BORUT JEREB

INFORMATIKA IN INFORMACIJSKA VARNOST

REPETITORIJ

Univerzitetna založba
Univerze v Mariboru

Univerza v Mariboru

Fakulteta za logistiko

Informatika in informacijska varnost

Repetitorij

Avtor
dr. Borut Jereb

Marec 2019

Naslov Informatika in informacijska varnost

Podnaslov Repetitorij

Title Informatics and Information Security

Subtitle Repetitorium

Avtor *Author*
izr. prof. dr. Borut Jereb
(Univerza v Mariboru, Fakulteta za logistiko)

Avtorja poglavja 8 (1. izdaja) *Authors chapter 8 (1st edition)*
dr. Borut Jereb in Mateja Izlakar

Recenzija *Review*
red. prof. dr. Bojan Rosi
(Univerza v Mariboru, Fakulteta za logistiko)

red. prof. dr. Tone Lerher
(Univerza v Mariboru, Fakulteta za logistiko)

Jezikovni pregled *Language editing in Slovenian*
dr. Vesna Mia Ipavec in Darja Kukovič, mag.

Tehnična urednika *Technical editors*
izr. prof. dr. Borut Jereb
(Univerza v Mariboru, Fakulteta za logistiko)

Jan Perša, mag. inž. prom.
(Univerzitetna založba Univerze v Mariboru)

Oblikovanje ovitka *Cover designer*
Jan Perša, mag. inž. prom.
(Univerzitetna založba Univerze v Mariboru)

Grafika na ovitku *Cover graphics*
Pixabay.org (CC 0)

Izdajatelj/ *Co-published by*
Univerza v Mariboru, Fakulteta za logistiko
Mariborska cesta 7, 3000 Celje, Slovenija
http://fl.um.si, info.fl@um.si

Založnik / *Published by*
Univerzitetna založba Univerze v Mariboru
Slomškov trg 15, 2000 Maribor, Slovenija
http://press.um.si, zalozba@um.si

Izdaja *Edition*
Prva izdaja

Vrsta publikacije *Type of publication*
E-knjiga

Dostopno na *Available at*
http://press.um.si/index.php/ump/catalog/book/385

Izdano *Published*
Maribor, marec 2019

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

004.4(075.8)

JEREB, Borut, 1962-
Informatika in informacijska varnost [Elektronski vir] : repetitorij / avtor Borut Jereb. - 1. izd. - El. učbenik. - Maribor : Univerzitetna založba Univerze, 2019

Način dostopa (URL): http://press.um.si/index.php/ump/catalog/book/385. - Nasl. v kolofonu: Informatics and information security

ISBN 978-961-286-251-0

doi: 10.18690/978-961-286-251-0
1. Dr. vzp. stv. nasl.
COBISS.SI-ID 96327681

ISBN 978-961-286-251-0 (PDF)

DOI https://doi.org/10.18690/978-961-286-251-0

Cena *Price* Brezplačni izvod

Odgovorna oseba založnika *For publisher* red. prof. dr. Zdravko Kačič, rektor Univerze v Mariboru

Univerzitetna založba
Univerze v Mariboru

Informatika in informacijska varnost

Repetitorij

BORUT JEREB

Povzetek Informatika je veda o informacijah in načinih njihovega procesiranja ter o upravljanju informacijskih sistemov. Ker se z informacijami srečujemo skoraj povsod v vsakdanjem življenju in se z njimi ukvarjamo vse bolj, je informatika vpeta v domala vse pore našega življenja. Predstavljata "infrastrukturo" in nudi podporo ostalim poslovnim procesom. Izzivi v informatiki so povezani z zahtevano kakovostjo storitev, z investicijami, tveganji, poslovnim lastništvom in z njihovim upravljanjem. V gradivu je informatika opisana z varnostnega vidika. Skladno s tem vidikom zahtevamo predvsem, da so informacije: (a) razpoložljive, (b) celovite in (c) zaupne, v obsegu kot je to potrebno za potrebe izvajanja poslovnih procesov. Informatika mora poskrbeti za širšo podporo poslovnim procesom v zahtevanem obsegu. Torej je informatika področje, ki predstavlja infrastrukturo v logistiki. V manjši meri velja tudi obratno, a vendarle je informatika podstat za logistiko, saj predvsem z informacijskimi procesi omogočamo izvajanje logističnih.

