Avtomatska odjava	Ni; Je
└ Aplikacija	neomejen; delno omejen; omejen
├ Večnivojski dostop	Ni izvedeno; Izvedeno
├ Prikritost gesel, minimalna dolžina gesel	Ni izvedeno; Izvedeno
└ Uporabniški računi	slabo urejeno; povprečno; dobro urejeno
├ Potek uporabniškega računa	Ne; Da
├ Periodično pregledovanje računov	Ne; Delno; Da
└ Detekcija nepooblaščenih poizkusov dostopa	Ne; Delno; Da
├ Zgodovina dogodkov	slabo urejeno; povprečno; dobro urejeno
├ Ročna zgodovina dogodkov	Slaba; Delna; Dobra
└ Računalniško generirana zgodovina dogodkov	Slaba; Delna; Dobra
├ Ohranitev zgodovine dogodkov	Slaba; Delna; Dobra
├ Varna povezava med zapisom in zgodovino dogodkov	Ni; Je
├ Zaščita pred spremembo, prenosom, brisanjem	Ne; Delno; Da
└ Arhiviranje, restavracija zgodovine dogodkov	Ne; Delno; Da
├ Časovna značka	slabo urejeno; povprečno; dobro urejeno
├ Možnost spremembe	Je možno; Ni možno
└ Periodična verifikacija	Ne; Da
└ Ustreznost zgodovine dogodkov	Ne; Delno; Da
├ Možnost izklopa zgodovine dogodkov	Je možno; Delno je možno; Ni možno
├ Operater	Je možno; Ni možno
└ Administrator	Je možno; Ni možno
├ Dogodki v zapisu zgodovine	Ne; Delno; Da
├ Kreacija	Ne; Da
├ Sprememba	Ne; Da
└ Brisanje	Ne; Da
├ Prikaz zgodovine dogodkov	Ne; Delno; Da
├ Elektronski	Ne; Da
├ Izpis	Ne; Da
└ Prenašanje v elektronski obliki	Ne; Da
└ Parametri	Ne; Delno; Da
├ Tip sistema	industrijski; laboratorijski
├ Namen spremembe	Ne; Da
└ Industrijski parametri	Ne; Delno; Da
├ Datum in čas	Ne; Da
├ Tiskano ime posameznika	Ne; Da
└ Staro in novo stanje	Ne; Da

└ Sistemska dokumentacija	slabo urejeno; povprečno; dobro urejeno
├ Nadzor nad uporabo in vzdrževanjem - kontrola dostopa	Slaba; Delna; Dobra
└ Kontrola sprememb	slabo urejeno; povprečno; dobro urejeno
├ Kontrola verzij dokumentov	Ni; Je
├ Pretečena dokumentacija - odstranitev, arhiviranje	Ne; Delno; Da
└ Zgodovina dogodkov	Slaba; Delna; Dobra
├ Možnost pregledovanja, inšpekcije	Ne; Da
├ Ohranitev povezave	Ne; Da
├ Povezava zgodovine z dokumentacijo	Ne; Da
└ Elementi zgodovine dogodkov	Ne; Delno; Da
├ Datum in čas	Ne; Da
├ Tiskano ime posameznika	Ne; Delno; Da
└ Staro in novo stanje	Ne; Delno; Da
└ Elektronski podpisi	neskladen; manj skladen; srednje skladen; precej skladen; popolno skladen
├ Validacija elektronskega podpisa	Slaba; Delna; Dobra
├ Validacija izvedbe in prikaza podpisa	Ne; Delno; Da
├ Validacija povezave podpis/zapis	Ne; Delno; Da
└ Validacija zahtev in nadzora podpisa	Ne; Delno; Da
├ Prikaz podpisa	slabo urejeno; povprečno; dobro urejeno
├ Vsebina prikaza	Ne; Delno; Da
├ Datum in čas	Ni; Je
├ Tiskano ime posameznika	Ni; Je
└ Namen podpisa	Ni; Je
└ Zaščita prikaza	Slaba; Delna; Dobra
├ Dostop do prikaza podpisa	Ne; Delno; Da
├ Zgodovina dogodkov pri spremembah prikaza	Ne; Delno; Da
└ Nadzor prikaza podpisa	Ne; Delno; Da
├ Povezava podpis/zapis	slabo urejeno; povprečno; dobro urejeno
├ Varnost povezave	Slaba; Delna; Dobra
└ Ukrepi za ohranitev povezave	Ne; Delno; Da
└ Zahteve in nadzor podpisa	slabo urejeno; povprečno; dobro urejeno
├ Enkratnost elektronskega podpisa	slabo urejeno; povprečno; dobro urejeno
├ Enak elektronski podpis	Je možno; Ni možno
├ Kasnejša dodelitev enakega elektronskega podpisa	Je možno; Ni možno
└ Ustrezen dokumentiran nadzor dodelitve EP	Ni; Je
├ Nadzor identifikacijskih kod in gesel	slab; povprečen; dober
├ Zaščita in integriteta	Ne; Delno; Da
├ Enkratnost identifikacijskih kod	Ne; Da
├ Periodično pregledovanje	Ne; Da
└ Časovni potek gesel	Ne; Da

├ Kartice, žetoni, naprave	Ne; Delno; Da
│ ├ Postopki za izdajo	Ne; Da
│ ├ Začetno testiranje	Ne; Da
│ └ Periodično testiranje	Ne; Da
└ Nepooblaščen dostop	Ne; Delno; Da
├ Odkrivanje	Ne; Da
├ Poročanje in ukrepanje	Ne; Da
└ Avtomatske blokade	Ne; Da
└ Nebiometrični podpis	slabo urejeno; povprečno; dobro urejeno
├ Administracija in izvedba EP	slabo urejeno; povprečno; dobro urejeno
├ Zaščita datotek z vsebino podpisa	Slaba; Delna; Dobra
├ Zaščita gesla pred administratorjem	Ni; Je
└ Minimalna dolžina gesla	Ni izvedeno; Izvedeno
├ Postopki in procedure	Ne; Delno; Da
├ So napisani	Ne; Da
├ Izobraženost	Ne; Da
└ Se izvajajo	Ne; Da
└ Neprekinjen dostop	slabo urejeno; povprečno; dobro urejeno
├ Je definiran	Ne; Da
├ Uporabniki so izobraženi	Ne; Da
└ Uporaba	neustrezno; delno ustrezno; ustrezno
├ Dve komponenti podpisa za prvi podpis - prijavo	Ne; Da
├ Samo geslo ob neprekinjenem dostopu	Ne; Da
└ Tehnične kontrole	Neustrezne; Povprečne; Ustrezne
├ Ohranjevalnik zaslona	Ne; Da
├ Avtomatska odjava	Ne; Da
└ Nivoja operacijskega sistema in aplikacije	Ne; Delno; Da

B. Tabele odločitvenih pravil

GXP	kritičnost sistema 48%	Skladnost z regulativo 52%	**Kritičnost računalniškega sistema**
1	visoka	neskladen	zelo kritičen
2	visoka	manj skladen	precej kritičen
3	srednja	neskladen	precej kritičen
4	visoka	srednje skladen	srednje kritičen
5	srednja	manj skladen	srednje kritičen
6	mala	neskladen	srednje kritičen
7	visoka	precej skladen	manj kritičen
8	srednja	srednje skladen	manj kritičen
9	mala	manj skladen	manj kritičen
10	*	popolno skladen	nekritičen
11	>=srednja	>=precej skladen	nekritičen
12	mala	>=srednje skladen	nekritičen

	Vpliv na kvaliteto izdelka 75%	Odprtost sistema 25%	**GXP kritičnost sistema**
1	neposredni	*	visoka
2	<=posredni	dostopen	visoka
3	posredni	delno dostopen	srednja
4	>=posredni	nedostopen	mala
5	ni vpliva	*	mala

	Klasifikacija sistema	Elektronski zapisi	Elektronski podpisi	**Skladnost z regulativo**
	63%	28%	9%	
1	zapisi in podpisi	<=srednje skladen	neskladen	neskladen
2	<=samo zapisi	neskladen	neskladen	neskladen
3	<=samo zapisi	neskladen	>=precej skladen	neskladen
4	samo zapisi	neskladen	*	neskladen
5	zapisi in podpisi	<=manj skladen	manj skladen	manj skladen
6	<=samo zapisi	manj skladen	manj skladen	manj skladen
7	zapisi in podpisi	>=precej skladen	neskladen	manj skladen
8	samo zapisi	manj skladen	*	manj skladen
9	zapisi in podpisi	manj skladen:precej skladen	srednje skladen	srednje skladen
10	zapisi in podpisi	srednje skladen:precej skladen	manj skladen:srednje skladen	srednje skladen
11	zapisi in podpisi	>=srednje skladen	manj skladen	srednje skladen
12	<=samo zapisi	srednje skladen	manj skladen:srednje skladen	srednje skladen
13	samo zapisi	srednje skladen	*	srednje skladen
14	zapisi in podpisi	srednje skladen:precej skladen	>=precej skladen	precej skladen
15	zapisi in podpisi	>=srednje skladen	precej skladen	precej skladen
16	zapisi in podpisi	popolno skladen	srednje skladen:precej skladen	precej skladen
17	samo zapisi	precej skladen	*	precej skladen
18	*	popolno skladen	popolno skladen	popolno skladen
19	>=samo zapisi	popolno skladen	*	popolno skladen
20	ni zapisov ni podpisov	*	*	popolno skladen

	Validacija elektronskih zapisov	Zaščita	Zgodovina dogodkov	Sistemska dokumentacija	**Elektronski zapisi**
	24%	30%	25%	21%	
1	Ne	slabo urejeno	slabo urejeno	*	neskladen
2	Ne	slabo urejeno	<=povprečno	slabo urejeno	neskladen
3	Ne	<=povprečno	slabo urejeno	slabo urejeno	neskladen
4	<=Delno	slabo urejeno	slabo urejeno	<=povprečno	neskladen
5	Ne	slabo urejeno	>=povprečno	>=povprečno	manj skladen
6	Ne	<=povprečno	povprečno	povprečno	manj skladen
7	<=Delno	slabo urejeno	povprečno	povprečno	manj skladen
8	Ne	slabo urejeno	dobro urejeno	*	manj skladen
9	Ne	<=povprečno	dobro urejeno	slabo urejeno	manj skladen
10	<=Delno	slabo urejeno	dobro urejeno	slabo urejeno	manj skladen
11	Ne	povprečno	slabo urejeno	>=povprečno	manj skladen
12	Ne	povprečno	povprečno	<=povprečno	manj skladen
13	Ne	povprečno	>=povprečno	slabo urejeno	manj skladen
14	<=Delno	povprečno	povprečno	slabo urejeno	manj skladen
15	Delno	slabo urejeno	slabo urejeno	dobro urejeno	manj skladen
16	<=Delno	povprečno	dobro urejeno	povprečno	srednje skladen
17	Ne	dobro urejeno	<=povprečno	dobro urejeno	srednje skladen
18	<=Delno	dobro urejeno	slabo urejeno	dobro urejeno	srednje skladen
19	Ne	dobro urejeno	povprečno	*	srednje skladen
20	Ne	dobro urejeno	>=povprečno	<=povprečno	srednje skladen
21	<=Delno	dobro urejeno	povprečno	<=povprečno	srednje skladen
22	<=Delno	dobro urejeno	>=povprečno	slabo urejeno	srednje skladen
23	*	dobro urejeno	povprečno	slabo urejeno	srednje skladen
24	Delno	<=povprečno	dobro urejeno	povprečno	srednje skladen
25	Delno	povprečno	>=povprečno	povprečno	srednje skladen
26	Delno	povprečno	dobro urejeno	<=povprečno	srednje skladen
27	Da	slabo urejeno	>=povprečno	>=povprečno	srednje skladen
28	Da	<=povprečno	povprečno	povprečno	srednje skladen
29	>=Delno	povprečno	dobro urejeno	dobro urejeno	precej skladen
30	Da	povprečno	>=povprečno	dobro urejeno	precej skladen
31	Da	povprečno	dobro urejeno	>=povprečno	precej skladen
32	Da	dobro urejeno	povprečno	>=povprečno	precej skladen
33	Da	dobro urejeno	dobro urejeno	slabo urejeno	precej skladen
34	>=Delno	dobro urejeno	dobro urejeno	dobro urejeno	popolno skladen
35	Da	dobro urejeno	dobro urejeno	>=povprečno	popolno skladen

