

Mars 2002

Áreiðanleiki gagna í upplýsingakerfum

Leiðbeiningar um vélrænt
innra eftirlit fyrir stjórnendur
og starfsmenn ríkisstofnana

Efnisyfirlit

INNGANGUR	5
1. ÁREIÐANLEIKI RAFRÆNNA GAGNA.....	7
HVAÐ ER ÁREIÐANLEIKI?	7
HVERSU ÁREIÐANLEG ÞURFA GÖGNIN AÐ VERA?	8
LEIÐIR TIL AÐ META ÁREIÐANLEIKA RAFRÆNNA GAGNA	9
<i>Hversu erfitt er að breyta gögnunum?</i>	9
<i>Er uppruni gagnanna traustur?</i>	10
<i>Eru gögnin heil?</i>	10
<i>Bera gögnin þess merki að þau hafi verið samþykkt?</i>	11
<i>Eru gögnin á réttu formi?</i>	11
<i>Eru gögnin nægilega skýr?</i>	11
MANNLEGI ÞÁTTURINN.....	12
3. FORVARNIR	13
RÉTT GÖGN.....	13
HEIL GÖGN	21
GILD GÖGN	23
4. PRÓFANIR	29
RÉTT GÖGN.....	29
HEIL GÖGN	37
GILD GÖGN	40
5. LEIÐRÉTTINGAR	43
RÉTT GÖGN.....	43
HEIL GÖGN	45
GILD GÖGN	48
ORÐALISTI.....	51
HELSTU HEIMILDIR	53

Inngangur

Tölvuvæðing síðustu ára hefur haft í för með sér að fjárhagslegt innra eftirlit ríkisstofnana er að stórum hluta orðið vélrænt. Þetta þýðir að hefðbundnar eftirlitsaðgerðir, sem hingað til hafa verið framkvæmdar „handvirkt“, hafa nú verið byggðar inn í upplýsingakerfin og eru að nokkru leyti orðnar sjálfvirkar.

Markmið ritsins er að auka þekkingu ríkisstarfsmanna á þeim aðferðum sem vélrænt innra eftirlit byggist á. Ritinu er m.a. ætlað að nýtast stofnunum við val og stillingar nýrra upplýsingakerfa og einnig við endurbætur eldri kerfa. Það er samið með þarfir stjórnenda og almennra starfsmanna í huga en ekki forritara. Umfjöllunin miðar þannig fyrst og fremst að því að lýsa aðferðunum með almennu orðalagi og ekki er fjallað um ýmis atriði sem forritarar verða að huga að við vinnu sína.

Í ritinu eru taldar upp 86 vélrænar eftirlitsaðgerðir/atriði og þeim lýst í fáum dráttum. Þar sem við á eru nefnd dæmi um hvernig einstakar aðgerðir hafa verið útfærðar í upplýsingakerfum ríkisstofnana. Rétt er að taka fram að ekki er um tæmandi upptalningu að ræða en leitast er við að lýsa þeim aðferðum sem algengastar má telja. Enda þótt ritið sé einkum miðað við fjárhagsupplýsingakerfi, geta þær aðferðir sem fjallað er um einnig nýst til að tryggja öryggi gagna í annars konar kerfum.

Heiti eftirlitsaðgerðanna eru í mörgum tilvikum fengin úr Tölvuorðasafni Orðanefndar Skýrslutæknifélags Íslands. Aftast í ritinu er að finna lista yfir helstu hugtök sem fyrir koma og er þar að finna bæði íslensk og ensk heiti þeirra.

Ríkisendurskoðun 22. mars 2002

1. Áreiðanleiki rafrænna gagna

Hvað er áreiðanleiki?

Hugtakið áreiðanleiki vísar til þess hversu traust gögn í upplýsingakerfum eru talin vera. Gögn eru áreiðanleg ef þau eru talin gefa rétta mynd af tilteknu ástandi, þ.e. eru talin vera í samræmi við tiltekinn veruleika. Ýmislegt getur orðið til að draga úr áreiðanleika rafrænna gagna.

Almennt má segja að áreiðanleiki rafrænna gagna byggist á því að þau séu:

- *Rétt* - þ.e. skráð á réttan hátt, rétt unnin og rétt geymd.
- *Heil* - þ.e. að skráning sé tæmandi gögn séu heildstæð.
- *Gild* - þ.e. ekki úrelt.

Það veltur bæði á því hvernig vélrænar innri eftirlitsaðgerðir eru útfærðar og á hæfni starfsmanna hvort gögn í upplýsingakerfum geti talist áreiðanleg í þeim skilningi sem að ofan greinir. Mikið er undir því komið að bæði stjórnendur sem taka ákvarðanir um val á nýjum upplýsingakerfum og starfsmenn sem vinna við kerfin og þeir sem forrita þau geri sér grein fyrir mikilvægi vélrænna eftirlitsaðgerða.

Vélrænar eftirlitsaðgerðir má í meginatriðum flokka í þrennt:

- *Forvarnir*
- *Prófanir*

▪ Leiðréttingar

Forvörnum er ætlað að koma í veg fyrir að röng gögn rati inn í upplýsingakerfi, prófanir leita að villum í gögnum sem þegar hafa verið skráð inn í kerfið, og leiðréttingum er síðan ætlað að lagfæra þær villur sem kunna að finnast.

Innan hvers aðgerðaflokks er gerður greinarmunur á því hvort aðgerðum er ætlað að tryggja að gögn séu rétt, heil eða gild. Í sumum tilvikum hafa aðgerðir tvíþætta virkni og geta þar af leiðandi fallið í fleiri en einn undirflokk.

Hversu áreiðanleg þurfa gögnin að vera?

Áður en hægt er að ákveða til hvaða vélrænna innri eftirlitsaðgerða skuli gripið þarf að svara eftirfarandi spurningu: Hversu áreiðanleg þurfa gögnin að vera sem unnið er með í kerfinu? Umfang aðgerða þarf að vera í samræmi við þá hagsmuni sem í húfi eru. Í sumum tilvikum er algerlega óásættanlegt að villa sé í gögnum. Slíkt á t.d. við um villu í lyfseðli sem getur bókstaflega verið lífshættuleg þeim sem seðillinn er stílaður á. Í öðrum tilvikum getur reynst nauðsynlegt að meta hvort of stífar vélrænar eftirlitsaðgerðir muni valda því að kerfi verði „þunglamalegt“ í vinnslu og skili þannig ekki þeim ávinningi og vinnusparnaði sem til er ætlast.

Leiðir til að meta áreiðanleika rafrænna gagna

Til að geta gengið úr skugga um áreiðanleika gagna í upplýsingakerfum þarf að spyrja eftirfarandi spurninga:¹

1. Hversu erfitt er að breyta gögnunum?
2. Er uppruni gagnanna traustur?
3. eru gögnin heil?
4. Bera gögnin þess merki að þau hafi verið samþykkt?
5. eru gögnin á réttu formi?
6. eru gögnin nægilega skýr?

Spurningarnar meta ólíka þætti sem tengjast áreiðanleiki gagna og er fjallað nánar um hvern og einn þeirra hér að neðan.

Hversu erfitt er að breyta gögnunum?

Ef auðvelt er að breyta þeim gögnum sem vistuð eru í upplýsingakerfum getur það vakið upp spurningar um áreiðanleika. Til samanburðar má nefna að yfirleitt er erfitt að breyta pappírsgögnum án þess að það sjáist. Þessi staðreynd veldur því að tiltölulega auðvelt er að staðfesta áreiðanleika pappírsgagna. Til að ganga úr skugga um að breytingar hafi ekki valdið villu í rafrænum gögnum verður að beita öðrum aðferðum, t.d. bera saman inntaksgögn og úttaksgögn. Einnig má nefna að þegar um er að ræða pappírsskjöl skiptir máli hvort skrifað er með blýanti eða penna. Svipuðu máli gegnir um rafræn gögn, þ.e. það skiptir máli hversu „varanleg“ skráning þeirra er.

¹ Þessar sex spurningar eru byggðar á matsþáttum sem fjallað er um í ritinu *The Information Technology Age: Evidential Matter in the Electronic Environment*. AICPA.

Er uppruni gagnanna traustur?

Líkur á því að gögn séu áreiðanleg aukast ef þau koma frá trúverðugum aðila og hægt er að fá staðfestingu hans á áreiðanleika þeirra. Sem dæmi má nefna að í sumum tilvikum getur reynst nauðsynlegt að stofnanir hafi aðgang að tölvukerfi banka, t.d. gegnum bankalínu eða heima-banka, til að geta útvegað staðfestingu á rafrænum gögnum.

Til að ganga úr skugga um áreiðanleika gagna sem eiga uppruna sinn hjá utanaðkomandi aðilum, þ.e. aðilum utan hlutaðeigandi stofnunar, er rétt að kanna hvaða innri eftirlitsaðgerðir sá aðili notar. T.d. eru gögn sem bera rafræna undirskrift að jafnaði trúverðugri en gögn sem ekki hafa hana. Rafrænar undirskriftir eru einnig í mörgum tilvikum mun áreiðanlegri heldur en hefðbundnar undirskriftir því að það er í flestum tilvikum nánast útilokað að breyta þeim.

Mun algengara er í rafrænum samskiptum en „hefðbundnum“ samskiptum að utanaðkomandi aðilar þurfi að staðfesta áreiðanleika gagna sérstaklega eftir að samskipti hafa farið fram. Í hefðbundnum viðskiptum er sjaldgæft að óskað sé eftir því að gögn séu staðfest skriflega eftir á. Eðli rafrænna viðskipta gerir slíkar staðfestingar í mörgum tilvikum æskilegar eða jafnvel nauðsynlegar.

Eru gögnin heil?

Pappírsskjal ber oftast með sér hvort það er heilt eða ekki. Auðvelt er að sjá hvort mikilvægar upplýsingar vantar eða hafa tapast af einhverjum ástæðum, t.d. vegna þess að skjalið hefur rifnað. Þegar um rafrænt skjal er að ræða getur oft verið erfiðara að sjá hvort um heilt skjal er að ræða eða ekki. Í skjölum á rafrænu formi eru oft kóðar sem ekki eru skiljanlegir nema þeir séu settir í

samhengi við önnur gögn. Þannig getur verið erfitt að gera sér grein fyrir því hvort þau séu heil eða ekki.

Bera gögnin þess merki að þau hafi verið samþykkt?

Þegar um er að ræða pappírsskjöl fer sjaldnast á milli mála hvort þau hafi verið samþykkt eða ekki. Það má yfirleitt ráða af því hvort þau bera undirskrift eða stimpil. Þegar um er að ræða rafræn gögn er samþykkið gjarnan rafrænt og innbyggt í færsluna. Erfitt getur verið að átta sig á hvað felst í samþykkinu, t.d. ef kóði er í samþykktarsvæði. Í slíkum tilvikum þarf að finna út hvað kóðinn merkir.

Eru gögnin á réttu formi?

Yfirleitt þarf ekki að nota sérstök verkfæri til að gera pappírsgögn skiljanleg, þ.e.a.s. að því gefnu að þau séu læsileg. Það sama á ekki við um rafræn gögn. Oftast er nauðsynlegt að nota sérstakan hugbúnað til að geta nálgast rafræn gögn á skiljanlegu formi. En ekki er sjálfgefið að það form sem þykir vera aðgengilegt og læsilegt sé jafnframt hentugt til að meta áreiðanleika gagnanna. Því er mikilvægt að starfsmenn þekki leiðir til að nálgast rafræn gögn á því formi sem gerir mögulegt að staðfesta áreiðanleika þeirra.