Ključne besede: • informatika • informacijska varnost • Varnostno kopiranje • Računalniški vdor • Varnostni incident • Standard • Upravljanje tveganj • IT investicija • Dokumentni sistemi • Vodenje projektov •

NASLOV AVTORJA: dr. Borut Jereb, izredni profesor, Univerza v Mariboru, Fakulteta za logistiko, Mariborska cesta 7, 3000 Celje, Slovenija, e-pošta: borut.jereb@um.si.

DOI https://doi.org/10.18690/978-961-286-251-0 ISBN 978-961-286-251-0
Dostopno na: http://press.um.si.

Kazalo

Slike

Tabele

Poglavje 1

Informatika in informacijska varnost

Informatika je veda o informacijah in načinih njihovega procesiranja ter o upravljanju informacijskih sistemov. Ker se z informacijami srečujemo skoraj povsod v vsakdanjem življenju in se z njimi ukvarjamo vse bolj, je informatika vpeta v domala vse pore našega življenja. Pri tem logistika ni izjema – celo več – v eni od definicij logistike je zapisano: "... logistika zajema fizični tok materiala in tok informacij od dobavitelja, ..." [33]. V tej definiciji pojem *informacija* nastopa kot predmet, na katerega se logistika osredotoča. Obe področji, informatika in logistika, se ukvarjata z informacijami.

Tako logistika kot informatika sta tudi nujni področji za izvajanje poslovnih procesov v podjetjih. Predstavljata "infrastrukturo" in nudita podporo ostalim poslovnim procesom. Imata podobne izzive, povezane z zahtevano kakovostjo storitev, z investicijami, tveganji, poslovnim lastništvom in z njihovim upravljanjem. In vendar je razlika v tem, da informatika predstavlja področje, ki mora podpirati nemoteno delovanje logistike. Torej je informatika področje, ki predstavlja infrastrukturo v logistiki. V manjši meri velja tudi obratno, a vendarle je informatika podstat za logistiko, saj predvsem z informacijskimi procesi omogočamo izvajanje logističnih.

V nadaljevanju bo predstavljena informatika v povezavi in v odnosu s splo-

šnimi poslovnimi procesi in ne le z logističnimi. Pri tem gre za dva vidika – v okviru prvega so logistični procesi tudi poslovni procesi, v okviru drugega so logistični procesi podporni procesi ostalim poslovnim procesom na višjem nivoju upravljavske piramide podjetja. Tako so hierarhično v podobnem položaju kot informacijski procesi. Iz slednjega izhajajo mnoge podobnosti in njihove lastnosti med informacijskimi in logističnimi procesi.

Na vsako področje lahko gledamo z več zornih kotov. V nadaljevanju bo opisana informatika z varnostnega vidika. Skladno s tem vidikom zahtevamo predvsem, da so informacije

- razpoložljive,
- celovite in
- zaupne

v obsegu kot je to potrebno za potrebe izvajanja poslovnih procesov. Informatika mora poskrbeti za širšo podporo poslovnim procesom v zahtevanem obsegu. V primeru logistike to pomeni, da moramo zagotavljati razpoložljivost, celovitost in zaupnost informacij v takšnem obsegu, da je mogoče zagotoviti, da je [33]

- pravo blago ali storitev,
- v pravi količini,
- v pravi kvaliteti,
- na pravem mestu,
- ob pravem času

tako, da so upoštevani kriteriji:

- najnižjih stroškov in
- najmanjših vplivov na okolje ter
- da je storitev opravljena v skladu s sklenjeno pogodbo.

V pomembnejših standardih in tudi v tem gradivu govorimo o pojmu *organizacija*, s katerim opisujemo vse tipe profitnih ali neprofitnih organizacij. Sem spadajo podjetja iz zasebnega in javnega sektorja ter ostale neprofitne organizacije.