	Validacija sistema glede na industrijske standarde	Validacija glede na regulativo o elektronskih podpisih in zapisih	**Validacija elektronskih zapisov**
	50%	50%	
1	Slaba	<=Delno	Ne
2	<=Delna	Ne	Ne
3	>=Delna	Da	Da
4	Dobra	>=Delno	Da

	Specifikacije	Kvalifikacija	Postopki	Izobraževanje	**Validacija sistema glede na industrijske standarde**
	37%	38%	17%	8%	
1	Neustrezne	<=Delna	<=Delno	Ne	Slaba
2	Neustrezne	*	Ne	*	Slaba
3	<=Povprečne	Slaba	*	*	Slaba
4	*	Slaba	Ne	Ne	Slaba
5	Povprečne	>=Delna	*	*	Delna
6	>=Povprečne	Delna	*	*	Delna
7	>=Povprečne	>=Delna	Ne	*	Delna
8	>=Povprečne	>=Delna	*	Ne	Delna
9	Ustrezne	Dobra	>=Delno	>=Delno	Dobra

	Zahteve uporabnika	Ocena dobavitelja	Programska in strojna specifikacija	**Specifikacije**
	24%	14%	62%	
1	Neustrezne	*	<=Delna	Neustrezne
2	<=Povprečne	Slaba	<=Delna	Neustrezne
3	*	*	Slaba	Neustrezne
4	Neustrezne	*	Dobra	Povprečne
5	*	Slaba	Dobra	Povprečne
6	>=Povprečne	>=Delna	Delna	Povprečne
7	>=Povprečne	>=Delna	Dobra	Ustrezne

	Kvalifikacija načrtovanja - DQ	Kvalifikacija montaže - IQ	Kvalifikacija obratovanja - OQ	Kvalifikacija delovanja - PQ	**Kvalifikacija**
	25%	25%	25%	25%	
1	Slaba	Slaba	Slaba	*	Slaba
2	Slaba	Slaba	<=Delna	<=Delna	Slaba
3	Slaba	Slaba	*	Slaba	Slaba
4	Slaba	<=Delna	Slaba	<=Delna	Slaba
5	Slaba	<=Delna	<=Delna	Slaba	Slaba
6	Slaba	*	Slaba	Slaba	Slaba
7	<=Delna	Slaba	Slaba	<=Delna	Slaba
8	<=Delna	Slaba	<=Delna	Slaba	Slaba
9	<=Delna	<=Delna	Slaba	Slaba	Slaba
10	*	Slaba	Slaba	Slaba	Slaba
11	*	Dobra	Dobra	Dobra	Dobra
12	>=Delna	>=Delna	Dobra	Dobra	Dobra
13	>=Delna	Dobra	>=Delna	Dobra	Dobra
14	>=Delna	Dobra	Dobra	>=Delna	Dobra
15	Dobra	*	Dobra	Dobra	Dobra
16	Dobra	>=Delna	>=Delna	Dobra	Dobra
17	Dobra	>=Delna	Dobra	>=Delna	Dobra
18	Dobra	Dobra	*	Dobra	Dobra
19	Dobra	Dobra	>=Delna	>=Delna	Dobra
20	Dobra	Dobra	Dobra	*	Dobra

	Validacijski protokol	Poročilo o validaciji	Sistemski splošni postopki	**Postopki**
	33%	33%	33%	
1	Ne	Ne	*	Ne
2	Ne	<=Delno	<=Delno	Ne
3	Ne	*	Ne	Ne
4	<=Delno	Ne	<=Delno	Ne
5	<=Delno	<=Delno	Ne	Ne
6	*	Ne	Ne	Ne
7	>=Delno	Ne	Da	Delno
8	Delno	Delno	>=Delno	Delno
9	Delno	>=Delno	Delno	Delno
10	>=Delno	Delno	Delno	Delno
11	>=Delno	Da	Ne	Delno
12	Da	Ne	>=Delno	Delno
13	Da	>=Delno	Ne	Delno
14	>=Delno	Da	Da	Da
15	Da	>=Delno	Da	Da

	Delovanje sistema	Administracija sistema	**Sistemski splošni postopki**
	50%	50%	
1	Ne	<=Delno	Ne
2	<=Delno	Ne	Ne
3	Da	<=Delno	Delno
4	Da	Da	Da

	Periodični pregled sistema	Arhiviranje, varnostno kopiranje, restavracija sistema in zapisov	Konfiguracija sistema in zaščit	**Administracija sistema**
	27%	33%	40%	
1	<=Delno	Ne	Ne	Ne
2	Ne	*	>=Delno	Delno
3	<=Delno	*	Delno	Delno
4	*	Ne	>=Delno	Delno
5	*	<=Delno	Delno	Delno
6	Ne	>=Delno	*	Delno
7	<=Delno	>=Delno	<=Delno	Delno
8	*	Delno	<=Delno	Delno
9	*	>=Delno	Ne	Delno
10	Da	Ne	*	Delno
11	Da	<=Delno	<=Delno	Delno
12	Da	*	Ne	Delno
13	>=Delno	>=Delno	Da	Da
14	Da	Da	>=Delno	Da

	Uporabniki, sistemski administratorji	Razvijalci, interni presojevalci, zunanji	Dokumentiranost	**Izobraževanje**
	33%	33%	33%	
1	Ni izvedeno	Ni izvedeno	*	Ne
2	Ni izvedeno	*	Ni	Ne
3	*	Ni izvedeno	Ni	Ne
4	Ni izvedeno	Izvedeno	Je	Delno
5	Izvedeno	Ni izvedeno	Je	Delno
6	Izvedeno	Izvedeno	Je	Da

	Neveljavni, spremenjeni zapisi	Generiranje kopij elektronskih zapisov	Ostale zahteve za validacijo elektronskih zapisov	**Validacija glede na regulativo o elektronskih podpisih in zapisih**
	53%	24%	24%	
1	Ne	Ne	*	Ne
2	Ne	<=Delno	<=Delno	Ne
3	Ne	*	Ne	Ne
4	<=Delno	>=Delno	Da	Delno
5	<=Delno	Da	>=Delno	Delno
6	Delno	*	*	Delno
7	>=Delno	Ne	*	Delno
8	>=Delno	<=Delno	<=Delno	Delno
9	>=Delno	*	Ne	Delno
10	Da	>=Delno	Da	Da
11	Da	Da	>=Delno	Da

	Neveljavni vnosi	Sposobnost razlikovanja spremenjenih zapisov	Test razlikovanja spremenjenih zapisov	**Neveljavni, spremenjeni zapisi**
	33%	33%	33%	
1	Ne	Ne	*	Ne
2	Ne	*	Ne	Ne
3	<=Delno	Ne	Ne	Ne
4	<=Delno	Da	Da	Delno
5	Da	Ne	*	Delno
6	Da	*	Ne	Delno
7	Da	Da	Da	Da

	Prikaz v elektronski obliki	Prikaz v obliki izpisa	Prenašanje v elektronski obliki	**Generiranje kopij elektronskih zapisov**
	33%	33%	33%	
1	Ni	Ni	Ni	Ne
2	Ni	*	Je	Delno
3	*	Ni	Je	Delno
4	*	Je	Ni	Delno
5	Je	*	Ni	Delno
6	Je	Je	Je	Da

	Zgodovina dogodkov	Zaporedje dogodkov	Zaščita zapisov in dostopa	**Ostale zahteve za validacijo elektronskih zapisov**
	38%	15%	46%	
1	Ne	<=Delno	ni izvedeno	Ne
2	<=Delno	Ne	ni izvedeno	Ne
3	<=Delno	*	>=delno izvedeno	Delno
4	*	*	delno izvedeno	Delno
5	Delno	>=Delno	*	Delno
6	>=Delno	>=Delno	<=delno izvedeno	Delno
7	Da	*	<=delno izvedeno	Delno
8	Da	*	izvedeno	Da

	Testiranje dostopa in avtorizacij	Testiranje arhiviranja in restavracije zapisov	Test naprav, ki so vir vhodnih podatkov	**Zaščita zapisov in dostopa**
	60%	35%	5%	
1	ni izvedeno	<=delno izvedeno	*	ni izvedeno
2	<=delno izvedeno	ni izvedeno	ni izvedeno	ni izvedeno
3	<=delno izvedeno	izvedeno	*	delno izvedeno
4	delno izvedeno	*	>=delno izvedeno	delno izvedeno
5	>=delno izvedeno	ni izvedeno	>=delno izvedeno	delno izvedeno
6	delno izvedeno	>=delno izvedeno	*	delno izvedeno
7	izvedeno	ni izvedeno	*	delno izvedeno
8	izvedeno	>=delno izvedeno	*	izvedeno

	Nadzor	Zaščita zapisov	Zaščita dostopa	**Zaščita**
	25%	38%	38%	
1	slab	slabo urejeno	*	slabo urejeno
2	slab	*	slabo urejeno	slabo urejeno
3	<=povprečen	slabo urejeno	<=povprečno	slabo urejeno
4	<=povprečen	<=povprečno	slabo urejeno	slabo urejeno
5	*	slabo urejeno	slabo urejeno	slabo urejeno
6	<=povprečen	povprečno	>=povprečno	povprečno
7	<=povprečen	>=povprečno	povprečno	povprečno
8	*	povprečno	povprečno	povprečno
9	dober	slabo urejeno	>=povprečno	povprečno
10	dober	<=povprečno	povprečno	povprečno
11	*	dobro urejeno	dobro urejeno	dobro urejeno

	Pregledi zapisov	Zaporedje dogodkov	Preverjanje naprav	**Nadzor**
	33%	33%	33%	
1	nikoli	Ne	<=delno izvedeno	slab
2	nikoli	<=Delno	ni izvedeno	slab
3	<=včasih	Ne	ni izvedeno	slab
4	>=včasih	Da	izvedeno	dober
5	redno	>=Delno	izvedeno	dober
6	redno	Da	>=delno izvedeno	dober