Eru gögnin nægilega skýr?

Yfirleitt er auðvelt að gera sér grein fyrir eðli og innihaldi pappírsgagna, sérstaklega þegar um er að ræða eyðublöð, t.d. reikninga, kvittanir o.s.frv. Eðli og innihald rafrænna gagna er hins vegar ekki ávallt jafn ljóst. Í þessu sambandi er mikilvægt að starfsmenn þekki leiðir til að bera kennsl á rafræn gögn. Í mörgum tilvikum verður að

lesa rafræn gögn í samhengi við önnur rafræn gögn til að komast að innihaldi þeirra. Einnig má gjarnan ráða ýmislegt af staðsetningu gagnanna, þ.e. hvar þau eru geymd í upplýsingakerfinu. Þetta bíður heim hættunni á því að túlkun gagna verði mismunandi eftir því hvaða starfsmaður á í hlut.

Mannlegi þátturinn

Þótt í ritinu sé fjallað um vélrænar innri eftirlitsaðgerðir nægja slíkar aðgerðir einar og sér ekki til þess að tryggja gott innra eftirlit. Nauðsynlegt er að starfsmenn átti sig vel á virkni aðgerðanna og því hvaða tilgangi þeim er ætlað að þjóna. Ef skilningur á hlutverki og eðli vélrænna innri eftirlitsaðgerða er ófullnægjandi nýtast þær ekki sem skyldi og jafnvel er hætta á að starfsmenn muni reyna að sniðganga þær til að komast hjá óþægindum.

Gjarnan eru upplýsingakerfi sem eru örugg og skila áreiðanlegum upplýsingum sögð vera „þunglamaleg“ í samanburði við „notendavæn kerfi“, sem í sumum tilvikum eru óörugg og ekki skila áreiðanlegum upplýsingum. Slík flokkun byggist oft á einföldunum og misskilningi. Oft á tíðum eru það innbyggð innri eftirlitsatriði sem gera það að verkum að kerfin þykja „þunglamaleg“. Eftir því sem meiri kröfur eru gerðar til áreiðanleika gagna í upplýsingakerfum, þeim mun meiri kröfur verður að gera til vélrænna innri eftirlitsaðgerða.

3. Forvarnir

Markmið forvarna er að reyna að koma í veg fyrir að óáreiðanleg gögn rati inn í upplýsingakerfi. Forvarnir á að byggja inn í kerfið við hönnun þess. Þær miða að því að koma í veg fyrir að tjón hljóttist af því að röng gögn eru vistuð í kerfinu.

Forvörnum má skipta í þrjá flokka eftir því hver tilgangur þeirra er, þ.e. hvort þeim er ætlað að tryggja að gögn séu rétt, heil eða gild.

Rétt gögn

Aðgerðir í þessum flokki eiga að tryggja að gögn séu rétt og að innbyrðis samkvæmni sé í þeim, þ.e. að gögn séu sett rétt inn, rétt sé unnið úr þeim og þau geymd rétt.

1. Vélræn innskráning: Með því að skrá vörur vélrænt inn í upplýsingakerfi með hjálp strikamerkingar eykst áreiðanleiki þeirra. Sama máli gegnir um gíróseðla og ávísanir sem hafa svokallaða OCR-línur.

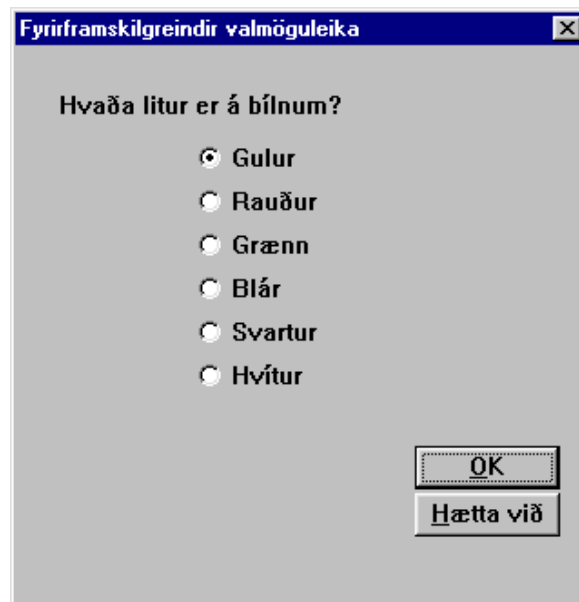


Mjög algengt er að vélræn innskráning sé notuð í verslunarrekstri og í bönkum til þess að auka áreiðanleika og hraða í afgreiðslu. Eina hættan sem fylgir þessari

aðferð er að ef rangt strikamerki er á vörunni eru minni líkur á að villan uppgötvist heldur en ef innskráning fer fram handvirkt. Gæta verður að því að ekki sé misræmi milli verðmerkingar vöru í hillu og þess verðs sem er skráð í upplýsingakerfinu.

2. Stöðluð skráning: Til eru mismunandi leiðir til að skrá gögn inn í upplýsingakerfi. Skráning getur verið ólík eftir því hvar hún fer fram og hvaða starfsmaður á í hlut. Þetta á ekki síst við um þegar skráning er háð huglægu mati. Í slíkum tilvikum getur reynst hentugt að nota staðlaða innsláttarmöguleika. Tilgangurinn með því er að minnka líkur á villum og auka samræmi í gagnasöfnum. Stöðluð skráning getur ennfremur verið nauðsynleg ef ætlunin er að vinna rafrænt með gögn, þ.e. vinna úr þeim í upplýsingakerfinu.

Dæmi: Þegar tiltekin einkenni hluta á borð við lit, lögun o.s.frv. eru skráð er hentugt að nota staðlaða valmöguleika.



Fyrirframskilgreindir valmöguleika

Hvaða litur er á bílnum?

- Gulur
- Rauður
- Grænn
- Blár
- Svartur
- Hvítur

OK

Hætta við

3. Sjálfshjálp: Æskilegt er að upplýsingakerfi séu með innbyggt kennsluefni fyrir atriði eins og hvernig standa eigi að innslætti gagna, uppfærslu gagna og leiðréttinga á villum.

4. Sjálfgefin gildi: Eru upplýsingar sem koma sjálfkrafa inn í innsláttarsvæði. Annað hvort hafa upplýsingarnar verið skilgreindar fyrirfram í kerfinu eða að sjálfgefna gildið er það sem síðast var slegið inn í svæðið.

Dæmi um sjálfgefin gildi eru t.d. fjárlaganúmer og ár, sem eru sjálfgefin gildi í Bókhalds- og áætlanagerfi ríkisins (BÁR). Sjálfgefið gildi í BÁR er byggt á síðasta fjárlaganúmeri sem viðkomandi notandi hefur slegið inn í kerfið.

Dæmi um atriði sem ekki ætti að nota sjálfgefin gildi um eru t.d. notandanöfn og lykilorð.



Sjálfgefin gildi

Nafn:

Heimili:

Sveitarfélag:

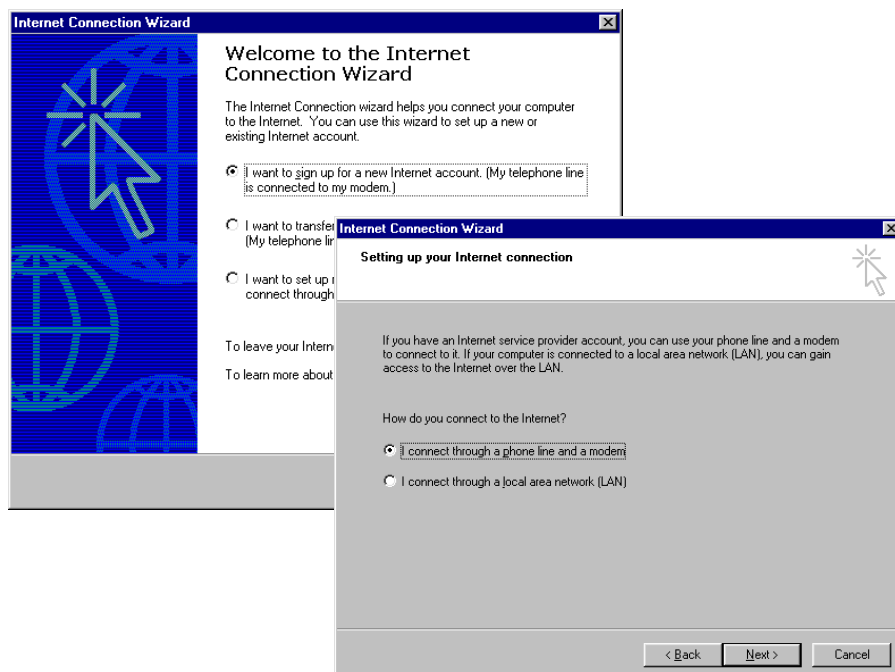
Land:

OK

Hætta við

5. Góð hönnun skjámynda: Hönnun skjámynda hefur mikla þýðingu fyrir það hversu auðvelt er að læra á og vinna í upplýsingakerfum. Verklag notanda á að ráða þeirri röð sem skjámyndir birtast í þegar unnið er að skráningu gagna. Eins er mikilvægt að ekki sé skráð of mikið af upplýsingum á eina og sömu skjámyndina. Mikilvægustu upplýsingarnar ætti að rita efst á skjámyndir og svipuð gögn ætti að hafa saman. Innsláttarröð gagna á skjámyndum ætti að vera eins og á innsláttareyðublaði eða öðrum upprunaskjöllum sem notendur vinna með.

6. Álfar (Wizards): Álfur er aðferð sem felst í því að notandinn er leiddur í gegnum ákveðið ferli þannig að hann slái inn umbeðin gögn á réttan hátt og í réttri röð. Þessari tækni er oft beitt þegar forrit eru sett upp í tölvu. Til dæmis mætti nefna uppsetningu á nettengingu með „Internet Connection Wizard“. Notandinn er leiddur í gegnum ferli spurninga og leiðbeininga, sbr. eftirfarandi dæmi.



7. Áherslumerkt svæði: Ein leið til að minnka líkur á villum er að draga athygli notandans að ákveðnum mikilvægum innsláttarsvæðum með því að merkja þau sérstaklega. Þetta er gjarnan gert með því að nota mismunandi liti í bakgrunni, feitletrun, undirstrikun eða jafnvel með blikkandi stöfum á skjánum.

Áherslumerking svæða er mikilvægt öryggisatriði í t.d. Gjaldkerakerfinu. Þar eru færslur merktar með þessum hætti til þess að sýna hvað er búið að afgreiða og hvað ekki.

Annað kerfi sem notar áherslumerkingar til að draga athygli notenda að ákveðnum svæðum er t.d. eignaskrárkerfi ríkisins þar sem svæði sem skylt er að slá inn í eru höfð gullituð á meðan önnur svæði eru með hvítum bakgrunni.