1.1 Definicije nekaterih najpogosteje uporabljanih izrazov s področja informatike

V tem poglavju bodo predstavljeni osnovni pojmi, ki so povezani z informatiko. Njihov pomen bo pojasnjen s pomočjo definicij. Pri tem moramo upoštevati, da ima lahko vsak pojem več pomenov, definicije se namreč razlikujejo tudi glede na konkretnost. Ker se z informatiko poglobljeno ukvarjamo šele v zadnjih nekaj desetletjih, pojmi niso splošno ponotranjeni in jih mnogokrat uporabljamo v njihovem približnem ali celo napačnem pomenu. Odvisni so tudi od popularnosti posameznega izraza v nekem okolju. Logistika je tehnično in timsko naravnano področje, zato je potrebno pri delu uporabljati čim bolj konkretno definirane in natančno razumljene pojme – tudi iz področja informatike. To je obenem pogoj za kompetentno izvajanje profesionalnega dela.

1.1.1 Informatika

V splošnem pomenu besede je informatika znanost o informacijah. Pri informatiki proučujemo strukture, algoritme, obnašanje in medsebojne vplive med naravnimi in umetnimi sistemi, ki shranjujejo in procesirajo informacije, omogočajo dostop do informacij in omogočajo njihovo izmenjevanje. Informatika proučuje sodelovanje in medsebojne vplive med ljudmi in informacijsko tehnologijo (IT). Kot takšna vključuje široko pahljačo strokovnjakov iz različnih področij. Z razvojem računalnikov se je procesiranje informacij digitaliziralo. To je pripeljalo do tega, da informatiko proučujemo predvsem skozi področje matematike, računalništva, kognitivnih in družbenih ved ter skozi druge vplive, ki jih ima informacijska tehnologija na družbo. Informatika kot področje znanosti ni odvisna le od tehnološkega vidika upravljanja z informacijami, medtem ko to velja za področji informacijske tehnologije in računalništva.

Pojem informatika ima v Evropi drugačen pomen kot v Angliji ali ZDA. V Evropi si pod tem pojmom predstavljamo največkrat zgolj računalništvo (ali računalniško znanost) v najširšem smislu in z njim povezane discipline. V ZDA pojem informatika predstavlja tudi dimenzijo umetnosti, človeškosti informacijskih tehnologij. V Angliji poudarjajo pri definiciji pojem procesiranja in komuniciranja z informacijami v nekem sistemu, tako da le to vključuje vidik računalništva,

kognitivni in socialni vidik.

Informatiko lahko definiramo kot znanstveno disciplino, ki raziskuje strukture in lastnosti informacij, neoziraje se na njihovo vsebino. Raziskuje zakonitosti izračunavanja informacij (računalništvo) in metodologije upravljanja informacij.

1.1.2 Informacijska tehnologija in informacijski sistem

Pod pojmom informacijska tehnologija (IT) si predstavljamo široko pahljačo tehnologij (računalniki, telekomunikacijska oprema, televizorji, telefoni in druge programabilne elektronske komponente in naprave) in dejavnosti (pridobivanje, prenos, obdelava, shranjevanje), ki so v organizacijah povezane z upravljanjem in procesiranjem informacij.

IT je po definiciji organizacije ITAA (Information Technology Association of America) študij, načrtovanje, implementacija, podpora in upravljanje informacijskih sistemov, ki temeljijo na programski in strojni opremi računalnikov [30].

Tako lahko v splošnem opišemo, da se IT ukvarja s:

- Strojno opremo računalnikov;
- Programsko opremo računalnikov, ki omogoča
  - pretvorbo,
  - shranjevanje,
  - zaščito,
  - procesiranje in
  - prenos podatkov; ter
- Pridobivanjem informacij v vsakem času iz katerega koli vira.

Na osnovi takšne definicije danes govorimo tudi o IT oddelkih v podjetjih in o IT strokovnjakih, o upravljanju IT tveganj, IT investicijah in o upravljanju IT na splošno.

Izraz informacijski sistem se nanaša na interakcijo med ljudmi, procesi in tehnologijo. Ti vplivi lahko presegajo okvir organizacije. Informacijski sistem tako ni samo tehnologija, temveč tudi način uporabe te tehnologije in medsebojnega vplivanja med ljudmi, prav tako pa pomeni tudi tehnologijo pri izvajanju poslovnih procesov in/ali njihovem nadzoru. Je oblika komunikacijskega sistema, v

katerem so informacije predstavljene in se obdelujejo kot oblika družbenega spomina. Informacijski sistemi tako vključujejo komponento IT takrat, ko imamo opraviti z interakcijo med ljudmi in procesi, ter predstavljajo pomemben del informatike [29].