	Uporabnika	Administratorja	Upravljanja kakovosti	**Pregledi zapisov**
	33%	33%	33%	
1	nikoli	nikoli	<=včasih	nikoli
2	nikoli	<=včasih	nikoli	nikoli
3	<=včasih	nikoli	nikoli	nikoli
4	>=včasih	redno	redno	redno
5	redno	>=včasih	redno	redno
6	redno	redno	>=včasih	redno

	Vsiljeno zaporedje dogodkov	Avtomatski mehanizem sekvenc	**Zaporedje dogodkov**
	50%	50%	
1	Ne	<=Delno	Ne
2	<=Delno	Ne	Ne
3	>=Delno	Da	Da
4	Da	>=Delno	Da

	Preverjanje vira vhodnih podatkov	Periodično testiranje naprav	**Preverjanje naprav**
	50%	50%	
1	Ne	<=delno izvedeno	ni izvedeno
2	<=Delno	ni izvedeno	ni izvedeno
3	>=Delno	izvedeno	izvedeno
4	Da	>=delno izvedeno	izvedeno

	Arhiviranje	Restavracija	Zaščita zapisov glede na lokacijo	**Zaščita zapisov**
	33%	33%	33%	
1	slabo urejeno	slabo urejeno	<=Delna	slabo urejeno
2	slabo urejeno	<=povprečno	Slaba	slabo urejeno
3	<=povprečno	slabo urejeno	Slaba	slabo urejeno
4	>=povprečno	dobro urejeno	Dobra	dobro urejeno
5	dobro urejeno	>=povprečno	Dobra	dobro urejeno
6	dobro urejeno	dobro urejeno	>=Delna	dobro urejeno

	Glede na čas	Glede na celovitost podatkov	Periodično testiranje restavracije	**Restavracija**
	10%	80%	10%	
1	*	neustrezno	*	slabo urejeno
2	Več kot 1 dan	ustrezno	*	povprečno
3	<=15 minut-1 dan	ustrezno	<=delno izvedeno	povprečno
4	*	ustrezno	ni izvedeno	povprečno
5	>=15 minut-1 dan	ustrezno	izvedeno	dobro urejeno
6	manj kot 15 minut	ustrezno	>=delno izvedeno	dobro urejeno

	Na sistemu	Na arhivskem mediju	Perioda arhiviranja	**Zaščita zapisov glede na lokacijo**
	33%	52%	14%	
1	Slaba	<=Delna	<=5 minut - 1 dan	Slaba
2	<=Delna	Slaba	*	Slaba
3	*	Delna	manj kot 5 minut	Delna
4	<=Delna	Dobra	<=5 minut - 1 dan	Delna
5	Delna	>=Delna	<=5 minut - 1 dan	Delna
6	>=Delna	Delna	*	Delna
7	Dobra	<=Delna	*	Delna
8	*	Dobra	manj kot 5 minut	Dobra
9	Dobra	Dobra	*	Dobra

	Fizični dostop	Arhiv konfiguracije zaščit	Logični dostop	**Zaščita dostopa**
	13%	25%	63%	
1	*	*	slabo urejeno	slabo urejeno
2	<=delno omejen	Ni	>=povprečno	povprečno
3	<=delno omejen	*	povprečno	povprečno
4	*	Ni	povprečno	povprečno
5	*	Je	dobro urejeno	dobro urejeno
6	omejen	*	dobro urejeno	dobro urejeno
7	omejen	Je	>=povprečno	dobro urejeno

	Avtorizacije	Dostop do sistema	**Logični dostop**
	50%	50%	
1	slabo urejeno	*	slabo urejeno
2	*	neomejen	slabo urejeno
3	povprečno	>=delno omejen	povprečno
4	>=povprečno	delno omejen	povprečno
5	dobro urejeno	omejen	dobro urejeno

	Način avtorizacije dostopa	Preverjanje avtorizacije za izvedbo podpisa	Preverjanje avtorizacije pri uporabi sistema	**Avtorizacije**
	34%	45%	20%	
1	nekontroliran	*	*	slabo urejeno
2	*	Ne	<=Delno	slabo urejeno
3	delno kontroliran	*	Da	povprečno
4	>=delno kontroliran	Ne	Da	povprečno
5	delno kontroliran	Da	*	povprečno
6	>=delno kontroliran	Da	<=Delno	povprečno
7	kontroliran	Da	Da	dobro urejeno

	Operacijski sistem	Avtomatska odjava	Aplikacija	**Dostop do sistema**
	33%	33%	33%	
1	Ne	Ni	<=delno omejen	neomejen
2	Ne	*	neomejen	neomejen
3	*	Ni	neomejen	neomejen
4	Da	Je	omejen	omejen

	Večnivojski dostop	Prikritost gesel, minimalna dolžina gesel	Uporabniški računi	**Aplikacija**
	41%	41%	18%	
1	Ni izvedeno	Ni izvedeno	*	neomejen
2	Ni izvedeno	*	slabo urejeno	neomejen
3	*	Ni izvedeno	slabo urejeno	neomejen
4	Ni izvedeno	Izvedeno	>=povprečno	delno omejen
5	Izvedeno	Ni izvedeno	>=povprečno	delno omejen
6	Izvedeno	Izvedeno	slabo urejeno	delno omejen
7	Izvedeno	Izvedeno	>=povprečno	omejen

	Potek uporabniskega računa	Periodično pregledovanje računov	Detekcija nepooblaščenih poizkusov dostopa	**Uporabniški računi**
	54%	23%	23%	
1	Ne	Ne	<=Delno	slabo urejeno
2	Ne	<=Delno	Ne	slabo urejeno
3	Ne	*	Da	povprečno
4	*	Ne	Da	povprečno
5	Ne	>=Delno	>=Delno	povprečno
6	Ne	Da	*	povprečno
7	*	Da	Ne	povprečno
8	Da	Ne	*	povprečno
9	Da	*	Ne	povprečno
10	Da	>=Delno	>=Delno	dobro urejeno

	Ročna zgodovina dogodkov	Računalniško generirana zgodovina dogodkov	**Zgodovina dogodkov**
	50%	50%	
1	Slaba	Slaba	slabo urejeno
2	<=Delna	Delna	povprečno
3	Delna	<=Delna	povprečno
4	*	Dobra	dobro urejeno
5	Dobra	*	dobro urejeno

	Ohranitev zgodovine dogodkov	Časovna značka	Ustreznost zgodovine dogodkov	**Računalniško generirana zgodovina dogodkov**
	35%	13%	52%	
1	Slaba	slabo urejeno	*	Slaba
2	Slaba	*	<=Delno	Slaba
3	*	*	Ne	Slaba
4	Slaba	>=povprečno	Da	Delna
5	<=Delna	povprečno	Da	Delna
6	Delna	<=povprečno	>=Delno	Delna
7	Delna	*	Delno	Delna
8	>=Delna	<=povprečno	Delno	Delna
9	>=Delna	dobro urejeno	Da	Dobra
10	Dobra	*	Da	Dobra
11	Dobra	dobro urejeno	>=Delno	Dobra

	Varna povezava med zapisom in zgodovino dogodkov	Zaščita pred spremembo, prenosom, brisanjem	Arhiviranje, restavracija zgodovine dogodkov	**Ohranitev zgodovine dogodkov**
	31%	35%	35%	
1	Ni	Ne	<=Delno	Slaba
2	Ni	<=Delno	Ne	Slaba
3	*	Ne	Ne	Slaba
4	*	Da	Da	Dobra
5	Je	>=Delno	Da	Dobra
6	Je	Da	>=Delno	Dobra

	Možnost spremembe	Periodična verifikacija	**Časovna značka**
	50%	50%	
1	Je možno	Ne	slabo urejeno
2	Je možno	Da	povprečno
3	Ni možno	Ne	povprečno
4	Ni možno	Da	dobro urejeno

	Možnost izklopa zgodovine dogodkov	Dogodki v zapisu zgodovine	Prikaz zgodovine dogodkov	Parametri	**Ustreznost zgodovine dogodkov**
	10%	25%	29%	36%	
1	<=Delno je možno	Ne	<=Delno	*	Ne
2	<=Delno je možno	Ne	*	<=Delno	Ne
3	<=Delno je možno	*	*	Ne	Ne
4	*	Ne	<=Delno	<=Delno	Ne
5	*	<=Delno	Ne	*	Ne
6	*	<=Delno	*	Ne	Ne
7	*	*	Ne	<=Delno	Ne
8	*	*	<=Delno	Ne	Ne
9	Je možno	*	Da	Da	Delno
10	*	<=Delno	Da	Da	Delno
11	Je možno	>=Delno	>=Delno	>=Delno	Delno
12	<=Delno je možno	>=Delno	Delno	>=Delno	Delno
13	<=Delno je možno	>=Delno	>=Delno	Delno	Delno
14	*	Delno	>=Delno	>=Delno	Delno
15	*	>=Delno	Delno	Delno	Delno
16	Je možno	Da	*	Da	Delno
17	<=Delno je možno	Da	<=Delno	Da	Delno
18	*	Da	Ne	Da	Delno
19	Ni možno	Da	Da	Ne	Delno
20	>=Delno je možno	Da	Da	Da	Da
21	Ni možno	Da	>=Delno	Da	Da
22	Ni možno	Da	Da	>=Delno	Da

	Operater	Administrator	**Možnost izklopa zgodovine dogodkov**
	75%	25%	
1	Je možno	*	Je možno
2	Ni možno	Je možno	Delno je možno
3	Ni možno	Ni možno	Ni možno

	Kreacija	Sprememba	Brisanje	**Dogodki v zapisu zgodovine**
	33%	33%	33%	
1	Ne	Ne	Ne	Ne
2	Da	Da	Da	Da

	Elektronski	Izpis	Prenašanje v elektronski obliki	**Prikaz zgodovine dogodkov**
	33%	33%	33%	
1	Ne	Ne	Ne	Ne
2	Da	Da	Da	Da

	Tip sistema	Namen spremembe	Industrijski parametri	**Parametri**
	14%	14%	72%	
1	*	*	Ne	Ne
2	*	*	Delno	Delno
3	laboratorijski	Ne	>=Delno	Delno
4	industrijski	*	Da	Da
5	*	Da	Da	Da

	Datum in čas	Tiskano ime posameznika	Staro in novo stanje	**Industrijski parametri**
	33%	33%	33%	
1	Ne	Ne	Ne	Ne
2	Da	Da	Da	Da

	Nadzor nad uporabo in vzdrževanjem - kontrola dostopa	Kontrola sprememb	**Sistemska dokumentacija**
	50%	50%	
1	Slaba	<=povprečno	slabo urejeno
2	<=Delna	slabo urejeno	slabo urejeno
3	>=Delna	dobro urejeno	dobro urejeno
4	Dobra	>=povprečno	dobro urejeno

	Kontrola verzij dokumentov	Pretečena dokumentacija - odstranitev, arhiviranje	Zgodovina dogodkov	**Kontrola sprememb**
	40%	15%	45%	
1	Ni	<=Delno	Slaba	slabo urejeno
2	Ni	<=Delno	>=Delna	povprečno
3	*	*	Delna	povprečno
4	*	Da	<=Delna	povprečno
5	Je	*	<=Delna	povprečno
6	*	Da	Dobra	dobro urejeno
7	Je	*	Dobra	dobro urejeno