8. Ábendingar byggðar á greiningu (Screen diagnostic messages): Éru ábendingar sem kerfi kemur sjálfst með ef innsláttur gagna fer ekki fram á þann hátt sem búið er við eða ætlast er til. Þetta geta verið ábendingar um að láðst hafi að skrá tiltekna upplýsingar eða að notandi er beðinn um að staðfesta að hann vilji framkvæma tiltekna aðgerð. Dæmi um ábendingar byggðar á greiningu eru: „Kennitölu vantar“ eða „Viltu halda áfram?“

9. Númeraröð úthlutað af kerfi: Upplýsingakerfi tölusetur færslur sjálfvirkt þannig að þær myndi samfellda númeraröð. Samfelld númeraröð er mikilvægt öryggisatriði í fjárhagskerfum. sbr. 2. mgr. 5. gr. reglugerðar nr. 598/1999 um rafrænt bókhald, geymslu rafrænna gagna og lágmarkskröfur til rafrænna bókhaldskerfa. Þar segir:

„Rafrænn sölureikningur skal auk númera í gagnadagbók og sem fylgiskjal í bókhaldi fá númer í samfelldri númeraröð. Þetta númer skal ávallt koma fram í gagnadagbók og á rafrænu fylgiskjali bókhalds, bæði hjá sendanda og móttakanda svo og á prentuðu eintaki hans.“

10. Forútfylltar skjámyndir/eyðublöð: Umfang þeirra upplýsinga sem eru „fastar“ á skjámynd/eyðublaði getur verið mismunandi. Á forútfylltum skjámyndum hafa ákveðnar upplýsingar verið festar inn í tiltekin innsláttarsvæði, líkt og þegar um er að ræða sjálfgefin gildi (sjá 4. tölulið). Munurinn á forútfylltum skjámyndum og sjálfgefnum gildum er að notandi getur auðveldlega breytt sjálfgefnum gildum á meðan það kunna að vera takmarkanir á heimildum hans til að breyta innsláttarsvæðum á forútfylltum skjámyndum.

Forútfyllt skjámynd getur aukið áreiðanleika gagna með því að minnka líkur á því að röng gögn séu færð inn. *Dæmi:* Bókunarlykill er prentaður á reikningseyðublöð, t.d. reikningseyðublöð Ríkisféhirðis og ferðareiknings-eyðublöð Ríkisbókhalds.

11. „Endursend“ skjöl (turnaround documents): Eru rafræn skjöl sem geta gegnt mismunandi hlutverki eftir því hvar þau eru vistuð hverju sinni. Til dæmis getur sama skjal í upphafi verið reikningur til viðskiptavinar en síðar orðið fylgiskjal í bókhaldi. Skjöl af þessu tagi hafa verið notuð t.d. í skattkerfinu. Sent er út eyðublað í margriti sem hefur að hluta verið útfyllt af skattstjóra. Skattgreiðandinn bætir upplýsingum á eyðublaðið og sendir það síðan til baka. Hlutaðeigandi skattstofa vistar síðan afrit sitt af skjalinu sem upprunaskjal.

12. Ekki harðkóða forsendur eða breytur í forritakóða: Til þess að auðvelda viðhald og uppfærslu kerfa er nauðsynlegt að halda forsendum og breytum aðskildum frá forritunarkóðanum. Til dæmis borgar sig að hafa ýmis reiknihlutföll í gagnagrunni en ekki innbyggð í forritunarkóðann.

Ekki geta talist góð vinnubrögð við forritun að setja forsendur eða aðrar breytur inn í forritunarkóða. Ef það er gert þarf að kalla til forritara í hvert sinn sem breyta þarf forsendum eða breytum. Ef þessi atriði eru harðkóðuð getur það leitt til þess að mjög erfitt verður að stemma af færslur og gera leiðréttingar eftir á. Í BÁR eru breytur geymdar í gagnagrunnum. Mikilvægt er að þetta sé einnig gert í öðrum upplýsingakerfum.

Dæmi um forsendur sem ætti ekki að kóða eru skatthlutföll. Þó svo að skatthlutfall virðisaukaskatts sé 24,5% nú um stundir getur það breyst. Ekki er gott að breyta þurfi forritum þó svo að skatthlutfall virðisaukaskatts breytist.

13. Dulkóðun gagna: Allar sendingar viðkvæmra og mikilvægra gagna milli tveggja kerfa ættu að fara fram á dulkóðuðu formi. Dulkóðun ætti að beita óháð þeim miðli sem notaður er við flutninginn. Jafnframt kann að vera nauðsynlegt að geyma gögn á dulkóðuðu formi.

Dulkóðun er beitt í BÁR-ET þar sem færsluskrár eru á dulkóðuðu formi til þess að tryggja áreiðanleika þeirra.

14. Brúun gagna milli ólíkra upplýsingakerfa: Gjarnan er nauðsynlegt að umbreyta formi gagna til að unnt sé að flytja þau milli upplýsingakerfa. Forrit sem umbreytir formi gagna og flytur þau milli kerfa kallast gagnabré en aðferðin sjálf er nefnd brúun.

Augljóst er að ef gagnabré er af einhverjum ástæðum ófullkomin er líklegt að gögnin skili sér ekki óbrengruð milli kerfa. Mikilvægt er að ef breytingar eru gerðar á því kerfi sem gögn eru flutt úr, t.d. bætt við bókhaldslyklum, séu samtímis gerðar breytingar á gagnabréunni þannig að gögn skili sér rétt yfir í móttökukerfið.

Gagnabré eru mjög mikilvægar í ríkisrekstrinum, eins og t.d. við flutning ganga frá launakerfi ríkisins yfir í BÁR. Einnig skipta þær máli í beinum rafrænum viðskiptum þar sem t.d. gögn úr bókhaldskerfi eru þýdd yfir á EDIFACT-form áður en þau eru send til viðskiptavinar.

15. Gögn frá utanaðkomandi aðila: Ef stofnun tekur við gögnum frá utanaðkomandi aðila þarf hún að þekkja hvaða vélrænum innri eftirlitsaðgerðum sá aðili beitir til þess að tryggja áreiðanleika gagnanna. Þetta verður stofnunin að gera til að tryggja að sömu öryggiskröfur séu gerðar til allra gagna sem vistuð eru í upplýsingakerfum hennar. Ef þetta er ekki gert getur niðurstaðan orðið sú að óáreiðanleg gögn séu vistuð hjá stofnuninni, enda þótt mjög gott skipulag sé á vélrænu innra eftirliti innan hennar.

16. Hlutbundin hönnun: Aðferðir við hönnun upplýsingakerfis geta skipt miklu fyrir áreiðanleika þeirra gagna sem síðar eru vistuð í því. Í stórum dráttum má segja að hlutbundin hönnun felist í því að áður en vinna við forritun hefst er verkefninu, þ.e. upplýsingakerfinu, skipt í marga aðgreinda hluta. Markmiðið með því að skipta kerfinu upp er auðvelda skilning á virkni einstakra hluta og áhrifum þeirra á aðra hluta. Ef uppbygging kerfis er flókin, t.d. ef erfitt er að meta hvaða áhrif breyting sem gerð er á einum stað í kerfinu hefur annarsstaðar í kerfinu, er hugsanlegt að „leiðrétting“ á einum stað skapi villu á öðrum stað. Til að koma í veg fyrir að áreiðanleika gagna sé stefnt í hættu á þennan hátt þarf því að greina forritunarverkefnið vel niður áður en hafist er handa.

Góð hönnun einkennist m.a. af því að:

- (1) Hverjum hluta forrits er aðeins ætlað að leysa eitt afmarkað verkefni sem hægt er að ráða við í „viðráðanlegri stærð“ af forriti sem er ekki meira en 100 til 200 línur af forritunarkóða.
- (2) Aðeins eitt „atriði“ fer inn í hvern hluta forrits og aðeins er skilað einni „niðurstöðu“.
- (3) Aðskildir forritunarhlutar sjá um inntak, úttak, útreikning, villumeðhöndlun og meðhöndlun frávik.

17. Forritunarvenjur: Forritunarvenjur skipta mjög miklu fyrir áreiðanleika gagna vegna þess að villur í hugbúnaði hafa veruleg áhrif á áreiðanleikann. Með því að fylgja viðteknum gæðastöðlum við forritun er unnt að tryggja góðan árangur. Nokkur hugbúnaðarfyrirtæki hér á landi hafa fengið vottun á ferli sitt við hugbúnaðargerð. Algengast er að stuðst sé við ISO 9001- gæðastaðalinn.

18. Skjölunarvenjur: Þegar viðteknum skjölunarvenjum er beitt eru kerfis-, forritunar-, rekstrar-, neteftirlits-, þjónustuborðs- og notendahandbækur skýrar og heildstæðar. Nú eru kerfin sjaldan skjöluð á pappírformi heldur er skjölunin samofin kerfinu og byggð inn í það.

Heil gögn

Í þessum undirkafla er fjallað um forvarnir sem eiga að tryggja að gögn séu heil, þ.e. öll gögn séu færð inn, unnið sé úr öllum gögnum og öll gögn séu geymd.

19. Fornúmeruð eyðublöð: Samhangandi númeraröð ákveðinna skjala eða innsláttareyðublaða (eins og pantanaeyðublaða, reikninga eða ávísana) eru fornúmeruð til þess að hægt sé að fylgjast með því síðar hvort einhver eyðublöð hafi glatast.

Til dæmis er mælt fyrir um í 4. gr. reglugerðar nr. 50/1993 um bókhald og tekjuskráningu virðisaukaskattskyldra aðila að reikningar (sem ekki teljast til rafrænna sölu-reikninga) skuli vera tölusettir í samfelldri töluröð og að þessar upplýsingar skuli vera áprentaðar á allt upplag reikningseyðublaðanna áður en þau eru tekin í notkun.

20. Hætta við skráningu: Hægt er að hanna upplýsingakerfi þannig að ekki sé hægt að skrá sama eyðublaðið tvisvar. Notandanum er þá gefið til kynna að búið sé að skrá eyðublaðið með merkingu á borð við „móttekin“, „búið að vinna úr“ eða „greitt“. Dæmi um færslur sem þetta getur átt við um eru pantanir. Einnig er hægt að beita þessari tækni til að ógilda skráningu á ákveðinni færslu til þess að ná fyrri stöðu. Þó svo að þetta sé óheimilt eftir að skráningu færslu er lokið í bókhaldskerfum þá kann þetta að geta átt við í einhverjum öðrum kerfum.

21. Tímabilaskipting: Í fjárhagskerfum er brýnt að skráningu gagna sé skipt niður á tímabil. Þetta er mikilvægt til að tryggja heildstæð bókhaldsgögn og er í raun forsenda þess að hægt sé að gera áreiðanlegt milliuppgjör. Nauðsynlegt er að einungis takmarkaður fjöldi tímabila sé opinn til bókunar, t.d. 3 tímabil eins og skilgreint er í BÁR. Jafnframt er nauðsynlegt að síðasta tímabili ársins sé lokað þegar búið er að færa síðustu færslu ársins. Ef þetta er ekki gert er ekki hægt að ganga úr skugga um að reikningsskilin séu í samræmi við bókhaldið. Ástæða þessa er að ef tímabil er ekki lokað er hægt að færa á fyrri tímabil eða fyrri ár sem hefur það í för með sér að upphafsstöður á síðari tímabilum breytast.