1.1.3 Računalništvo

Računalništvo je študij teoretičnih osnov informacij, izračunavanja in praktičnih tehnik za njihovo implementacijo na računalnikih ali računalniških sistemih. Pri tem gre za sistematičen študij vseh procesov, ki ustvarjajo, opisujejo in transformirajo informacijo. Računalništvo sestavlja pahljača disciplin, ki segajo od izračunavanja specifičnih rezultatov (kot je računalniška grafika), do disciplin, ki se ukvarjajo s posameznimi lastnostmi algoritmov (na primer z njihovo kompleksnostjo) za izvajanje izračunavanja. Poleg tega so tudi discipline, ki pokrivajo različne problematike, povezane s samo implementacijo izračunavanja. V slednjo skupino spada na primer teorija programskih jezikov, s katero opisujemo izračunavanje.

V nadaljevanju so navedena teoretična področja računalništva, ki so združena v več skupin [28].

1. Teoretične osnove računalništva, kamor spadajo:
   (a) matematična logika;
   (b) teorija avtomatov;
   (c) teorija števil;
   (d) teorija tipov – formalna analiza podatkovnih tipov in njihova uporaba, ki je potrebna za razumevanje lastnosti programov; še posebej njihove varnosti;
   (e) matematične strukture;
   (f) teorija grafov – osnova za strukture podatkovnih skladišč in iskalnih algoritmov;
   (g) kriptografija – algoritmi za zaščito zasebnih podatkov, ki vsebuje tudi enkripcijo;
   (h) kvantni Turing-ovi stroji.

2. Teorija izračunavanja, ki se deli na:
   (a) teorijo izračunavanja v ožjem pomenu – Turing-ovi stroji in
   (b) teorijo kompleksnosti – osnova za izračunavanje časovnih kompleksnosti in zahtev za potreben prostor ob izračunavanju.
3. Algoritmi in podatkovne strukture, med katere sodijo naslednja področja:
   (a) analiza algoritmov,
   (b) algoritmi – formalni procesi, ki jih uporabljamo za izračunavanje, in njihova učinkovitost ter
   (c) podatkovne strukture.
4. Programski jeziki in prevajalniki:
   (a) Programski jeziki – formalni jeziki, ki predvsem omogočajo izraziti algoritme in tudi lastnosti teh jezikov.
   (b) Prevajalniki – prevajanje računalniških programov, ponavadi iz višjenivojskih v nižjenivojske.
5. Numerično in simbolično izračunavanje, med katere sodi pahljača naslednjih področij:
   (a) Bioinformatika;
   (b) Kognitivna znanost;
   (c) Izračunavanje v kemiji;
   (d) Nevronske mreže;
   (e) Izračunavanje v fiziki;
   (f) Numerični algoritmi; ter
   (g) Simbolna matematika.

Vsa ta teoretična računalniška področja uporabljamo pri naslednjih tehničnih računalniških področjih (pozor: prej smo govorili o teoretičnih, zdaj pa o tehničnih področjih):

1. Operacijski sistemi – sistemi za upravljanje računalniških programov in podatkovnih struktur;

2. Računalniške mreže – algoritmi in protokoli za zanesljivo izmenjavo podatkov prek večjih razdalj; večkrat vsebuje detekcijo in korekcijo napak;
3. Računalniška grafika;
4. Računalniški vid;
5. Podatkovne baze;
6. Računalniška varnost;
7. Umetna inteligenca;
8. Robotika;
9. Interakcija med ljudmi in računalnikom; ter
10. Sočasni, paralelni in distribuirani sistemi.

Pestrost področij potrjuje izjava enega od očetov računalniške znanosti Edsgerja Dijkstro, ki je izjavil: "Računalniška znanost ima prav toliko skupnega z računalniki, kot ima observatorij skupnega s teleskopi." [28]

1.1.4 Upravljanje z informacijami in informacijska arhitektura

Upravljanje z informacijskimi viri (ki so: informacije, aplikacije, IT infrastruktura in ljudje) predstavlja razvoj in izvajanje načrtov, politik, praks in procedur, ki na pravilen način upravljajo s celotnim življenjskim ciklom informacij tako, da zagotavljamo zahteve in potrebe organizacije.