	Možnost pregledovanja, inspekcije	Ohranitev povezave	Povezava zgodovine z dokumentacijo	Elementi zgodovine dogodkov	**Zgodovina dogodkov**
	19%	19%	19%	43%	
1	Ne	Ne	Ne	<=Delno	Slaba
2	*	*	*	Ne	Slaba
3	Da	*	Da	Da	Dobra
4	Da	Da	*	Da	Dobra

	Datum in čas	Tiskano ime posameznika	Staro in novo stanje	**Elementi zgodovine dogodkov**
	35%	33%	33%	
1	Ne	Ne	*	Ne
2	Ne	<=Delno	<=Delno	Ne
3	Ne	*	Ne	Ne
4	*	Ne	<=Delno	Ne
5	*	<=Delno	Ne	Ne
6	Ne	>=Delno	Da	Delno
7	Ne	Da	>=Delno	Delno
8	Da	Da	Da	Da

	Validacija elektronskega podpisa	Prikaz podpisa	Povezava podpis/zapis	Zahteve in nadzor podpisa	**Elektronski podpisi**
	23%	23%	22%	31%	
1	Slaba	slabo urejeno	slabo urejeno	*	neskladen
2	Slaba	slabo urejeno	<=povprečno	<=povprečno	neskladen
3	Slaba	slabo urejeno	*	slabo urejeno	neskladen
4	Slaba	<=povprečno	slabo urejeno	<=povprečno	neskladen
5	Slaba	<=povprečno	<=povprečno	slabo urejeno	neskladen
6	Slaba	*	slabo urejeno	slabo urejeno	neskladen
7	<=Delna	slabo urejeno	slabo urejeno	<=povprečno	neskladen
8	<=Delna	slabo urejeno	<=povprečno	slabo urejeno	neskladen
9	<=Delna	<=povprečno	slabo urejeno	slabo urejeno	neskladen
10	*	slabo urejeno	slabo urejeno	slabo urejeno	neskladen
11	Slaba	povprečno	dobro urejeno	<=povprečno	manj skladen
12	*	>=povprečno	dobro urejeno	slabo urejeno	manj skladen
13	Slaba	dobro urejeno	povprečno	<=povprečno	manj skladen
14	*	dobro urejeno	>=povprečno	slabo urejeno	manj skladen
15	Delna	slabo urejeno	dobro urejeno	<=povprečno	manj skladen
16	>=Delna	*	dobro urejeno	slabo urejeno	manj skladen
17	Delna	povprečno	povprečno	<=povprečno	manj skladen
18	>=Delna	>=povprečno	>=povprečno	slabo urejeno	manj skladen
19	Delna	dobro urejeno	slabo urejeno	<=povprečno	manj skladen
20	>=Delna	dobro urejeno	*	slabo urejeno	manj skladen
21	Dobra	slabo urejeno	povprečno	<=povprečno	manj skladen
22	Dobra	*	>=povprečno	slabo urejeno	manj skladen
23	Dobra	dobro urejeno	povprečno	dobro urejeno	precej skladen
24	Dobra	dobro urejeno	dobro urejeno	dobro urejeno	popolno skladen

	Validacija izvedbe in prikaza podpisa	Validacija povezave podpis/zapis	Validacija zahtev in nadzora podpisa	**Validacija elektronskega podpisa**
	33%	33%	33%	
1	Ne	Ne	<=Delno	Slaba
2	Ne	<=Delno	Ne	Slaba
3	<=Delno	Ne	Ne	Slaba
4	>=Delno	Da	Da	Dobra
5	Da	>=Delno	Da	Dobra
6	Da	Da	>=Delno	Dobra

	Vsebina prikaza	Zaščita prikaza	**Prikaz podpisa**
	50%	50%	
1	Ne	<=Delna	slabo urejeno
2	<=Delno	Slaba	slabo urejeno
3	>=Delno	Dobra	dobro urejeno
4	Da	>=Delna	dobro urejeno

	Datum in čas	Tiskano ime posameznika	Namen podpisa	**Vsebina prikaza**
	33%	33%	33%	
1	Ni	Ni	Ni	Ne
2	Je	Je	Je	Da

	Dostop do prikaza podpisa	Zgodovina dogodkov pri spremembah prikaza	Nadzor prikaza podpisa	**Zaščita prikaza**
	33%	33%	33%	
1	Ne	Ne	<=Delno	Slaba
2	Ne	<=Delno	Ne	Slaba
3	<=Delno	Ne	Ne	Slaba
4	>=Delno	Da	Da	Dobra
5	Da	>=Delno	Da	Dobra
6	Da	Da	>=Delno	Dobra

	Varnost povezave	Ukrepi za ohranitev povezave	**Povezava podpis/zapis**
	50%	50%	
1	Slaba	<=Delno	slabo urejeno
2	<=Delna	Ne	slabo urejeno
3	>=Delna	Da	dobro urejeno
4	Dobra	>=Delno	dobro urejeno

	Enkratnost elektronskega podpisa	Nadzor identifikacijskih kod in gesel	Nebiometrični podpis	**Zahteve in nadzor podpisa**
	20%	60%	20%	
1	slabo urejeno	<=povprečen	slabo urejeno	slabo urejeno
2	*	slab	*	slabo urejeno
3	slabo urejeno	>=povprečen	>=povprečno	povprečno
4	<=povprečno	povprečen	>=povprečno	povprečno
5	<=povprečno	>=povprečen	povprečno	povprečno
6	*	povprečen	povprečno	povprečno
7	slabo urejeno	dober	*	povprečno
8	<=povprečno	dober	<=povprečno	povprečno
9	*	dober	slabo urejeno	povprečno
10	povprečno	povprečen	*	povprečno
11	povprečno	>=povprečen	<=povprečno	povprečno
12	>=povprečno	povprečen	<=povprečno	povprečno
13	>=povprečno	>=povprečen	slabo urejeno	povprečno
14	>=povprečno	dober	dobro urejeno	dobro urejeno
15	dobro urejeno	>=povprečen	dobro urejeno	dobro urejeno
16	dobro urejeno	dober	>=povprečno	dobro urejeno

	Enak elektronski podpis	Kasnejša dodelitev enakega elektronskega podpisa	Ustrezen dokumentiran nadzor dodelitve EP	**Enkratnost elektronskega podpisa**
	56%	33%	11%	
1	Je možno	*	*	slabo urejeno
2	*	Je možno	Ni	slabo urejeno
3	Ni možno	Je možno	Je	povprečno
4	Ni možno	Ni možno	*	dobro urejeno

	Zaščita in integriteta	Kartice, žetoni, naprave	Nepooblaščen dostop	**Nadzor identifikacijskih kod in gesel**
	69%	19%	13%	
1	Ne	*	*	slab
2	<=Delno	Ne	Ne	slab
3	Delno	*	>=Delno	povprečen
4	>=Delno	<=Delno	>=Delno	povprečen
5	Delno	>=Delno	*	povprečen
6	>=Delno	Delno	*	povprečen
7	>=Delno	>=Delno	Ne	povprečen
8	Da	<=Delno	*	povprečen
9	Da	*	Ne	povprečen
10	Da	Da	>=Delno	dober

	Enkratnost ID kod	Periodično pregledovanje	Časovni potek gesel	**Zaščita in integriteta**
	71%	14%	14%	
1	Ne	*	*	Ne
2	Da	Ne	*	Delno
3	Da	*	Ne	Delno
4	Da	Da	Da	Da

	Postopki za izdajo	Začetno testiranje	Periodično testiranje	**Kartice, žetoni, naprave**
	33%	33%	33%	
1	Ne	Ne	Ne	Ne
2	Da	Da	Da	Da

	Odkrivanje	Poročanje in ukrepanje	Avtomatske blokade	**Nepooblaščen dostop**
	33%	33%	33%	
1	Ne	Ne	Ne	Ne
2	Da	Da	Da	Da

	Administracija in izvedba EP	Postopki in procedure	Neprekinjen dostop	**Nebiometrični podpis**
	33%	33%	33%	
1	slabo urejeno	Ne	<=povprečno	slabo urejeno
2	slabo urejeno	<=Delno	slabo urejeno	slabo urejeno
3	<=povprečno	Ne	slabo urejeno	slabo urejeno
4	>=povprečno	Da	dobro urejeno	dobro urejeno
5	dobro urejeno	>=Delno	dobro urejeno	dobro urejeno
6	dobro urejeno	Da	>=povprečno	dobro urejeno

	Zaščita datotek z vsebino podpisa	Zaščita gesla pred administratorjem	Minimalna dolžina gesla	**Administracija in izvedba elektronskega podpisa**
	33%	33%	33%	
1	Slaba	Ni	*	slabo urejeno
2	Slaba	*	Ni izvedeno	slabo urejeno
3	<=Delna	Ni	Ni izvedeno	slabo urejeno
4	Dobra	Je	Izvedeno	dobro urejeno

	So napisani	Izobraženost	Se izvajajo	**Postopki in procedure**
	33%	33%	33%	
1	Ne	Ne	Ne	Ne
2	Da	Da	Da	Da

	Je definiran	Uporabniki so izobraženi	Uporaba	**Neprekinjen dostop**
	33%	33%	33%	
1	Ne	Ne	<=delno ustrezno	slabo urejeno
2	Ne	*	neustrezno	slabo urejeno
3	*	Ne	neustrezno	slabo urejeno
4	Da	Da	ustrezno	dobro urejeno

	Dve komponenti podpisa za prvi podpis-prijavo	Samo geslo ob neprekinjenem dostopu	Tehnične kontrole	**Uporaba**
	33%	33%	33%	
1	Ne	Ne	<=Povprečne	neustrezno
2	Ne	*	Neustrezne	neustrezno
3	*	Ne	Neustrezne	neustrezno
4	Da	Da	Ustrezne	ustrezno

	Ohranjevalnik zaslona	Avtomatska odjava	Nivoja operacijskega sistema in aplikacije	**Tehnične kontrole**
	33%	33%	33%	
1	Ne	Ne	<=Delno	Neustrezne
2	Ne	*	Ne	Neustrezne
3	*	Ne	Ne	Neustrezne
4	Da	Da	Da	Ustrezne