Lotun gagna í tímabil er ekki aðeins mikilvægt atriði í fjárhagskerfum heldur nauðsynlegt í öllum upplýsingakerfum þar sem staða tiltekinna gagna á ákveðnum tímamarki skiptir máli.

22. Endamerking („End-of-file“ merking): Í mörgum tilvikum er nauðsynlegt að setja skýrar merkingar á enda skráa til að þeir sem nota skrána geti samfærst um það að þeir séu að vinna með gögnin í heild sinni. Þetta getur einnig átt við um aðrar tegundir gagna eins og t.d. útprentanir. Merkingu á enda skráar er ætlað að tryggja að verið sé að vinna með heildstæð gögn.

23. Aðskilnaður þróunarumhverfis og rekstrarumhverfis: Erfitt getur reynst að tryggja að gögn séu heil ef ekki er skýr aðskilnaður milli annars vegar þess tölvuumhverfis þar sem hugbúnaður er þróaður og prófaður, og hins vegar þess tölvuumhverfisins þar sem unnið er með raungögn. Ef gerðar eru breytingar á forriti í raunumhverfi geta komið villur í raungögnin sem erfitt er að finna og ógerningur verður að finna út hvað fór úrskeiðis ef slíkar villur finnast. Aðskilnaður af þessu tagi hefur því mjög mikla þýðingu fyrir áreiðanleika gagna.

Gild gögn

Í þessum kafla er fjallað um forvarnir sem ætlað er að tryggja að gögn séu gild, þ.e. þau séu ekki úrelt og að aðili sem til þess hefur heimild hafi skráð þau.

24. Samþykktarferli: Hægt er að byggja inn í upplýsingakerfi rafrænt samþykktarferli þannig að skráning sé ekki bæði framkvæmd og staðfest/samþykkt af einum og sama notandanum. Samþykktarferlið byggist yfirleitt á aðgangsorðum og lykilorðum en líklega verður stutt í það að farið verði að nota snjallkort eða fingrafaralesara til að auðkenna notendur. Dæmi um notkun rafræns samþykktarferlis er að finna í gjaldkerakerfinu þar sem gjaldkeri verður að fá samþykki aðalgjaldkera fyrir uppgjöri dagsins.

25. Umsjónarmenn: Skynsamlegt er að fela ákveðnum starfsmönnum að hafa umsjón með tilteknum gögnum og

kerfum eða vera „eigandi“ þeirra. Umsjónarmenn eiga að sjá til þess að gögn sem eru á þeirra ábyrgð séu áreiðanleg. Eðlilegt er að umsjónarmenn gefi samþykki sitt áður en aðrir starfsmenn fá aðgang að gögnum eða forritum í umsjá þeirra.

26. Öryggisflokkun gagna: Þegar takmarka þarf aðgengi að ákveðnum upplýsingum er skynsamlegt að gögn séu merkt sérstaklega. Dæmi um slíkar merkingar eru „mikilvægt“, „viðkvæmt“, „trúnaðarmál“ o.s.frv. Öryggisflokkun gagna er nauðsynleg þegar tryggja þarf leynd upplýsinga, t.d. í heilsugæslunni og annarsstaðar þar sem unnið er með persónuupplýsingar. Til þessa hefur öryggisflokkun ekki farið fram í fjárhagskerfum ríkisins.

27. Lykilorð að ákveðnum aðgerðum: Í flestum rekstri er nauðsynlegt að búa þannig um hnúta að mismunandi starfsmenn hafi ólíkar heimildir til að vinna með gögn í upplýsingakerfum. Sérhvert kerfi þarf að geta greint á milli mismunandi notenda eftir því hversu langt heimildir þeirra ná. Með öðrum orðum, kerfið þarf að vita hvort notandi hafi aðeins rétt til að skrá og skoða upplýsingar, eða hvort hann megi breyta eða jafnvel eyða gögnum. Þetta er gert með því að auðkenna mismunandi notendur með lykilorðum. Einnig þarf að ákveða hvaða starfsmenn geti hundsáð villuboð, þ.e. þegar um óvenjulegar færslur er að ræða sem upplýsingakerfið gerir athugasemdir við. Dæmi um ábendingu sem kerfi kemur með ef starfsmaður hefur ekki heimild til að hundsá villuboð: „Útstöð eða notandi hefur ekki heimild til þess að gera þess aðgerð.“

Þessi tegund vélræns innra eftirlits er til staðar í BÁR. Hægt er að skilgreina mismunandi viðtækan aðgang og aðgerðir fyrir einstaka notendur.

28. Samþykki yfirmanns: Gera á kröfu um yfirmenn samþykki mikilvægar eða viðkvæmar færslur. Með því móti er komið á innra eftirliti í formi verkaskiptingar. Yfirmaður á að veita samþykki sitt rafrænt með því að slá

inn sérstakt leyniorð. Einnig er hægt að útfæra þetta samþykktuferli í formi rafrænnar undirskriftar ef t.d. færslan þarf að fara á milli mismunandi upplýsingakerfa.

Þetta öryggisatriði er notað í „Gjaldkerakerfinu“ þar sem einungis aðalgjaldkeri getur gert ákveðna hluti.

29. Stýring á samtímaaðgangi (Concurrent access controls): Stýra þarf aðgangi notenda í gagnagrunnskerfum á þann hátt að aðeins einn notandi geti uppfært gögn í einu. Ef þetta er ekki tryggt getur áreiðanleiki gagnanna verið í hættu. Yfirleitt er sjálfvirk læsing á skráum/færslum/svæðum þannig að einungis einn notandi getur unnið með þau í senn. Öll nýrri gagnagrunnskerfi hafa slíka sjálfvirka læsingu en huga verður að þessu atriði í sérsmíðuðum lausnum. Sérstaklega á þetta við hugbúnaðarlausnir sem upphaflega hafa verið forritaðar fyrir einn notanda en eru síðan keyrðar í fjölnotenduumhverfi.

Rétt er að taka fram að núorðið heyrir til algerra undantekninga að aðgangsstýring sé ekki fullnægjandi í upplýsingakerfum þar sem það er orðin regla frekar en undantekning að fleiri en einn notandi vinni í sama kerfinu í einu. Hins vegar þarf að gæta vel að því að aðgangsstýring sé í lagi þegar fartölvur eða lófátölvur koma við sögu. *Dæmi:* Starfsmaður A sækir skrá inn á staðarnet stofnunar en ákveður að vinna síðan með hana í fartölvu sem ekki er tengd við staðarnetið. Á meðan sækir starfsmaður B sömu skrá inn á staðarnetið og breytir henni þar. Þegar starfsmaður A hefur lokið vinnu sinni afritar hann skrána aftur á staðarnetið. Við þetta tapast þær breytingar sem starfsmaður B hefur gert.

Þess má geta að í nýlegri útgáfu af algengu ritvinnslukerfi er að finna möguleika til þess að bera saman mismunandi útgáfur af sömu skránni og að samræma innihaldið.

30. Sjálfvirk eyðing gagna: Í mörgum tilvikum er nauðsynlegt að haga málum þannig að gögn hafi takmarkaðan „líftíma“ í upplýsingakerfi. Það þýðir að gögnum er sjálfkrafa eytt þegar þau hafa verið vistuð í ákveðinn tíma í kerfinu. Þetta er gert til að koma í veg fyrir að ákvarðanir séu teknar á grundvelli úreltra gagna.

Í sumum tilvikum nægir að dagsetja gögn þannig að notandi geti gert sér grein fyrir því hversu gamlar upplýsingarnar eru. Dæmi: Fréttæfni á Netinu. Í öðrum tilvikum, t.d. þegar um er að ræða ýmiss konar töluleg gögn, getur reynst nauðsynlegt að byggja inn í upplýsingakerfi sjálfvirka eyðingu úreltra gagna.

31. Útgáfustjórn: Í ákveðnum tilvikum er nauðsynlegt að gögn og forrit lúti útgáfustjórnun. Hentugt getur verið að fela sérstökum starfsmanni að hafa umsjón með uppfærslu gagna í upplýsingakerfum. Sem dæmi um útgáfustýrð gögn má nefna lagasafn Alþingis á Netinu. Þegar lögum er flett upp á Netinu kemur jafnframt fram hvaða útgáfu lagasafnsins verið er að skoða ásamt upplýsingum um hvenær lagasafnið var síðast uppfært.

32. Rafræn undirskrift: Ein þeirra aðferða sem hægt er að beita til þess að tryggja að gögn séu gild eru rafrænar undirskriftir. Í gildi eru lög nr. 28/2001 um rafrænar undirskriftir. Í lögnum eru rafrænar undirskriftir skilgreindar á þessa leið: „Gögn í rafrænu formi sem fylgja eða tengjast rökrænt öðrum rafrænum gögnum og eru notuð til að sannprófa frá hverjum hin síðarnefndu gögn stafa.“

Þegar þær aðferðir sem beitt er við gerð rafrænna undirskrifta eru skoðaðar sést að þær eru í raun ekkert annað en dulkóðað tætigildi. Um tætigildi og dulkóðun er fjallað á öðrum stað í þessu riti.

33. Rafræn skilríki: Rafræn skilríki eru notuð til þess að auðkenna einstaklinga eða tölvur. Hafa svipað notagildi

og ökuskírteini þ.e. framvísun þeirra er krafist til þess að ganga úr skugga um það að aðili sé sá sem hann segist vera. Þó svo að notagildið rafrænna skírteina sé svipað og ökuskírteina þá er útfærslan allt önnur í rafræna umhverfinu. Rafræn skilríki kunna að vera geymd í snjallkortum eða á tölvu viðkomandi aðila. Tölvur geta einnig haft sín eigin rafrænu skilríki. Tilgangur þeirra er að votta að verið sé að eiga samskipti við t.d. réttan vefþjón.

Rafrænar undirskriftir og rafræn skírteini hafa fram til þessa lítið verið notaðar sem eftirlitsatriði hjá ríkisstofnunum. Helsta skýringin er sú að notkunarvið og kröfur í sambandi við rafrænar skilríki voru ekki skilgreindar af ríkinu fyrir en með skýrslu nefndar á vegum fjármálaráðuneytisins, sk. dreifilyklaneftndar, sem kom út nóvember 2001.²

34. Dagsetning upplýsinga. Mikilvægt er að skjöl sem sett eru á Netið séu dagsett þannig að lesendur þeirra hafi forsendur til þess að meta hvort upplýsingar eru gildar.

² Öryggisstefna fyrir rafræna stjórnsýslu á Íslandi - tillaga um að hrinda dreifilyklastefnu í framkvæmd -Nefnd um skipan dreifilykla í rafrænum viðskiptum. Fjármálaráðuneytið 2001. Sjá einnig: [www.fjarmalaraduneyti.is/interpro/fjr/fjr.nsf/Files/dreifilyklar/\\$file/dreifilyklar.pdf](http://www.fjarmalaraduneyti.is/interpro/fjr/fjr.nsf/Files/dreifilyklar/$file/dreifilyklar.pdf) .

4. Prófanir

Markmiðið með prófunum er að leiða í ljós mistök og villur sem gerðar hafa verið í tengslum við skráningu gagna í upplýsingakerfum. Prófanir beinast þannig að liðnum atburðum. Á grundvelli niðurstaðna prófana er síðan hægt að leiðrétta mistökin ef talin er þörf á.