Sem spadajo naslednja področja:

1. Modeliranje informacij;
2. Administracija informacijskih baz;
3. Skladiščenje informacij;
4. Prenašanje informacij;
5. Rudarjenje v/po informacijskih bazah;
6. Zagotavljanje kvalitete informacij;

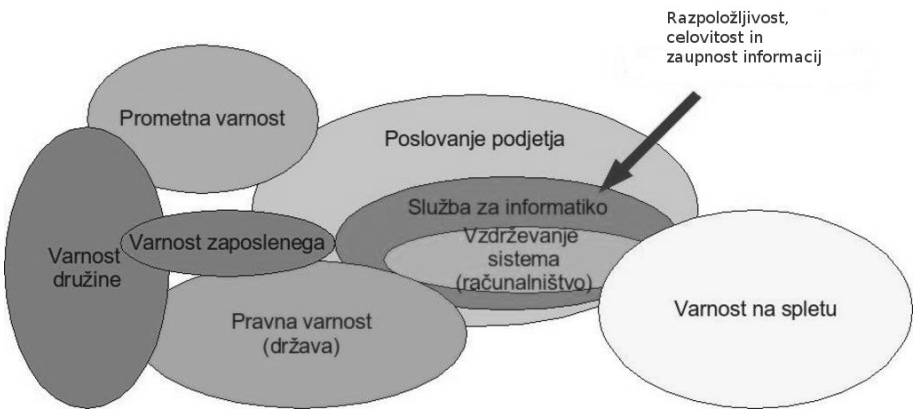
7. Varnost informacij;
8. Upravljanje z informacijami o podatkih (meta-data); ter
9. Strategije informacijskih arhitektur.

Informacijska arhitektura je upravljanje s strukturiranjem informacij in znanj. Te so ponavadi strukturirane glede na njihov kontekst (pomen). Izraz uporabljamo pri uporabi spleta ali pri večjih informacijskih bazah in opisuje specializirana znanja za upravljanje z informacijami in uporabo informacijskih orodij. V veliki meri je v interakciji z bibliotekarstvom, dokumentnim poslovanjem in arhiviranjem.

Pri načrtovanju informacijskega sistema pomeni modeliranje podatkovnega modela analiziranje in načrtovanje informacij v sistemu in njihovih medsebojnih odvisnosti. Pri informacijski arhitekturi podatkovno modeliranje postane predvsem abstrakcija. Medsebojne odvisnosti med deli podatkov postanejo pomembnejše od posameznih podatkovnih zapisov, zato izdelujemo kataloge vseh mogočih podatkovnih vrednosti, načini dostopa do teh vrednosti pa postanejo osrednja problematika arhitekture.

1.2 Uporaba informatike kot orodja za doseganje ciljev organizacij

Poglavje o uporabi informatike je za naš namen najenostavneje predstaviti skozi optiko sloja uporabnikov in upravljavcev organizacije. To napravimo prek opisovanja varnostnih zahtev za delovanje informatike v neki organizaciji. Varnostni vidik informatike ni samo pisan na kožo upravljavskemu in uporabniškemu sloju v posamezni organizaciji, temveč je tudi najširše in najkvalitetnejše opisan pristop za upravljanje informatike nasploh. Za zaposlene na področju logistike je informatika infrastruktura, kjer zaposleni nastopajo v smislu *odjemalcev* ali *kupcev* informacijskih storitev. Odjemalci teh storitev in upravljavski sloj organizacije morajo vedeti, kaj lahko in kaj morajo pričakovati od informatike, kakšna je njihova vloga pri določanju zahtev in odgovornosti. To ne velja samo za zgornji upravljavski sloj, temveč tudi za vse vmesne sloje (in seveda za uporabnike na splošno). S takšnim pristopom se bomo v nadaljevanju osredotočili predvsem na