C. Rezultati vrednotenja variant

Kriterij	NADZORNI SISTEM	TESTIRANJE TABLET	NADZOR KOMOR
Kritičnost računalniškega sistema ,	srednje kritičen	precej kritičen	zelo kritičen
├ GXP kritičnost sistema	visoka	visoka	visoka
│ ├ Vpliv na kvaliteto izdelka	neposredni	neposredni	neposredni
│ └ Odprtost sistema	nedostopen	delno dostopen	delno dostopen
└ Skladnost z regulativo	srednje skladen	manj skladen	neskladen
├ Klasifikacija sistema	samo zapisi	samo zapisi	samo zapisi
├ Elektronski zapisi	srednje skladen	manj skladen	neskladen
│ ├ Validacija elektronskih zapisov	Delno	Delno	Ne
│ │ ├ Validacija sistema glede na industrijske standarde	Delna	Delna	Slaba
│ │ │ ├ Specifikacije	Povprečne	Povprečne	Neustrezne
│ │ │ │ ├ Zahteve uporabnika	Neustrezne	Ustrezne	Neustrezne
│ │ │ │ ├ Ocena dobavitelja	Delna	Slaba	Slaba
│ │ │ │ └ Programska in strojna specifikacija	Dobra	Dobra	Delna
│ │ │ ├ Kvalifikacija	Dobra	Dobra	Slaba
│ │ │ │ ├ Kvalifikacija načrtovanja - DQ	Delna	Delna	Slaba
│ │ │ │ ├ Kvalifikacija montaže - IQ	Dobra	Dobra	Slaba
│ │ │ │ ├ Kvalifikacija obratovanja - OQ	Dobra	Dobra	Delna
│ │ │ │ └ Kvalifikacija delovanja - PQ	Dobra	Dobra	Slaba
│ │ │ ├ Postopki	Da	Da	Delno
│ │ │ │ ├ Validacijski protokol	Da	Da	Da
│ │ │ │ ├ Poročilo o validaciji	Da	Da	Delno
│ │ │ │ └ Sistemski splošni postopki	Delno	Delno	Delno
│ │ │ │ ├ Delovanje sistema	Da	Da	Da
│ │ │ │ └ Administracija sistema	Delno	Delno	Ne
│ │ │ │ ├ Periodični pregled sistema	Ne	Ne	Ne
│ │ │ │ ├ Arhiviranje, varnostno kopiranje, restavracija sistema in zapisov	Da	Da	Ne
│ │ │ │ └ Konfiguracija sistema in zaščit	Ne	Ne	Ne
│ │ │ └ Izobraževanje	Delno	Delno	Delno
│ │ │ ├ Uporabniki, sistemski administratorji	Izvedeno	Izvedeno	Izvedeno
│ │ │ ├ Razvijalci, interni presojevalci, zunanji	Ni izvedeno	Ni izvedeno	Ni izvedeno
│ │ │ └ Dokumentiranost	Je	Je	Je
│ │ └ Validacija glede na regulativo o elektronskih podpisih in zapisih	Delno	Delno	Ne
│ │ ├ Neveljavni, spremenjeni zapisi	Ne	Ne	Ne
│ │ │ ├ Neveljavni vnosi	Delno	Delno	Ne
│ │ │ ├ Sposobnost razlikovanja spremenjenih zapisov	Ne	Ne	Ne
│ │ │ └ Test razlikovanja spremenjenih zapisov	Ne	Ne	Ne

├ Generiranje kopij elektronskih zapisov	Da	Da	Da
│ ├ Prikaz v elektronski obliki	Je	Je	Je
│ ├ Prikaz v obliki izpisa	Je	Je	Je
│ └ Prenašanje v elektronski obliki	Je	Je	Je
└ Ostale zahteve za validacijo elektronskih zapisov	Delno	Delno	Ne
├ Zgodovina dogodkov	Ne	Ne	Ne
├ Zaporedje dogodkov	Delno	Delno	Ne
└ Zaščita zapisov in dostopa	delno izvedeno	izvedeno	ni izvedeno
├ Testiranje dostopa in avtorizacij	izvedeno	izvedeno	ni izvedeno
├ Testiranje arhiviranja in restavracije zapisov	ni izvedeno	delno izvedeno	ni izvedeno
└ Test naprav, ki so vir vhodnih podatkov	delno izvedeno	izvedeno	ni izvedeno
├ Zaščita	povprečno	slabo urejeno	slabo urejeno
├ Nadzor	povprečen	povprečen	povprečen
├ Pregledi zapisov	nikoli	nikoli	nikoli
├ Uporabnika	včasih	včasih	včasih
├ Administratorja	nikoli	nikoli	nikoli
└ Upravljanja kakovosti	nikoli	nikoli	nikoli
├ Zaporedje dogodkov	Ne	Delno	Da
├ Vsiljeno zaporedje dogodkov	Delno	Delno	Da
└ Avtomatski mehanizem sekvenc	Ne	Delno	Da
└ Preverjanje naprav	izvedeno	izvedeno	delno izvedeno
├ Preverjanje vira vhodnih podatkov	Da	Da	Da
└ Periodično testiranje naprav	izvedeno	izvedeno	ni izvedeno
├ Zaščita zapisov	povprečno	povprečno	slabo urejeno
├ Arhiviranje	povprečno	povprečno	slabo urejeno
├ Restavracija	povprečno	povprečno	slabo urejeno
├ Glede na čas	15 minut-1 dan	15 minut-1 dan	Več kot 1 dan
├ Glede na celovitost podatkov	ustrezno	ustrezno	neustrezno
└ Periodično testiranje restavracije	ni izvedeno	ni izvedeno	ni izvedeno
└ Zaščita zapisov glede na lokacijo	Delna	Delna	Slaba
├ Na sistemu	Delna	Delna	Slaba
├ Na arhivskem mediju	Dobra	Dobra	Slaba
└ Perioda arhiviranja	5 minut - 1 dan	več kot 1 dan	več kot 1 dan
└ Zaščita dostopa	povprečno	slabo urejeno	povprečno
├ Fizični dostop	omejen	omejen	omejen
├ Arhiv konfiguracije zaščit	Ni	Ni	Ni
└ Logični dostop	povprečno	slabo urejeno	povprečno
├ Avtorizacije	povprečno	povprečno	povprečno
├ Način avtorizacije dostopa	kontroliran	delno kontroliran	kontroliran
├ Preverjanje avtorizacije za izvedbo podpisa	Ne	Ne	Ne
└ Preverjanje avtorizacije pri uporabi sistema	Da	Da	Da

│ │ └ Dostop do sistema	delno omejen	neomejen	delno omejen
│ │ ├ Operacijski sistem	Ne	Da	Da
│ │ ├ Avtomatska odjava	Ni	Ni	Ni
│ │ └ Aplikacija	omejen	neomejen	delno omejen
│ │ ├ Večnivojski dostop	Izvedeno	Izvedeno	Izvedeno
│ │ ├ Prikritost gesel, minimalna dolžina gesel	Izvedeno	Ni izvedeno	Izvedeno
│ │ └ Uporabniški računi	povprečno	slabo urejeno	slabo urejeno
│ │ ├ Potek uporabniškega računa	Ne	Ne	Ne
│ │ ├ Periodično pregledovanje računov	Ne	Ne	Ne
│ │ └ Detekcija nepooblaščenih poizkusov dostopa	Da	Ne	Ne
│ ├ Zgodovina dogodkov	dobro urejeno	povprečno	slabo urejeno
│ ├ Ročna zgodovina dogodkov	Slaba	Slaba	Slaba
│ └ Računalniško generirana zgodovina dogodkov	Dobra	Delna	Slaba
│ ├ Ohranitev zgodovine dogodkov	Dobra	Delna	Slaba
│ │ ├ Varna povezava med zapisom in zgodovino dogodkov	Je	Je	Ni
│ │ ├ Zaščita pred spremembo, prenosom, brisanjem	Da	Delno	Ne
│ │ └ Arhiviranje, restavracija zgodovine dogodkov	Da	Ne	Ne
│ ├ Časovna značka	dobro urejeno	povprečno	slabo urejeno
│ │ ├ Možnost spremembe	Ni možno	Je možno	Je možno
│ │ └ Periodična verifikacija	Da	Da	Ne
│ └ Ustreznost zgodovine dogodkov	Da	Da	Ne
│ ├ Možnost izklopa zgodovine dogodkov	Ni možno	Ni možno	Je možno
│ │ ├ Operater	Ni možno	Ni možno	Je možno
│ │ └ Administrator	Ni možno	Ni možno	Je možno
│ ├ Dogodki v zapisu zgodovine	Da	Da	Ne
│ │ ├ Kreacija	Da	Da	Ne
│ │ ├ Sprememba	Da	Da	Ne
│ │ └ Brisanje	Da	Da	Ne
│ ├ Prikaz zgodovine dogodkov	Da	Da	Ne
│ │ ├ Elektronski	Da	Da	Ne
│ │ ├ Izpis	Da	Da	Ne
│ │ └ Prenašanje v elektronski obliki	Da	Da	Ne
│ └ Parametri	Delno	Delno	Ne
│ ├ Tip sistema	industrijski	laboratorijski	laboratorijski
│ ├ Namen spremembe	Ne	Da	Ne
│ └ Industrijski parametri	Delno	Delno	Ne
│ ├ Datum in čas	Da	Da	Ne
│ ├ Tiskano ime posameznika	Ne	Ne	Ne
│ └ Staro in novo stanje	Da	Da	Ne

└ Sistemska dokumentacija	povprečno	povprečno	povprečno
├ Nadzor nad uporabo in vzdrževanjem - kontrola dostopa	Dobra	Dobra	Dobra
└ Kontrola sprememb	slabo urejeno	slabo urejeno	slabo urejeno
├ Kontrola verzij dokumentov	Ni	Ni	Ni
├ Pretečena dokumentacija - odstranitev, arhiviranje	Delno	Delno	Delno
└ Zgodovina dogodkov	Slaba	Slaba	Slaba
├ Možnost pregledovanja, inšpekcije	Ne	Ne	Ne
├ Ohranitev povezave	Ne	Ne	Ne
├ Povezava zgodovine z dokumentacijo	Ne	Ne	Ne
└ Elementi zgodovine dogodkov	Ne	Ne	Ne
├ Datum in čas	Ne	Ne	Ne
├ Tiskano ime posameznika	Ne	Ne	Ne
└ Staro in novo stanje	Ne	Ne	Ne
└ Elektronski podpisi	neskladen	neskladen	neskladen
├ Validacija elektronskega podpisa	Slaba	Slaba	Slaba
├ Validacija izvedbe in prikaza podpisa	Ne	Ne	Ne
├ Validacija povezave podpis/zapis	Ne	Ne	Ne
└ Validacija zahtev in nadzora podpisa	Ne	Ne	Ne
├ Prikaz podpisa	slabo urejeno	slabo urejeno	slabo urejeno
├ Vsebina prikaza	Ne	Ne	Ne
├ Datum in čas	Ni	Ni	Ni
├ Tiskano ime posameznika	Ni	Ni	Ni
└ Namen podpisa	Ni	Ni	Ni
└ Zaščita prikaza	Slaba	Slaba	Slaba
├ Dostop do prikaza podpisa	Ne	Ne	Ne
├ Zgodovina dogodkov pri spremembah prikaza	Ne	Ne	Ne
└ Nadzor prikaza podpisa	Ne	Ne	Ne
├ Povezava podpis/zapis	slabo urejeno	slabo urejeno	slabo urejeno
├ Varnost povezave	Slaba	Slaba	Slaba
└ Ukrepi za ohranitev povezave	Ne	Ne	Ne
└ Zahteve in nadzor podpisa	slabo urejeno	slabo urejeno	slabo urejeno
├ Enkratnost elektronskega podpisa	slabo urejeno	slabo urejeno	slabo urejeno
├ Enak elektronski podpis	Je možno	Je možno	Je možno
├ Kasnejša dodelitev enakega elektronskega podpisa	Je možno	Je možno	Je možno
└ Ustrezen dokumentiran nadzor dodelitve elektronskega podpisa	Ni	Ni	Ni
├ Nadzor identifikacijskih kod in gesel	slab	slab	slab
├ Zaščita in integriteta	Ne	Ne	Ne
├ Enkratnost identifikacijskih kod	Ne	Ne	Ne
├ Periodično pregledovanje	Ne	Ne	Ne
└ Časovni potek gesel	Ne	Ne	Ne