Prófunum má skipta í þrjá flokka eftir tilgangi þeirra, þ.e. að tryggja að gögn séu rétt, heildstæð eða gild. Skipting kaflans í undirkafla er í samræmi við þessa flokkun.

Rétt gögn

Hér að neðan er fjallað um uppgötvandi vélrænar eftirlitsaðgerðir sem ætlað er að tryggja að gögn séu rétt og að innbyrðis samkvæmni sé í þeim, þ.e. gögn séu sett rétt inn, rétt sé unnið úr þeim og þau geymist rétt.

35. Tætisumma (hash totals): Tætifall er notað til þess að búa til tætisummu. Tætiföll eru reiknireglur sem notaðar eru í margvíslegum tilgangi. Tætiföll eru einnig mjög mikilvægur þáttur í mörgum aðgerðum þar sem dulkóðum kemur við sögu. Líkja má tætisummum við bunkasamtölur að öðru leyti en því að þær vinna á gagnasvæðum þar sem útkoman skilar engri merkingu, s.s. með samlagningu á tegundarlyklum allra færslna í bunka sem slá á inn eða samlagningu einhverra annarra svæða í færslunum. Dæmi um villuboð: Innslegin tætisumma er ekki sú sama og útreiknaða tætisumman.

Dulkóðað tætisumma er sú eftirlitsaðgerð sem áreiðanleiki rafrænnar undirskriftar hvílir á. Mikilvægi

Þessa eftirlitsaðgerðar er því mjög mikið. Rafræn undirskrift skv. lögum nr. 28/2001 er grundvölluð á tæti summu öryggisaðgerðinni. Rafræn undirskrift er í raun og veru ekkert annað en dulkóðuð tæti summa. Ef einum staf í texta sem hefur verið vottaður með rafrænni undirskrift er breytt stemmir tæti summan í undirskriftinni ekki lengur við útreiknaða tæti summu skjalsins sem leiðir til þess að rafræna undirskriftin verður ógild. Mikilvægi tæti summu sem eftirlitsaðferðar er því mjög mikið.

36. Stærðarprófanir:

Stærðarprófanir felast í því að kanna hvort tölur sem slegnar eru inn í innsláttarsvæði séu af réttri stærð miðað við tiltekna forsendur. Stærðarprófanir eru tvö konar:

Hámarks-/lágmarkspróf (limit check): Upplýsingakerfi kannar hvort tala fer yfir eða er undir skilgreindum mörkum. Kerfið birtir villuboð í þeim tilvikum þegar tala er hærri eða lægri en mörkin segja til um. Dæmi um villuboð: „Fjárhæð færslu er hærri en kr. 1.000.000“ eða „Pöntun er stærri en kr. 2.000.000“.

Talnabilspróf (range test): Upplýsingakerfi kannar hvort tala í tilteknu svæði sé á ákveðnu bili. Kerfið birtir villuboð í þeim tilvikum þegar tala fellur utan við bilið. Dæmi um villuboð: „Hlutfallið verður að vera á bilinu 10 til 75.“

37. Prófun á samræmi milli færslna (cross-record editing): Kannað er samræmi einnar færslu við aðrar færslur út frá tilteknum forsendum og leitar að færslum sem á einhvern hátt skera sig úr. Ef óregla uppgötvast birtir tölvakerfið villuboð.

Útfærsla prófana af þessu tagi getur verið með ýmsu móti. Í sumum tilvikum getur verið um að ræða prófun á því hvort færslur séu númeraðar í reglulegri röð. Í slíkum tilvikum birtir kerfið villuboð ef það finnur færslur sem ekki passa inn í röðina. Einnig má hugsa sér að samhengi færslna yfir tíma sé kannað og leitað að óreglu. Dæmi

um villuboð í slíkum tilvikum væri: „Tegundarlykill er ekki til í stofnskrá“.

38. Prófun á samræmi innan færslu (field combination test, cross-field editing o.fl.): Kannað er út frá tilteknum forsendum samræmi milli upplýsinga í svæðum innan sömu færslu. Ef ósamræmi uppgötvast birtir kerfið villuboð. Hægt er að útfæra þessa tegund prófunar á ýmsan hátt. Dæmi um villuboð: „Einstaklingur er fæddur 1980 og hefur því ekki rétt á því að vera á gjaldskrá ellilífeyrisþega“.

39. Könnun á líkindum (reasonableness test): Þessi prófun felst í því að kanna hvort gögn séu líkleg út frá fyrirframskilgreindum forsendum. Prófuð eru atriði eins og t.d. hvort tiltekin atriði séu „óeðlilega“ há eða „óeðlilega“ lág. Dæmi um villuboð: „Pantað magn þessa viðskiptavinar er ekki líklegt í ljósi viðskiptasögu hans.“

40. Sniðprófanir (format checks): Sniðprófanir eru notaðar til þess að kanna hvort gögn uppfylli ákveðnar formkröfur. Dæmi um villuboð sem sniðprófun sendir frá sér er: „Dagsetning er ekki sett fram með réttu sniði (dagsetning verður að vera á forminu dd.mm.áá)“.

41. Vartölur (check digits): Hægt er að láta gögn innihalda svokallaða vartölu sem reiknuð hefur verið út með ákveðinni formúlu. Forrit geta prófað með útreikningi hvort gögn standist vartölupróf. Í tölvukerfum hjá ríkinu hefur vartölupróf verið notað við tölvuvinnslu á kennitölum. Vartöluprófun kennitalna fer fram með eftirfarandi hætti:



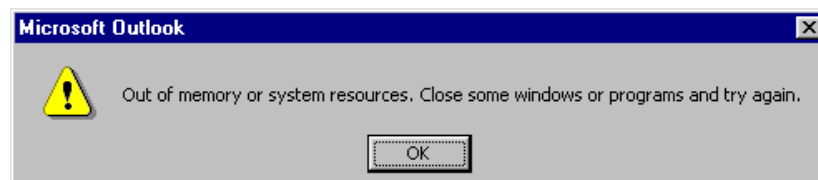
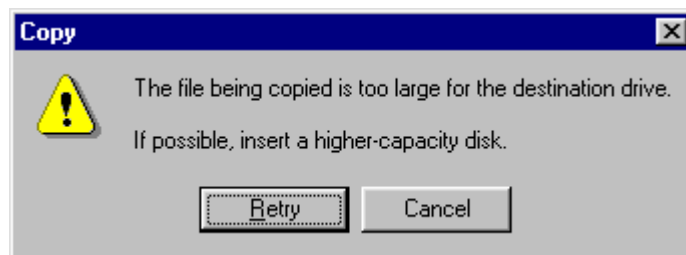
kennitala:	5 4 0 2 6 9 1 8 1 9
	* * * * * * * * * *
stuðlar:	3 2 7 6 5 4 3 2 1

Hver tala í kennitölunni er margfölduð með tölunni sem stendur fyrir neðan hana (stuðli) og síðan er útkoman lögð saman. Síðan er summunni deilt í 11 og ef útkoman er heil tala þá er kennitalan formlega gild. Vartalan er næstsíðasta talan í kennitölunni og hún tryggir að útkoman gangi upp í 11.

Kennitalan er ekki eina talan þar sem vartölupróf er notað. Algengt er að þessi próf séu innbyggð í vörunúmer. Sem dæmi mætti nefna þá er EAN-vörunúmerkerfið með innbyggða vartölu.³

42. Yfirflæðisprófanir (Overflow checks): Felast í því að áður en gögn eru vistuð, kannar kerfið hvort rúm sé fyrir þau í minni tölvu. Ef minni er á þrotum birtir kerfið sjálfkrafa viðvörðun um það. Hætta getur verið á að hluti gagna, t.d. fyrsti stafur í númeraröð, tapist ef kerfið varar notandann ekki við þannig að hann geti hætt við skráningu.

Dæmi um þessa tegund prófana eru t.d. eftirfarandi aðvaranir:



³ Sjá: www.ean.is

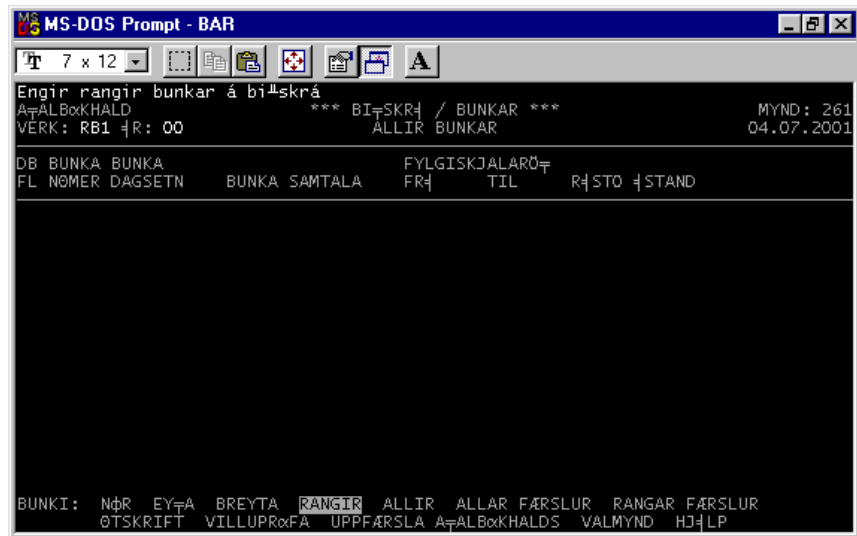
43. Formerkjaprófun (Sign test): Upplýsingakerfi gengur úr skugga um að rétt formerki, þ.e. + eða -, sé fyrir framan tölu í gagnasvæði og lætur notanda vita ef villa finnst. Eftirlit af þessu tagi er gjarnan notað í tölvukerfum til þess að greina á milli debit- og kredit-talna í bókhaldi. Dæmi um villuboð: „Fjárhæð í þessum tegundarflokki getur ekki verið með (-) sem formerki“.

44. Staðfesting á gildi (Validity checks): Upplýsingakerfi kannar hvort tilteknir kóðar eins og pósthúmer, starfsmannanúmer, skatthlutfall eða viðskiptanúmer séu gildir. Venjulega er þetta gert með því að bera skrá með gildum upplýsingum saman við það sem slegið hefur verið inn, t.d. skrá um pósthúmer. Dæmi um villuboð: „Pósthúmer er ekki til“ eða „Starfsmannanúmer er ekki til“.

45. Staðfestingar á haus og hala (Header and trailer record verifications): Þessi eftirlitsaðgerð gengur úr skugga um að:

- (1) Upplýsingar í haus (header) séu réttar, þ.e. að upplýsingar í fyrstu færslu í sérhverri skrá séu í samræmi við tilteknar forsendur.
- (2) Afstemmingarsamtölur í hala (trailer) séu réttar, þ.e. að tölur í síðustu færslu í sérhverri skrá séu í samræmi við samtölur eða talningar færslna.

Dæmi um villuboð: „Röng skrá hefur verið tekin til vinnslu“ eða „Upplýsingar í hala stemma ekki við útreiknaðar samtölur“.



46. Afstemmingarprófun (Balance controls): Hægt er að hanna upplýsingakerfi þannig að í sérhvert skipti sem upplýsingar eru skráðar inn í kerfið séu þær sjálfkrafa stemmdar af við aðrar færslur. Ef ósamræmi kemur í ljós birtir kerfið villuboð. Þetta er eftirlitsaðgerð sem oft er notuð í bókhaldskerfum, t.d. með því að stemma af debit- og kredit-fjárhæðir. Dæmi um villuboð: „Heildarfjöldi eininga stemmir ekki við fjölda eininga sem afgreiða á af hverjum lager fyrir sig.”

47. Samanburðarprófun (Comparison controls): Unnt er að hanna forrit þannig að það beri saman ákveðin gildi innan sömu færslu eða milli færslna. Dæmi um þessar tegundir eftirlitsaðgerða eru:

- (1) Samanburður á því verði sem fram kemur á pöntun annars vegar og reikningi hins vegar.
- (2) Samanburður á verði vöru við afhendingu og því verði sem fram kemur á reikningi.
- (3) Samanburður á þess sem greitt er fyrir vöru að viðbættum flutningskostnaði og sköttum við heildarfjárhæð reiknings.

- (4) Samanburður á einingarfjölda seldra afurða á síðasta uppgjörstímabili við einingarfjölda samkvæmt birgðastöðu.
- (5) Samanburður á samanlögðum debit fjárhæðum við samanlagðar kredit fjárhæðir í fjárhagsbókhaldi. Beiting þessar eftirlitsaðgerðar er háð viðfangsefni viðkomandi forrits sem þessar aðgerðir eru innbyggðar í.

48. Prófun á útreikningi (Computation controls): Unnt er að láta forrit leggja saman ýmsar stærðir og stemma af við aðrar stærðir. Ef villa uppgötvast birtir kerfið villuboð. Dæmi: „Heildarfjárhæð stemmir ekki við samlagningu á öllum færslulínum“.

49. Hlutfallaprófun (Ratio tests): Kerfið reiknar út hlutföll milli stærða í skráðum gögnum og kannar hvort þau eru rétt. Ef villa uppgötvast birtir kerfið villuboð. Til dæmis er hægt að láta kerfið reikna út hlutfall virðisaukaskatts af heildarvörusölu eða einhver önnur tiltölulega stöðug og þekkt hlutföll.

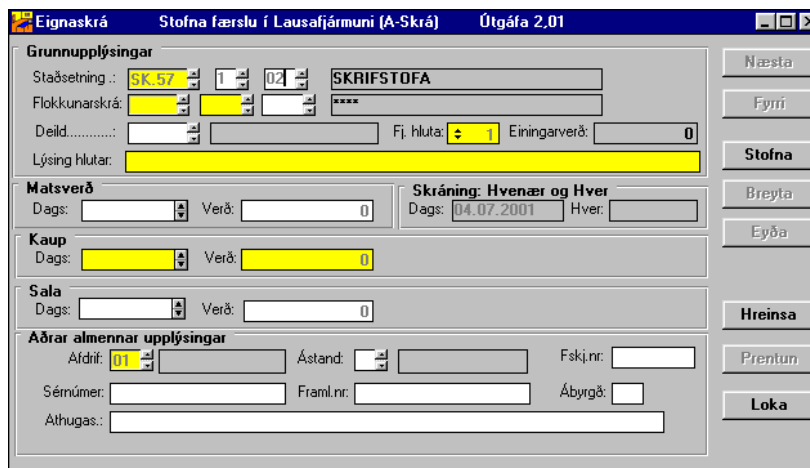
50. Afrúnnunaraðferðir (Rounding technique):

Í fjárhags- og bókhaldskerfum er gjarnan verið að reikna út tölur, margfalda, deila, leggja saman og draga frá fjárhæðir. Mjög mikilvægt er að skýrar reglur gildi um hvernig afrúnnun skuli fara fram. Mikilvægt er að fyrir liggi með hversu mörgum aukastöfum er unnið við margföldun og deilingu. Ákveða þarf hvort reikna eigi í aurum eða lækka alla útreikninga í næstu heilu krónu. Jafnframt verður að liggja ljóst fyrir hvernig farið verður með mismuninn sem getur skapast þegar afrúnnun er beitt. Samkvæmni verður að gæta þannig að sömu reglum sé beitt í öllum útreikningum sem gerð eru í tilteknu kerfi.

Þetta eftirlitsatriði er mjög mikilvægt í t.d. lánakerfum. Hjá ríkisaðilum gildir víða sú regla að við reikningagerð sé fjárhæð lækkuð niður í næstu heilu krónu. Einkafyrirtæki

beita hins vegar gjarnan þeirri reglu að lækka þær fjárhæðir sem eru innan við 50 auro en hækka þær fjárhæðir í næstu heilu krónu sem eru 50 auro eða hærri.

51. Gagnsær innsláttur (Descriptive readback): Er tækni við hönnun sem felst í því að þegar sleginn er inn kóði eða tala birtist skrifleg lýsing á því sem kóðinn eða talan vísar til sjálfkrafa í öðru innsláttarsvæði. Notandinn á því auðveldara en ella með að átta sig á því hvort hann hefur slegið inn réttan kóða eða tölu. Dæmi um notkun þessa öryggisatriðis: Þegar kóði er sleginn inn í eignarskárkerfi ríkisins birtist tegundarheiti þess sem slegið er inn.

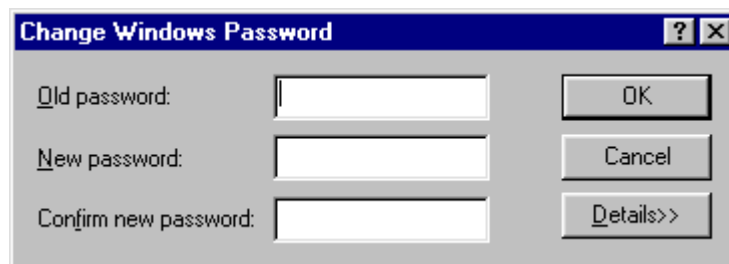


52. Kerfisrýni (System walk-throughs): Felst í því að áður en gerð upplýsingakerfis hefst fara aðilar skipulega í gegnum hönnun þess, kröfulýsingu, forritunarkóða, áætlun um prófanir kerfisins og gerð prófunargagna sem líkleg eru til leiða í ljós galla á kerfinu. Kerfisrýni er ætlað að koma í veg fyrir að forritarar misskilji hverjar þarfir notenda eru. Kerfisrýni getur sparað fé því ódýrara er að leiðrétta atriði sem vantar og villur á fyrstu stigum kerfisgerðarinnar heldur en á loka stigum hennar. Kerfisrýni er hægt að framkvæma bæði við gerð nýrra kerfa og þegar meiriháttar viðhald eða við endurbætur á kerfum sem fyrir eru.

53. Prófun gagnasvæða (Data checks): Forritarar eða þeir sem prófa forrit ættu að prófa að setja inn eyður í þau svæði þar sem tölur eiga að vera og prófa að deila með núlli þar sem innbyggður útreikningur byggist á deilingu. Prófun gagnasvæða á að koma í veg fyrir að tölvuvinnsla raskist vegna þess að forrit ræður ekki við að vinna úr tilteknum gagnasvæðum, t.d. vegna þess að það á í vandræðum með að deila með núlli.

54. Staðfestingarskráning (Key verification): Gjarnan er krafist tvískráningar á mikilvægum gögnum í þeim tilgangi að tryggja og staðfesta að þau hafi verið rétt slegin inn.

Þessi tegund eftirlitsaðgerð er t.d. alltaf notuð þegar lykilorði er breytt, sbr. myndin hér að neðan.



Heil gögn

Í þessum undirkafla er fjallað um prófanir sem hægt er að beita til þess að tryggja að gögn séu heil, þ.e. að öll gögn séu færð inn, unnið sé úr þeim öllum og þau séu geymd.

55. Bunkasamtölur: Upplýsingakerfi geta borið saman bunkasamtölur við handútreiknaðar og innslegnar afstemmingartölur. Hægt er að nota magntölur, línufjölda, skjöl eða fjárhæðir í þessu skyni. Þessari tegund prófunar er beitt við innslátt gagna í Bókhalds- og áætlanagerfi ríkisins (BÁR).

56. Prófun dagsetninga (Date checks): Þessa tegund prófana er hægt að nota til að tryggja að færsla sé skráð á rétt uppgjörstímabil. Í forrit eru innbyggð innbyrðis tengsl dagsetninga, t.d. getur afhendingardagsetning ekki komið á undan pöntunardagsetningu. Innbyrðis tengsl dagsetninga eru oft fyrir hendi í bókhaldskerfum þar sem ákveðin atburðarás er tímasett.

57. Staðfesting innri merkinga (Label checks): Upplýsingakerfi gengur úr skugga um að innri merking skráar eða segulbands sé rétt. Þetta er gert í því skyni að tryggja að við tölvuvinnslu sé verið að vinna með rétta skrá. Þegar verið er að vinna með gagnaskrár á geisladiskum, segulböndum eða öðrum miðli þar sem margar útgáfur eru til á skrá með sama nafni er þessi tegund eftirlitsaðgerða mjög mikilvæg. Dæmi um villuboð sem staðfesting á innri merkingu sendir frá sér er: „Reynt er að vinna með ranga skrá“.

58. Prófun á heildstæði (Completeness tests): Upplýsingakerfi getur kannað hvort eitthvað sé í svæðum sem eiga að vera auð eða hvort ákveðin gagnastök vanti eða sé ofaukið. Dæmi um villuboð sem þessi tegund eftirlitsaðgerðar sendir frá sér er: „Ekki heildstæð skráning þar sem heimilisfang vantar“.

59. Færslutalning: Upplýsingakerfi getur haft eftirlit með því að ekki sé unnið með fleiri færslur í einu en sem nemur tilteknum hámarksfjölda. Þetta er gert til að skrár sem unnið er með séu af viðráðanlegri stærð og til þess að tryggja að einstakar færslur tapist ekki í vinnslunni. Dæmi um villuboð sem kerfið sendir frá sér ef farið er yfir skilgreindan hámarksfjölda færslna: „Fjöldi færslna sem unnið var úr stemmir ekki við fjölda færsla í skránni sem unnið var með“.

60. Stærðarprófun: Þessi prófun er notuð til þess að kanna stærð innsleginna gagna. Til dæmis eru

símanúmer hér á landi almennt sjö tölustafir. Hægt er að búa þannig um hnúta að upplýsingakerfi aðvari notanda ef innslegið símanúmer er ekki nákvæmlega sjö stafir að lengd. Dæmi um villuboð: „Athugið að fjöldi tölustafa í innskráðum kennitölum á að vera tíu stafir“.

61. Prófun á samhengi raðar (Sequence checks):

Upplýsingakerfi kannar hvort röð eða númer færslna séu í réttu samhengi. Þessa prófun er t.d. hægt að nota til þess að kanna hvort númeraröð reikninga sé óslitin. Óslitin númeraröð getur í fyrsta lagi verið samfelld númeraröð. Dæmi: 1, 2, 3, 4, 5 o.s.frv. Í öðru lagi getur óslitin númeraröð falið í sér annars konar samhengi, t.d. getur hver færsla haft tvær slembitölur þannig að síðari talan sé jafnframt fyrri talan í númerinu sem kemur næst á eftir. Dæmi: 123-543, 543-265, 265-987, 987-345 o.s.frv.