├ Kartice, žetoni, naprave	Ne	Ne	Ne
│ ├ Postopki za izdajo	Ne	Ne	Ne
│ ├ Začetno testiranje	Ne	Ne	Ne
│ └ Periodično testiranje	Ne	Ne	Ne
└ Nepooblaščen dostop	Ne	Ne	Ne
├ Odkrivanje	Ne	Ne	Ne
├ Poročanje in ukrepanje	Ne	Ne	Ne
└ Avtomatske blokade	Ne	Ne	Ne
└ Nebiometrični podpis	slabo urejeno	slabo urejeno	slabo urejeno
├ Administracija in izvedba elektronskega podpisa	slabo urejeno	slabo urejeno	slabo urejeno
├ Zaščita datotek z vsebino podpisa	Slaba	Slaba	Slaba
├ Zaščita gesla pred administratorjem	Ni	Ni	Ni
└ Minimalna dolžina gesla	Ni izvedeno	Ni izvedeno	Ni izvedeno
├ Postopki in procedure	Ne	Ne	Ne
├ So napisani	Ne	Ne	Ne
├ Izobraženost	Ne	Ne	Ne
└ Se izvajajo	Ne	Ne	Ne
└ Neprekinjen dostop	slabo urejeno	slabo urejeno	slabo urejeno
├ Je definiran	Ne	Ne	Ne
├ Uporabniki so izobraženi	Ne	Ne	Ne
└ Uporaba	neustrezno	neustrezno	neustrezno
├ Dve komponenti podpisa za prvi podpis-prijavo	Ne	Ne	Ne
├ Samo geslo ob neprekinjenem dostopu	Ne	Ne	Ne
└ Tehnične kontrole	Neustrezne	Neustrezne	Neustrezne
├ Ohranjevalnik zaslona	Ne	Ne	Ne
├ Avtomatska odjava	Ne	Ne	Ne
└ Nivoja operacijskega sistema in aplikacije	Ne	Ne	Ne

D. Rezultati vrednotenja izboljšanih variant

Kriterij	NADZORNI SISTEM	TESTIRANJE TABLET	NADZOR KOMOR
Kritičnost računalniškega sistema	nekritičen	nekritičen	nekritičen
├ GXP kritičnost sistema	visoka	visoka	visoka
│ ├ Vpliv na kvaliteto izdelka	neposredni	neposredni	neposredni
│ └ Odprtost sistema	nedostopen	delno dostopen	delno dostopen
└ Skladnost z regulativo	popolno skladen	popolno skladen	popolno skladen
├ Klasifikacija sistema	samo zapisi	zapisi in podpisi	samo zapisi
├ Elektronski zapisi	popolno skladen	popolno skladen	popolno skladen
│ ├ Validacija elektronskih zapisov	Delno	Delno	Delno
│ │ ├ Validacija sistema glede na industrijske standarde	Delna	Delna	Delna
│ │ │ ├ Specifikacije	Povprečne	Povprečne	Povprečne
│ │ │ │ ├ Zahteve uporabnika	Neustrezne	Ustrezne	Neustrezne
│ │ │ │ ├ Ocena dobavitelja	Delna	Slaba	Slaba
│ │ │ │ └ Programska in strojna specifikacija	Dobra	Dobra	Dobra
│ │ │ ├ Kvalifikacija	Dobra	Dobra	Dobra
│ │ │ │ ├ Kvalifikacija načrtovanja - DQ	Delna	Delna	Delna
│ │ │ │ ├ Kvalifikacija montaže - IQ	Dobra	Dobra	Dobra
│ │ │ │ ├ Kvalifikacija obratovanja - OQ	Dobra	Dobra	Dobra
│ │ │ │ └ Kvalifikacija delovanja - PQ	Dobra	Dobra	Dobra
│ │ │ ├ Postopki	Da	Da	Da
│ │ │ │ ├ Validacijski protokol	Da	Da	Da
│ │ │ │ ├ Poročilo o validaciji	Da	Da	Da
│ │ │ │ └ Sistemski splošni postopki	Da	Da	Da
│ │ │ │ ├ Delovanje sistema	Da	Da	Da
│ │ │ │ └ Administracija sistema	Da	Da	Da
│ │ │ │ ├ Periodični pregled sistema	Da	Da	Da
│ │ │ │ ├ Arhiviranje, varnostno kopiranje, restavracija sistema in zapisov	Da	Da	Da
│ │ │ │ └ Konfiguracija sistema in zaščit	Da	Da	Da
│ │ │ └ Izobraževanje	Delno	Delno	Delno
│ │ │ ├ Uporabniki, sistemski administratorji	Izvedeno	Izvedeno	Izvedeno
│ │ │ ├ Razvijalci, interni presojevalci, zunanji	Ni izvedeno	Ni izvedeno	Ni izvedeno
│ │ │ └ Dokumentiranost	Je	Je	Je
│ │ └ Validacija glede na regulativo o elektronskih podpisih in zapisih	Delno	Delno	Delno
│ │ ├ Neveljavni, spremenjeni zapisi	Delno	Delno	Delno
│ │ │ ├ Neveljavni vnosi	Da	Da	Ne
│ │ │ ├ Sposobnost razlikovanja spremenjenih zapisov	Ne	Ne	Da
│ │ │ └ Test razlikovanja spremenjenih zapisov	Da	Da	Da

├ Generiranje kopij elektronskih zapisov	Da	Da	Da
│ ├ Prikaz v elektronski obliki	Je	Je	Je
│ ├ Prikaz v obliki izpisa	Je	Je	Je
│ └ Prenašanje v elektronski obliki	Je	Je	Je
└ Ostale zahteve za validacijo elektronskih zapisov	Da	Da	Delno
├ Zgodovina dogodkov	Da	Da	Delno
├ Zaporedje dogodkov	Delno	Delno	Ne
└ Zaščita zapisov in dostopa	izvedeno	izvedeno	izvedeno
├ Testiranje dostopa in avtorizacij	izvedeno	izvedeno	izvedeno
├ Testiranje arhiviranja in restavracije zapisov	izvedeno	izvedeno	izvedeno
└ Test naprav, ki so vir vhodnih podatkov	izvedeno	izvedeno	izvedeno
├ Zaščita	dobro urejeno	dobro urejeno	dobro urejeno
├ Nadzor	povprečen	dober	dober
├ Pregledi zapisov	redno	redno	redno
├ Uporabnika	redno	redno	redno
├ Administratorja	redno	redno	redno
└ Upravljanja kakovosti	redno	redno	redno
├ Zaporedje dogodkov	Ne	Delno	Da
├ Vsiljeno zaporedje dogodkov	Delno	Delno	Da
└ Avtomatski mehanizem sekvenc	Ne	Delno	Da
└ Preverjanje naprav	izvedeno	izvedeno	izvedeno
├ Preverjanje vira vhodnih podatkov	Da	Da	Da
└ Periodično testiranje naprav	izvedeno	izvedeno	izvedeno
├ Zaščita zapisov	dobro urejeno	dobro urejeno	dobro urejeno
├ Arhiviranje	dobro urejeno	dobro urejeno	dobro urejeno
├ Restavracija	dobro urejeno	dobro urejeno	dobro urejeno
├ Glede na čas	15 minut-1 dan	15 minut-1 dan	15 minut-1 dan
├ Glede na celovitost podatkov	ustrezno	ustrezno	ustrezno
└ Periodično testiranje restavracije	izvedeno	izvedeno	izvedeno
└ Zaščita zapisov glede na lokacijo	Dobra	Dobra	Dobra
├ Na sistemu	Dobra	Dobra	Dobra
├ Na arhivskem mediju	Dobra	Dobra	Dobra
└ Perioda arhiviranja	5 minut - 1 dan	5 minut - 1 dan	5 minut - 1 dan
└ Zaščita dostopa	dobro urejeno	dobro urejeno	dobro urejeno
├ Fizični dostop	omejen	omejen	omejen
├ Arhiv konfiguracije zaščit	Je	Je	Je
└ Logični dostop	povprečno	povprečno	povprečno
├ Avtorizacije	povprečno	povprečno	povprečno
├ Način avtorizacije dostopa	kontroliran	kontroliran	kontroliran
├ Preverjanje avtorizacije za izvedbo podpisa	Ne	Ne	Ne
└ Preverjanje avtorizacije pri uporabi sistema	Da	Da	Da

└ Dostop do sistema	delno omejen	delno omejen	delno omejen
├ Operacijski sistem	Da	Da	Da
├ Avtomatska odjava	Ni	Ni	Ni
└ Aplikacija	omejen	omejen	omejen
├ Večnivojski dostop	Izvedeno	Izvedeno	Izvedeno
├ Prikritost gesel, minimalna dolžina gesel	Izvedeno	Izvedeno	Izvedeno
└ Uporabniški računi	dobro urejeno	dobro urejeno	dobro urejeno
├ Potek uporabniskega računa	Da	Da	Da
├ Periodično pregledovanje računov	Da	Da	Da
└ Detekcija nepooblaščenih poizkusov dostopa	Da	Da	Da
├ Zgodovina dogodkov	dobro urejeno	dobro urejeno	dobro urejeno
├ Ročna zgodovina dogodkov	Slaba	Slaba	Slaba
└ Računalniško generirana zgodovina dogodkov	Dobra	Dobra	Dobra
├ Ohranitev zgodovine dogodkov	Dobra	Dobra	Dobra
├ Varna povezava med zapisom in zgodovino dogodkov	Je	Je	Je
├ Zaščita pred spremembo, prenosom, brisanjem	Da	Da	Da
└ Arhiviranje, restavracija zgodovine dogodkov	Da	Da	Da
├ Časovna značka	dobro urejeno	dobro urejeno	povprečno
├ Možnost spremembe	Ni možno	Ni možno	Je možno
└ Periodična verifikacija	Da	Da	Da
└ Ustreznost zgodovine dogodkov	Da	Da	Da
├ Možnost izklopa zgodovine dogodkov	Ni možno	Ni možno	Ni možno
├ Operater	Ni možno	Ni možno	Ni možno
└ Administrator	Ni možno	Ni možno	Ni možno
├ Dogodki v zapisu zgodovine	Da	Da	Da
├ Kreacija	Da	Da	Da
├ Sprememba	Da	Da	Da
└ Brisanje	Da	Da	Da
├ Prikaz zgodovine dogodkov	Da	Da	Da
├ Elektronski	Da	Da	Da
├ Izpis	Da	Da	Da
└ Prenasanje v elektronski obliki	Da	Da	Da
└ Parametri	Da	Da	Da
├ Tip sistema	industrijski	laboratorijski	laboratorijski
├ Namen spremembe	Ne	Da	Da
└ Industrijski parametri	Da	Da	Da
├ Datum in čas	Da	Da	Da
├ Tiskano ime posameznika	Da	Da	Da
└ Staro in novo stanje	Da	Da	Da