Þessi tegund eftirlitsaðgerða er ekki einungis mikilvæg í fjárhagskerfum heldur er hún einnig mikilvæg þegar tvær eða fleiri tölvur þurfa að eiga samskipti. Dæmi um villuboð sem upplýsingakerfi birtir ef samhengi raðar er brenglað: „Reikning númer 1234567 vantar“.

62. Prófun á tvítekningum (Duplicate checks): Upplýsingakerfi kannar hvort færsla sé tvítekin og birtir villuboð ef svo er. Dæmi um villuboð: „Reikningur 1234567 virðist vera tvígreiddur“.

63. Kerfislæg útjöfnun (System matching): Í upplýsingakerfum er unnt að spyrða saman ákveðnar færslur. Til dæmis er hægt að jafna út pantanir og móttökustaðfestingar. Starfsmenn geta síðan prentað út lista yfir stakar færslur og gripið til viðeigandi ráðstafana ef t.d. vara sem þönguð hefur verið berst ekki.

64. Afstemming samtalna (Run-to-run totals): Unnt er að láta upplýsingakerfi reikna út ýmiss konar samtölur ólíkra færslna og stemma þær af. Ef misræmi uppgötvast birtir kerfið villuboð. Dæmi um villuboð: „Heildarfjárhæð

keyþtra vara er ekki jöfn samanlögðum kostnaði að viðbættum flutningskostnaði að frádregnum fengnum afsláttum”.

65. Úrkastsskrár (Suspense files): Upplýsingakerfi heldur utan um óunnar færslur og færslur sem unnar hafa verið að hluta og geymir í sérstökum biðskrá. Allar færslur sem bíða vinnslu eða hefur verið hafnað (vegna villu) eru geymdar í biðskrám svo hægt sé að skoða þær síðar og leiðrétt. Kerfið birtir villuboð um leið og færsla er flutt í biðskrá. Þetta fyrirkomulag er viðhaft svo að tryggt sé að allar villur séu leiðréttar. Dæmi um þessa tegund eftirlitsaðgerðar er fyrirkomulag innsláttar í BÁR-ET þar sem villuprófa þarf gögn áður en hægt er að uppfæra færslur í bókhaldið (sjá mynd 261 í BÁR-ET). Dæmi um villuboð: „Færslu hafnað” eða „Færsla ófullkomin, sett í biðskrá”.

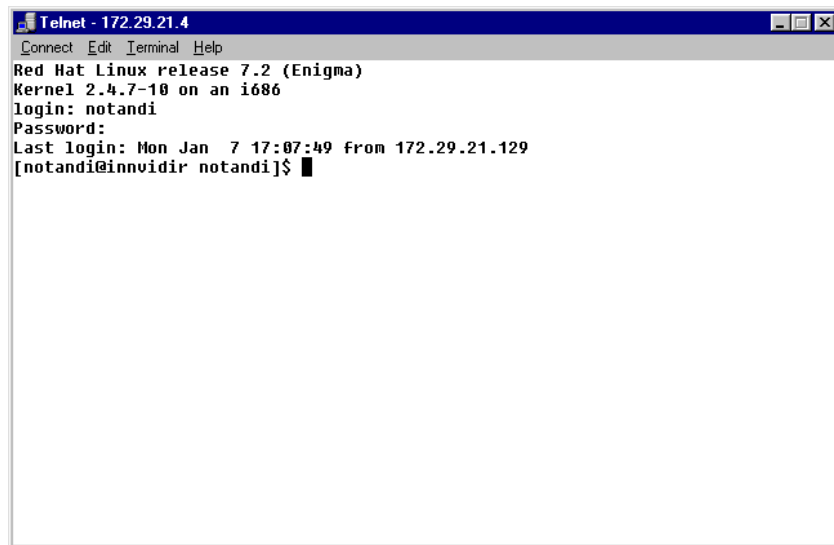
66. Færsla fyrir færslu eftirlit (One-for-One checking): Mikilvægar skýrslur eða innsláttargögn ætti að bera saman færslu fyrir færslu við niðurstöðu útprentunar til að staðfesta áreiðanleika, nákvæmni og heildstæðan gagnainnslátt og gagnavinnslu.

Gild gögn

Í þessum kafla er fjallað um prófanir sem ætlað er að tryggja að gögn séu gild, þ.e. þau séu ekki úrelt og að aðili sem til þess hefur heimild hafi slegið þau inn.

67. Skráning færslna í kerfisdagbók (System logging of transactions): Mikilvægt er að haldin sé dagbók yfir það hvaða notendur tengjast eða geta tengst kerfinu, færslunúmer, númer útstöðvarinnar sem notuð er, dagsetningu og tíma. Tilgangur þessarar dagbókar er að halda endurskoðunarslóð yfir það sem gerist í kerfinu og hvaða notendur er ábyrgir fyrir því.

Kerfisdagbækur er t.d. hægt að nota með þeim hætti að notanda er sagt hvenær hann var síðast að vinna í kerfinu þegar hann tengist kerfinu. Þetta er prófun sem getur upplýst viðkomandi notanda um það ef einhver annar hefur komist yfir leyniorð hans að kerfinu og er að nota viðkomandi kerfi í hans nafni (sjá mynd hér að neðan).



```
Telnet - 172.29.21.4
Connect Edit Terminal Help
Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686
login: notandi
Password:
Last login: Mon Jan  7 17:07:49 from 172.29.21.129
[notandi@innvidir notandi]$
```


5. Leiðréttingar

Leiðréttingar eru oftast gerðar í framhaldi af því að prófun hefur leitt í ljós villu. Leiðréttingar geta falist í beinni leiðréttingu eða í uppsetningu á nýrri forvörn eða prófun.

Mikilvægt er að leiðrétting sé gerð eins nálægt uppruna villunnar og kostur er. Ef starfsmaður hefur gert villu í t.d. gagnainnslætti ætti hann að fá villuboð um það og vera gefinn kostur á að leiðrétta villuna strax. Það þykir ekki gott fyrirkomulag að sérstakur starfsmaður sé í því að leiðrétta villur eftir aðra starfsmenn. Í þeim tilvikum þegar tölvari leiðréttir villur sem einhverjir aðrir starfsmenn hafa gert verður að tryggja að þeim sem villuna gerði sé gerð grein fyrir henni og því að hún hafi verið leiðrétt.

Leiðréttingum má skipta í þrjá flokka með sama hætti og forvörnum og prófunum, þ.e. í fyrsta lagi leiðréttingar til að tryggja að gögn séu rétt, í öðru lagi heil og þriðja lagi gild. Skipting kaflans í undirkafla er í samræmi við þessa flokkun.

Rétt gögn

Í þessum kafla er að finna leiðréttingandi aðgerðir sem ætlað er að tryggja að gögn séu rétt og að innbyrðis samkvæmni sé í þeim, þ.e. gögn séu rétt skráð, rétt sé unnið úr þeim og þau geymist rétt.

68. Skýringartexti í forritunarkóða: Gott er að hafa skýringartexta í forritunarkóða til að hjálpa forriturum að

skilja forritið. Þannig verður auðveldara að leiðrétta og uppfæra forritin.

Dæmi um skýringartexta í forritunarkóða er:

```
if(a > 0.0 && b == 0 ) { /* Skýringartexti */  
  if(c == 0.0) {  
    e = e + d; /* skýring á þessari samlagningu*/  
    f = g * h; /* fleiri skýringar */  
    ....
```

69. Skýringar í verkstýriskrá (Job control comments): Gott er að hafa skýringartexta í fjölvum sem stýra tölvuvinnslum til þess að hjálpa forriturum að leiðrétta og viðhalda kóðanum og tölvurum til þess að skilja tilgang verksins.

70. Dagbækur með endurskoðunarslóð (Audit trail reports): Kerfi ætti að hafa innbyggða skýra og heildstæða endurskoðunarslóð sem hægt er að nota til þess að rekja og staðfesta hvaða framgangur og aðgerðir hafa verið framkvæmdar í kerfinu.

71. Afstemmingarskýrslur (Control reports): Út úr kerfinu ætti að vera hægt að fá skýran og heildstæðan lista yfir runuvinnslueftirlit og kerfisdagbækur sem það heldur. Notendur eiga að geta nýtt sér slíka lista við afstemmingar og staðfestingar.

72. Skýrslur um frávik (Exception report): Skýrslur um frávik verður að vera hægt að búa til þegar nota á upplýsingar af því tagi. Útfærsla slíkra skýrslna er háð þeim verkefnum sem viðkomandi upplýsingakerfi er ætlað að fást við.

73. Aldursgreiningar: Unnt er að láta upplýsingakerfi aldursgreina ýmis gögn og birta yfirlit um niðurstöðuna. Til dæmis er hægt að láta kerfi gefa skýrslu um allar viðskiptakröfur sem eru orðnar eldri en 30 daga.

74. Villulistar: Hægt er að láta upplýsingakerfi prenta út lista sem sýnir allar færslur sem hafnað hefur verið vegna villu í þeim. Í listanum þarf að koma fram eðli villunnar, hversu alvarleg hún er og tillaga um hvernig leiðréttta eigi þær.

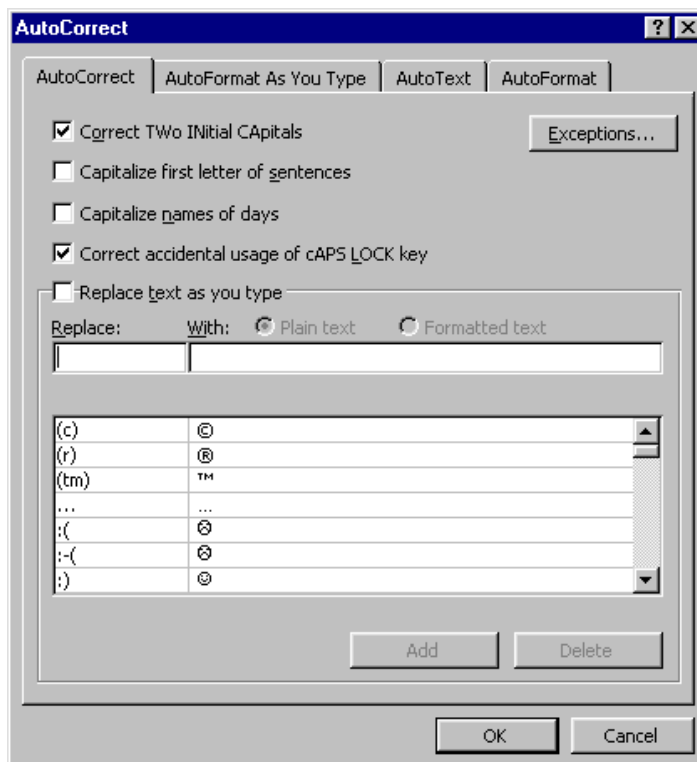
75. Staða fyrir og eftir breytingu (Before/after image record reporting for file maintenance): Þótt breytingar séu gerðar á gögnum í innsláttarsvæðum verður upplýsingakerfi að geta sýnt hvaða gildi voru svæðunum áður en breyting var gerð. Notendur eiga þá auðvelt með að ganga úr skugga um að ekki hafi orðið mistök við breytingar, t.d. á forsenduskrám.

76. Villusamtölur: Til þess að auðvelda leiðréttingar á villum ætti að láta upplýsingakerfi skila villusamtölum þar sem villur eru sundurliðaðar eftir tegundum, deildum, stöðum, færslutegundum, útibúum eða fyrirtækjum. Hægt er að gera samtölur yfir villur í fjárhæðum, einingafjölda eða fjölda færslna.

Heil gögn

Í þessum kafla er fjallað um leiðréttingar sem hægt er að gera til þess að tryggja að gögn séu heildstæð þ.e. öll gögn færð inn, unnið sé úr öllum gögnum og öll gögn séu geymd.

77. Sjálfvirk leiðrétting: Upplýsingakerfi er hannað þannig að það leiðréttir villur sjálfkrafa út frá skilgreindum forsendum. Sjálfvirk leiðrétting á einkum við þar sem ekki er nauðsynlegt að starfsmaður meti hvort slík leiðrétting eigi rétt á sér. Dæmi um sjálfvirka leiðréttingu sem byggð er inn í forrit er t.d. sjálfvirk stafsetningarleiðrétting í Microsoft Word.

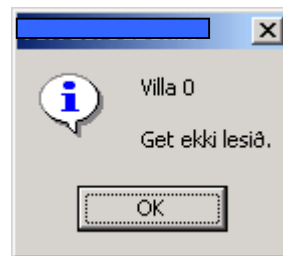


78. Framleiðnimælingar: Skýrslur sem sína vinnumagn á ákveðnu tímabili. Til dæmis fjölda innsleginna tákna, fjölda skjala sem unnið er með, fjölda forritaðra lína, fjölda afgreiddra mála o.s.frv. Framleiðnimælikvarða sem hægt er að byggja inn í upplýsingakerfi er hægt að nota sem verkefnavísa fyrir viðkomandi stofnun eða sem grundvöll launagreiðslna (bónusgreiðslna). Þegar fyrirhugað er að nota slíka framleiðnimælikvarða verður að kanna hvort þeir samrýmist lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

79. Skýr og heildstæð villuboð: Til þess að auðvelda leiðréttingar ættu öll villuboð að vera auðskiljanleg og hafa skýra merkingu. Villuboð ætti að orða á einfaldan

hátt, ekki vera með neikvæðu orðalagi og ekki vísa í villukóða.

Dæmi um óskýrt villuboð:



80. Sjálfvirk afritataka og endurheimt (Automatic backup and recovery): Upplýsingakerfi ætti að hanna með þeim hætti það taki reglulega sjálfkrafa afrit af öllum skráum þannig að hægt sé að endurræsa kerfið eftir að það hefur hrunið af einhverjum ástæðum. Í sumum tilvikum er endurræsing kerfisins sjálfvirk eftir að það hefur „hrunið“. „Autosave“ í Word er dæmi um útfærslu á sjálfvirkri afritatöku.

81. Dagbókarfærsla (Journaling): Allar færslur sem skráðar eru inn í upplýsingakerfi ætti að geyma í sérstakri dagbókarskrá (log) sem gerir mögulegt að ná inntaksfærslunni til baka og endurtaka úrvinnslu ef kerfið hrynur.

82. Geymsla gagna: Skilgreina þarf geymslutíma fyrir öll gögn hvort heldur sem þau eru á pappír eða rafrænu formi. Sé reglum um geymslu gagna fylgt er tryggt að stofnun geti mætt kröfum innri eða utanaðkomandi aðila um upplýsingar.

83. „Bakka með“ færslur (Transaction backout): Í upplýsingakerfum ætti að bjóða upp á þann möguleika að hægt sé að „bakka með“ færslur sem valda villum í viðkomandi kerfi, eins og t.d. ógildar færslur.

Dæmi um þetta er að finna í BÁR. Í BÁR er hægt að bakka með færslur sem eru rangar því að villuþrófa verður allar færslur og stemma af bunka áður en mögulegt er að uppfæra færslur endanlega inn í bókhaldið.

84. Endurheimtugabók (Recovery logging): Í gagnagrunnskerfum ætti að vera sérstök endurheimtugabók sem geymir upplýsingar um stöðu einstakra færslna sem eru í vinnslu auk þess að geyma upplýsingar um þau atriði sem breytt hefur verið í gagnagrunninum. Bæði upplýsingar um gögn sem voru í einstökum svæðum fyrir og eftir breytingar er hægt að geyma í endurheimtugabókum. Þetta er grundvöllur þess að hægt sé að ná aftur rétttri stöðu gagnagrunns þegar mistök hafa orðið við breytingar (rollback).

Endurheimtugabók er gjarnan útfærð þannig að þegar breyting er gerð á gögnum eða ný gögn eru skráð inn þá eru þau ekki skráð inn í aðalskrár gagnagrunnsins heldur eru þau skráð í biðskrá (database buffer). Gögn er ekki færð inn í aðalskrána fyrr en ákveðnum tíma liðnum eða með sérstakri uppfærsluaðgerð. Á meðan færslan er í biðskránni er hægt að ná henni til baka (rollback) og þar með ná upphaflegri stöðu gagnagrunnsins.

Gild gögn

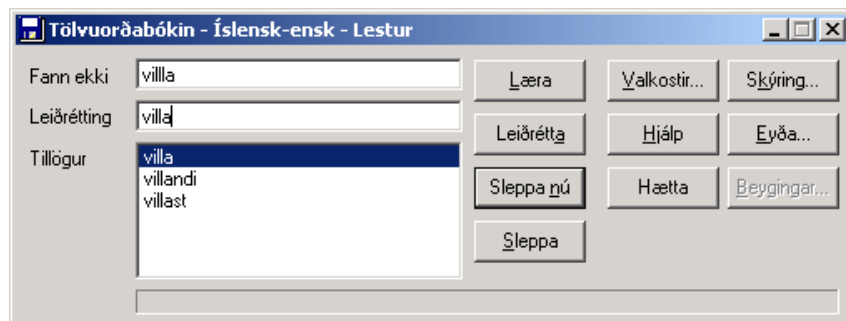
Í þessum kafla er gerð grein fyrir leiðréttingum sem ætlað er að tryggja að gögn séu gild, þ.e. séu ekki úrelt og að aðili sem til þess hefur heimild hafi slegið þau inn.

85. Rétt skjölun: Réttar og uppfærðar kerfis-, forritunar-, tölvurekstrar-, netkerfis-, hjálpar- og notendahandbækur eru mikilvægar. Þær aðstoða þá sem greina, forrita, reka og nota upplýsingakerfi við að leiðrétta villur, svara spurningum og leysa vandamál sem upp koma við viðhald, rekstur og notkun upplýsingakerfa. Skjölun er því

mjög mikilvæg eftirlitsaðgerð til þess að tryggja áreiðanlega gagnavinnslu.

86. Heimildir yfirmanna til þess að hundsá villur (Overrides by supervisors): Í sumum tilvikum eru þau villuboð sem upplýsingakerfi birtir ekki rétt af einhverjum ástæðum. Kerfi verður að hanna með þeim hætti að heimild til þess að hundsá mikilvæg og alvarleg villuboð og láta hjá líða að leiðrétta þær villur sem um ræðir, sé takmörkuð við fáa og vel skilgreinda yfirmenn. Að auki er rétt að sérstaks leyniorðs sé krafist til að unnt sé að hundsá villur.

Þegar því verður við komið ætti að hanna kerfi með þeim hætti að þegar villuboð er hundsá sé það dagbókarfært þannig að hægt sé að finna tilvikið síðar ef ágreiningur kemur upp. Einfaldasta dæmið um hvernig kerfi gerir ráð fyrir að hægt sé að hundsá villuboð eru leiðréttingarforrit fyrir stafsetningu. Slík forrit gera tillögur að leiðréttingum sem notandi getur hundsá („Sleppa nú“ og „Sleppa“ í myndinni hér fyrir neðan). Þótt e.t.v. sé að jafnaði ekki þörf á því að samþykki yfirmanns sé gert að skilyrði fyrir því að unnt sé að hundsá stafsetningarvilluboð. Hins vegar getur samþykki yfirmanns verið mjög mikilvægt í ýmsum fjárhagskerfum.



Orðalisti

Forvarnir (fyrirbyggjandi aðgerðir) - Preventive Controls
Prófanir (uppgötvandi aðgerðir) - Detective Controls
Leiðréttingar (leiðréttandi aðgerðir) - Corrective Controls

Netið - The Internet
Álfar - Wizards
Sjálfgefin gildi - Default Options
Upplýst svæði - Field highlighting
Heimakær skjöl - Turnaround documents
Dulkóðun - Encryption
Bunkasamtölur - batch control totals

Tætigildi - hash totals
Markgildisprófun - Limit Check
Líkindaprófun - Reasonableness Test
Vartala - Check Digit
Yfirflæðisprófun - Overflow check
Sniðprófun - Format Check
Prófun dagsetninga - Date Check
Staðfesting innri merkinga - Label Check
Könnun á heildstæði - Completeness test
Jaðraprófun - Range Test
Færslutalning - Record Count
Formerkjaþrófun - Sign Test
Könnun á stærð - Size Test
Könnun á samfelldni raðar - Sequence Check
Könnun á tvítekingum - Duplicate Checks
Könnun á samræmi innan færslu - Cross-field Editing

Könnun á samræmi við aðrar færslur - Cross-record Editing

Kerfislæg jöfnun - System matching

Prófun á samræmi milli svæða - Field Combination Test

Staðfesting á gildi - Validity Check

Afstemming samtalna milli vinnslna - Run-to-run Totals

Úrkastsskrá - Suspense Files

Staðfestingar á haus og hala - Header and Trailer Record Verification

Könnun á jöfnuði - Balance Control

Skráning færslna í kerfisdagbók - System Logging of Transactions

Samanburðarprófun - Comparison Controls

Prófun á útreikningi - Computation Controls

Könnun á hlutföllum - Ratio Tests

Afrúnnunaraðferðir - Rounding Technique

Gagnsær innsláttur - Descriptive Readback

Kerfisrýni - System Walk-through

Prófun gagnasvæða - Data Check

Staðfestingarskráning - Key Verification

Færsla fyrir færslu eftirlit - One-for-One Checking

Sjálfvirkar leiðréttingar - Automatic error correction

Hunsa stjórnenda á villum - Management Overrides

Endurskoðunarslóð - Audit Trail

Villusamtölur - Error Totals

Helstu heimildir

ÍST ISO/IEC 17799:2000 Upplýsingatækni -

Starfsvenjur fyrir stjórnun upplýsingaöryggis

Staðlaráð Íslands (2001)

1998 CISA Review Technical Information Manual

Information System Audit and Control Association (1998)

CISA Examination Review Book, Volume 1: Theory

S. Rao Vallabhaneni (1991)

Tölvuorðasafn

Orðanefnd Skýrslutæknifélags Íslands

Íslensk málnefnd (1998)

Rekstraröryggi upplýsingakerfa

Ríkisendurskoðun (1998)

Computer Related Risks

Peter G. Neumann

ACM Press (1995)

The Software Conspiracy

Mark Minasi

McGraw Hill (2000)

Rätt data?

Studier av informationskvalitet i statliga ADB-system

Riksrevisionsverket, Sverige (1990)

The Information Technology Age: Evidential Matter in the Electronic Environment

AICPA