│ └ Sistemska dokumentacija	dobro urejeno	dobro urejeno	dobro urejeno
│ ├ Nadzor nad uporabo in vzdrževanjem - kontrola dostopa	Dobra	Dobra	Dobra
│ └ Kontrola sprememb	povprečno	povprečno	povprečno
│ ├ Kontrola verzij dokumentov	Je	Je	Je
│ ├ Pretečena dokumentacija - odstranitev, arhiviranje	Delno	Delno	Delno
│ └ Zgodovina dogodkov	Slaba	Slaba	Slaba
│ ├ Možnost pregledovanja, inšpekcije	Ne	Ne	Ne
│ ├ Ohranitev povezave	Ne	Ne	Ne
│ ├ Povezava zgodovine z dokumentacijo	Ne	Ne	Ne
│ └ Elementi zgodovine dogodkov	Ne	Ne	Ne
│ ├ Datum in čas	Ne	Ne	Ne
│ ├ Tiskano ime posameznika	Ne	Ne	Ne
│ └ Staro in novo stanje	Ne	Ne	Ne
└ Elektronski podpisi	neskladen	popolno skladen	neskladen
├ Validacija elektronskega podpisa	Slaba	dobra	Slaba
│ ├ Validacija izvedbe in prikaza podpisa	Ne	Da	Ne
│ ├ Validacija povezave podpis/zapis	Ne	Da	Ne
│ └ Validacija zahtev in nadzora podpisa	Ne	Da	Ne
├ Prikaz podpisa	slabo urejeno	dobro urejeno	slabo urejeno
│ ├ Vsebina prikaza	Ne	Da	Ne
│ │ ├ Datum in čas	Ni	Je	Ni
│ │ ├ Tiskano ime posameznika	Ni	Je	Ni
│ │ └ Namen podpisa	Ni	Je	Ni
│ └ Zaščita prikaza	Slaba	Dobra	Slaba
│ ├ Dostop do prikaza podpisa	Ne	Da	Ne
│ ├ Zgodovina dogodkov pri spremembah prikaza	Ne	Da	Ne
│ └ Nadzor prikaza podpisa	Ne	Da	Ne
├ Povezava podpis/zapis	slabo urejeno	dobro urejeno	slabo urejeno
│ ├ Varnost povezave	Slaba	Dobra	Slaba
│ └ Ukrepi za ohranitev povezave	Ne	Da	Ne
└ Zahteve in nadzor podpisa	slabo urejeno	dobro urejeno	slabo urejeno
├ Enkratnost elektronskega podpisa	slabo urejeno	dobro urejeno	slabo urejeno
│ ├ Enak elektronski podpis	Je možno	Ni možno	Je možno
│ ├ Kasnejša dodelitev enakega elektronskega podpisa	Je možno	Ni možno	Je možno
│ └ Ustrezen dokumentiran nadzor dodelitve EP	Ni	Je	Ni
├ Nadzor identifikacijskih kod in gesel	slab	dober	slab
│ ├ Zaščita in integriteta	Ne	Da	Ne
│ │ ├ Enkratnost identifikacijskih kod	Ne	Da	Ne
│ │ ├ Periodično pregledovanje	Ne	Da	Ne
│ │ └ Časovni potek gesel	Ne	Da	Ne

├ Kartice, žetoni, naprave	Ne	Da	Ne
│ ├ Postopki za izdajo	Ne	Da	Ne
│ ├ Začetno testiranje	Ne	Da	Ne
│ └ Periodično testiranje	Ne	Da	Ne
└ Nepooblaščen dostop	Ne	Da	Ne
├ Odkrivanje	Ne	Da	Ne
├ Poročanje in ukrepanje	Ne	Da	Ne
└ Avtomatske blokade	Ne	Da	Ne
└ Nebiometrični podpis	slabo urejeno	dobro urejeno	slabo urejeno
├ Administracija in izvedba EP	slabo urejeno	dobro urejeno	slabo urejeno
├ Zaščita datotek z vsebino podpisa	Slaba	Dobra	Slaba
├ Zaščita gesla pred administratorjem	Ni	Je	Ni
└ Minimalna dolžina gesla	Ni izvedeno	Izvedeno	Ni izvedeno
├ Postopki in procedure	Ne	Da	Ne
├ So napisani	Ne	Da	Ne
├ Izobraženost	Ne	Da	Ne
└ Se izvajajo	Ne	Da	Ne
└ Neprekinjen dostop	slabo urejeno	povprečno	slabo urejeno
├ Je definiran	Ne	Da	Ne
├ Uporabniki so izobraženi	Ne	Da	Ne
└ Uporaba	neustrezno	delno ustrezno	neustrezno
├ Dve komponenti podpisa za prvi podpis-prijavo	Ne	Da	Ne
├ Samo geslo ob neprekinjenem dostopu	Ne	Ne	Ne
└ Tehnične kontrole	Neustrezne	povprečne	Neustrezne
├ Ohranjevalnik zaslona	Ne	Ne	Ne
├ Avtomatska odjava	Ne	Da	Ne
└ Nivoja operacijskega sistema in aplikacije	Ne	Delno	Ne

E. Povprečne uteži kriterijev

Kriterij	Lokalne	Globalne	Lok.norm.	Glob.norm.
Kritičnost računalniškega sistema				
├ GXP kritičnost sistema	47,7	47,7	35,4	35,4
│ ├ Vpliv na kvaliteto izdelka	75,0	35,8	75,0	26,5
│ └ Odprtost sistema	25,0	11,9	25,0	8,8
└ Skladnost z regulativo	52,3	52,3	64,6	64,6
├ Klasifikacija sistema	62,7	32,8	50,2	32,4
├ Elektronski zapisi	28,0	14,6	37,4	24,1
│ ├ Validacija elektronskih zapisov	24,3	3,6	24,3	5,9
│ │ ├ Validacija sistema glede na industrijske standarde	50,0	1,8	50,0	2,9
│ │ │ ├ Specifikacije	36,5	0,7	36,5	1,1
│ │ │ │ ├ Zahteve uporabnika	23,8	0,2	23,8	0,3
│ │ │ │ ├ Ocena dobavitelja	14,3	0,1	14,3	0,2
│ │ │ │ └ Programska in strojna specifikacija	61,9	0,4	61,9	0,7
│ │ │ ├ Kvalifikacija	38,5	0,7	38,5	1,1
│ │ │ │ ├ Kvalifikacija načrtovanja - DQ	25,0	0,2	25,0	0,3
│ │ │ │ ├ Kvalifikacija montaže - IQ	25,0	0,2	25,0	0,3
│ │ │ │ ├ Kvalifikacija obratovanja - OQ	25,0	0,2	25,0	0,3
│ │ │ │ └ Kvalifikacija delovanja - PQ	25,0	0,2	25,0	0,3
│ │ │ ├ Postopki	17,3	0,3	17,3	0,5
│ │ │ │ ├ Validacijski protokol	33,3	0,1	33,3	0,2
│ │ │ │ ├ Poročilo o validaciji	33,3	0,1	33,3	0,2
│ │ │ │ └ Sistemski splošni postopki	33,3	0,1	33,3	0,2
│ │ │ │ ├ Delovanje sistema	50,0	0,1	50,0	0,1
│ │ │ │ └ Administracija sistema	50,0	0,1	50,0	0,1
│ │ │ │ ├ Periodični pregled sistema	26,7	0,0	26,7	0,0
│ │ │ │ ├ Arhiviranje, varnostno kopiranje, restavracija sistema in zapisov	33,3	0,0	33,3	0,0
│ │ │ │ └ Konfiguracija sistema in zaščit	40,0	0,0	40,0	0,0
│ │ │ └ Izobraževanje	7,7	0,1	7,7	0,2
│ │ │ ├ Uporabniki, sistemski administratorji	33,3	0,0	33,3	0,1
│ │ │ ├ Razvijalci, interni presojevalci, zunanji	33,3	0,0	33,3	0,1
│ │ │ └ Dokumentiranost	33,3	0,0	33,3	0,1
│ │ └ Validacija glede na regulativo o elektronskih podpisih in zapisih	50,0	1,8	50,0	2,9
│ │ ├ Neveljavni, spremenjeni zapisi	52,9	0,9	52,9	1,6
│ │ │ ├ Neveljavni vnosi	33,3	0,3	42,9	0,7
│ │ │ ├ Sposobnost razlikovanja spremenjenih zapisov	33,3	0,3	28,6	0,4
│ │ │ └ Test razlikovanja spremenjenih zapisov	33,3	0,3	28,6	0,4

├ Generiranje kopij elektronskih zapisov	23,5	0,4	23,5	0,7
├ Prikaz v elektronski obliki	33,3	0,1	33,3	0,2
├ Prikaz v obliki izpisa	33,3	0,1	33,3	0,2
└ Prenašanje v elektronski obliki	33,3	0,1	33,3	0,2
└ Ostale zahteve za validacijo elektronskih zapisov	23,5	0,4	23,5	0,7
├ Zgodovina dogodkov	38,5	0,2	38,5	0,3
├ Zaporedje dogodkov	15,4	0,1	15,4	0,1
└ Zaščita zapisov in dostopa	46,2	0,2	46,2	0,3
├ Testiranje dostopa in avtorizacij	60,0	0,1	60,0	0,2
├ Testiranje arhiviranja in restavracije zapisov	35,0	0,1	35,0	0,1
└ Test naprav, ki so vir vhodnih podatkov	5,0	0,0	5,0	0,0
├ Zaščita	29,6	4,3	29,6	7,1
├ Nadzor	25,0	1,1	25,0	1,8
├ Pregledi zapisov	33,3	0,4	33,3	0,6
├ Uporabnika	33,3	0,1	33,3	0,2
├ Administratorja	33,3	0,1	33,3	0,2
└ Upravljanja kakovosti	33,3	0,1	33,3	0,2
├ Zaporedje dogodkov	33,3	0,4	33,3	0,6
├ Vsiljeno zaporedje dogodkov	50,0	0,2	50,0	0,3
└ Avtomatski mehanizem sekvenc	50,0	0,2	50,0	0,3
└ Preverjanje naprav	33,3	0,4	33,3	0,6
├ Preverjanje vira vhodnih podatkov	50,0	0,2	50,0	0,3
└ Periodično testiranje naprav	50,0	0,2	50,0	0,3
├ Zaščita zapisov	37,5	1,6	37,5	2,7
├ Arhiviranje	33,3	0,5	33,3	0,9
├ Restavracija	33,3	0,5	33,3	0,9
├ Glede na čas	10,0	0,1	13,6	0,1
├ Glede na celovitost podatkov	80,0	0,4	72,7	0,6
└ Periodično testiranje restavracije	10,0	0,1	13,6	0,1
└ Zaščita zapisov glede na lokacijo	33,3	0,5	33,3	0,9
├ Na sistemu	33,3	0,2	33,3	0,3
├ Na arhivskem mediju	52,4	0,3	52,4	0,5
└ Perioda arhiviranja	14,3	0,1	14,3	0,1
└ Zaščita dostopa	37,5	1,6	37,5	2,7
├ Fizični dostop	12,5	0,2	13,6	0,4
├ Arhiv konfiguracije zaščit	25,0	0,4	18,2	0,5
└ Logični dostop	62,5	1,0	68,2	1,8
├ Avtorizacije	50,0	0,5	50,0	0,9
├ Način avtorizacije dostopa	34,1	0,2	40,2	0,4
├ Preverjanje avtorizacije za izvedbo podpisa	45,5	0,2	35,7	0,3
└ Preverjanje avtorizacije pri uporabi sistema	20,5	0,1	24,1	0,2

│ │ └ Dostop do sistema	50,0	0,5	50,0	0,9
│ │ ├ Operacijski sistem	33,3	0,2	28,6	0,3
│ │ ├ Avtomatska odjava	33,3	0,2	28,6	0,3
│ │ └ Aplikacija	33,3	0,2	42,9	0,4
│ │ ├ Večnivojski dostop	40,8	0,1	37,4	0,1
│ │ ├ Prikritost gesel, minimalna dolžina gesel	40,8	0,1	37,4	0,1
│ │ └ Uporabniški računi	18,4	0,0	25,2	0,1
│ │ ├ Potek uporabniškega računa	53,8	0,0	43,7	0,0
│ │ ├ Periodično pregledovanje računov	23,1	0,0	28,1	0,0
│ │ └ Detekcija nepooblaščenih poizkusov dostopa	23,1	0,0	28,1	0,0
│ ├ Zgodovina dogodkov	25,2	3,7	25,2	6,1
│ │ ├ Ročna zgodovina dogodkov	50,0	1,8	50,0	3,0
│ │ └ Računalniško generirana zgodovina dogodkov	50,0	1,8	50,0	3,0
│ │ ├ Ohranitev zgodovine dogodkov	34,8	0,6	34,8	1,1
│ │ │ ├ Varna povezava med zapisom in zgodovino dogodkov	30,8	0,2	22,9	0,2
│ │ │ ├ Zaščita pred spremembo, prenosom, brisanjem	34,6	0,2	38,6	0,4
│ │ │ └ Arhiviranje, restavracija zgodovine dogodkov	34,6	0,2	38,6	0,4
│ │ ├ Časovna značka	13,0	0,2	13,0	0,4
│ │ │ ├ Možnost spremembe	50,0	0,1	50,0	0,2
│ │ │ └ Periodična verifikacija	50,0	0,1	50,0	0,2
│ │ └ Ustreznost zgodovine dogodkov	52,2	1,0	52,2	1,6
│ │ ├ Možnost izklopa zgodovine dogodkov	10,2	0,1	10,2	0,2
│ │ │ ├ Operater	75,0	0,1	75,0	0,1
│ │ │ └ Administrator	25,0	0,0	25,0	0,0
│ │ ├ Dogodki v zapisu zgodovine	25,4	0,2	25,4	0,4
│ │ │ ├ Kreacija	33,3	0,1	33,3	0,1
│ │ │ ├ Sprememba	33,3	0,1	33,3	0,1
│ │ │ └ Brisanje	33,3	0,1	33,3	0,1
│ │ ├ Prikaz zgodovine dogodkov	28,8	0,3	28,8	0,5
│ │ │ ├ Elektronski	33,3	0,1	33,3	0,2
│ │ │ ├ Izpis	33,3	0,1	33,3	0,2
│ │ │ └ Prenašanje v elektronski obliki	33,3	0,1	33,3	0,2
│ │ └ Parametri	35,6	0,3	35,6	0,6
│ │ ├ Tip sistema	13,8	0,0	10,1	0,1
│ │ ├ Namen spremembe	13,8	0,0	10,1	0,1
│ │ └ Industrijski parametri	72,4	0,2	79,7	0,5
│ │ ├ Datum in čas	33,3	0,1	33,3	0,2
│ │ ├ Tiskano ime posameznika	33,3	0,1	33,3	0,2
│ │ └ Staro in novo stanje	33,3	0,1	33,3	0,2

└ Sistemska dokumentacija	20,9	3,1	20,9	5,0
├ Nadzor nad uporabo in vzdrževanjem - kontrola dostopa	50,0	1,5	50,0	2,5
└ Kontrola sprememb	50,0	1,5	50,0	2,5
├ Kontrola verzij dokumentov	40,0	0,6	30,8	0,8
├ Pretečena dokumentacija - odstranitev, arhiviranje	15,0	0,2	17,3	0,4
└ Zgodovina dogodkov	45,0	0,7	51,9	1,3
├ Moznost pregledovanja, inšpekcije	19,0	0,1	15,7	0,2
├ Ohranitev povezave	19,0	0,1	15,7	0,2
├ Povezava zgodovine z dokumentacijo	19,0	0,1	15,7	0,2
└ Elementi zgodovine dogodkov	42,9	0,3	52,9	0,7
├ Datum in čas	34,8	0,1	26,2	0,2
├ Tiskano ime posameznika	32,6	0,1	36,9	0,3
└ Staro in novo stanje	32,6	0,1	36,9	0,3
└ Elektronski podpisi	9,3	4,9	12,5	8,0
├ Validacija elektronskega podpisa	23,4	1,1	23,4	1,9
├ Validacija izvedbe in prikaza podpisa	33,3	0,4	33,3	0,6
├ Validacija povezave podpis/zapis	33,3	0,4	33,3	0,6
└ Validacija zahtev in nadzora podpisa	33,3	0,4	33,3	0,6
├ Prikaz podpisa	23,4	1,1	23,4	1,9
├ Vsebina prikaza	50,0	0,6	50,0	0,9
├ Datum in čas	33,3	0,2	33,3	0,3
├ Tiskano ime posameznika	33,3	0,2	33,3	0,3
└ Namen podpisa	33,3	0,2	33,3	0,3
└ Zaščita prikaza	50,0	0,6	50,0	0,9
├ Dostop do prikaza podpisa	33,3	0,2	33,3	0,3
├ Zgodovina dogodkov pri spremembah prikaza	33,3	0,2	33,3	0,3
└ Nadzor prikaza podpisa	33,3	0,2	33,3	0,3
├ Povezava podpis/zapis	22,3	1,1	22,3	1,8
├ Varnost povezave	50,0	0,5	50,0	0,9
└ Ukrepi za ohranitev povezave	50,0	0,5	50,0	0,9
└ Zahteve in nadzor podpisa	30,9	1,5	30,9	2,5
├ Enkratnost elektronskega podpisa	20,0	0,3	20,0	0,5
├ Enak elektronski podpis	55,6	0,2	55,6	0,3
├ Kasnejša dodelitev enakega elektronskega podpisa	33,3	0,1	33,3	0,2
└ Ustrezen dokumentiran nadzor dodelitve EP	11,1	0,0	11,1	0,1
├ Nadzor identifikacijskih kod in gesel	60,0	0,9	60,0	1,5
├ Zaščita in integriteta	68,7	0,6	68,8	1,0
├ Enkratnost identifikacijskih kod	71,4	0,4	71,4	0,7
├ Periodično pregledovanje	14,3	0,1	14,3	0,1
└ Časovni potek gesel	14,3	0,1	14,3	0,1

├ Kartice, žetoni, naprave	18,8	0,2	18,8	0,3
│ ├ Postopki za izdajo	33,3	0,1	33,3	0,1
│ ├ Začetno testiranje	33,3	0,1	33,3	0,1
│ └ Periodično testiranje	33,3	0,1	33,3	0,1
└ Nepooblaščen dostop	12,5	0,1	12,5	0,2
├ Odkrivanje	33,3	0,0	33,3	0,1
├ Poročanje in ukrepanje	33,3	0,0	33,3	0,1
└ Avtomatske blokade	33,3	0,0	33,3	0,1
└ Nebiometrični podpis	20,0	0,3	20,0	0,5
├ Administracija in izvedba EP	33,3	0,1	33,3	0,2
│ ├ Zaščita datotek z vsebino podpisa	33,3	0,0	42,9	0,1
│ ├ Zaščita gesla pred administratorjem	33,3	0,0	28,6	0,0
│ └ Minimalna dolžina gesla	33,3	0,0	28,6	0,0
├ Postopki in procedure	33,3	0,1	33,3	0,2
│ ├ So napisani	33,3	0,0	33,3	0,1
│ ├ Izobraženost	33,3	0,0	33,3	0,1
│ └ Se izvajajo	33,3	0,0	33,3	0,1
└ Neprekinjen dostop	33,3	0,1	33,3	0,2
├ Je definiran	33,3	0,0	28,6	0,0
├ Uporabniki so izobraženi	33,3	0,0	28,6	0,0
└ Uporaba	33,3	0,0	42,9	0,1
├ Dve komponenti podpisa za prvi podpis – prijavo	33,3	0,0	28,6	0,0
├ Samo geslo ob neprekinjenem dostopu	33,3	0,0	28,6	0,0
└ Tehnične kontrole	33,3	0,0	42,9	0,0
├ Ohranjevalnik zaslona	33,3	0,0	28,6	0,0
├ Avtomatska odjava	33,3	0,0	28,6	0,0
└ Nivoja operacijskega sistema in aplikacije	33,3	0,0	42,9	0,0

F. Vprašalnik za oceno kriterijev – primeri vprašanj

D Electronski zapisi; nadzor za zaprte in odprte sisteme:			
Oznaka	**Vprašanje**	**Odgovor**	**Razlaga/komentar**
D.1	Ali je sistem validiran (referiraj se glede na odgovore v sekciji B tega vprašalnika)?		
D.2	Ali so validacijske aktivnosti primerno obravnavale Part11 zahteve (ustreznost testiranja zgodovine dogodkov, elektronskih podpisov)?		
D.3	Ali validacijska dokumentacija dokazuje, da sistem ustrezno reagira na napačne vnose (ali so bili kritični vnosi podatkov sistema testirani glede na neveljavne vnose ali vnose izven območja)?		
D.4	Ali ima sistem zmožnost prepoznavanja spremenjenih zapisov (skozi zgodovino dogodkov ali drugih mehanizmov, ki uporabnika opozarjajo na spremembo zapisov)?		
D.5	Če ima sistem zmožnost prepoznavanja spremenjenih zapisov, ali obstaja validacijska dokumentacija, ki dokazuje, da je bil ta mehanizem ustrezno testiran?		
D.6	Ali lahko pregledujemo "točne in popolne" kopije zapisov (n.pr.:surovi podatki, meta podatki) na računalniškem prikazu v obliki berljivi ljudem?		
D.7	Ali lahko "točne in popolne" kopije zapisov (n.pr.:surovi podatki, meta podatki) izpišemo?		
D.8	Ali lahko "točne in popolne" kopije zapisov (n.pr.:surovi podatki, meta podatki) kopiramo na prenosne elektronske medije oz. jih prenašamo elektronsko?		
D.9	Ali so možne skrite opombe ali skriti podatki za sistem? Če da, ali so opombe ali ti skriti podatki vključeni kot del zapisov pri izpisih ali elektronskem prenašanju zapisov?		
D.10	Ali nadzorno osebje področja trenutno pregleduje elektronske zapise o sistemu (Odgovori z NE, če se pregledujejo le papirni zapisi.)?		
D.11	Ali osebje za kakovost periodično inspicira ali pregleduje elektronske zapise na tem sistemu?		