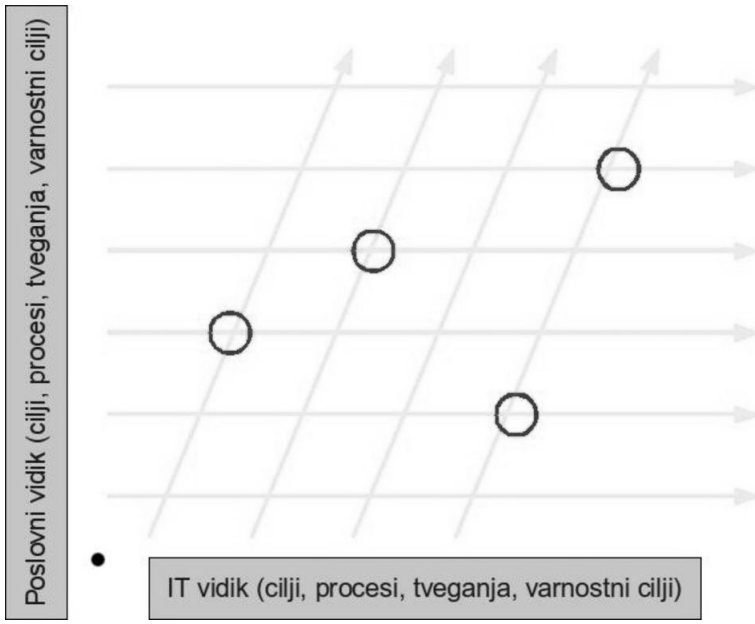


Slika 1.1: Varnost, s katero se srečujemo v vsakdanjem življenju (lasten vir)

organizacijski vidik upravljanja z informacijami, ki naj bo prilagojen srednjemu upravljavkemu sloju (na področju logistike) v podjetjih. Slika 1.1 predstavlja različne varnosti, s katerimi se srečujemo v vsakdanjem življenju, njihovo prepletanje in medsebojne odvisnosti.

1.2.1 Osnovna vloga IT v luči varovanja informacij

V vsaki organizaciji je osnovna vloga informatike podpora, vzdrževanje in razvoj poslovnih strategij in ciljev organizacije. Pri tem se pri posameznih poslovnih procesih, ciljih, tveganjih in navsezadnje s poslovnimi varnostnimi cilji srečujemo z informacijskimi procesi, cilji, tveganji in varnostnimi cilji. Pri tem praviloma (vendar ne vedno) poslovni (tudi varnostni) cilji definirajo informacijske (tudi varnostne) cilje, informacijska tveganja pa se prenašajo na nivo poslovnih tveganj. Te medsebojne odvisnosti prikazuje slika 1.2, na kateri s krogci označujemo presečišča, kjer bodisi z informacijskimi procesi podpiramo izvajanje poslovnih procesov bodisi poslovne cilje prenašamo na informacijske cilje tako, da bodisi prvi določajo druge bodisi informacijska tveganja postanejo del poslovnih tveganj, ali pa celo investicticije v informacijsko infrastrukturo postanejo integralni



Slika 1.2: Križanje poslovnega in IT področja (lasten vir)

del vseh (poslovnih) investicij in jih kot takšne tudi obravnavamo.

Sistemi za upravljanje informacijskega varovanja so načrtovani tako, da zagotavljajo primerno in proporcionalno izbiro varnostnih kontrol, s katerimi varujemo informacijske vire. To je predpogoj za potrebno zaupanje vsem zainteresiranim uporabnikom v izvajanje osnovne vloge informacijskih tehnologij v neki organizaciji.

Sistemi za upravljanje informacijskega varovanja predstavljajo varnostni model, ki organizaciji zagotavlja predvsem:

1. *Razpoložljivost* informacij – pravočasno zagotavljanje informacij uporabnikom na način, kot jih potrebujejo in uporabljajo za izvajanje svojih poslovnih zahtev;

2. *Celovitost* informacij – zagotavljanje točnosti, popolnosti in neoporečnost informacij; ter

3. *Zaupnost* informacij – zagotavljanje varovanja informacij pred razkritjem nepooblaščenim osebam in zagotavljanje odgovornosti oseb za dejanja v zvezi z njim dostopnimi informacijami.

Pri vpeljavi sistema za upravljanje informacijskega varovanja gre za strateško odločitev same organizacije glede zahtev za:

- vzpostavitev,
- implementacijo,
- obratovanje,
- spremljanje delovanja,
- vzdrževanje ter
- nenehno izboljševanje

sistema informacijskega varovanja, v kontekstu splošnih operativnih in poslovnih tveganj organizacije. Pri tem je verjetno samo po sebi razumljivo, da mora biti sistem informacijskega varovanja dokumentiran.

Vse aktivnosti, od vzpostavitve, prek implementacije, obratovanja, spremljanja, vzdrževanja, pa do nenehnega izboljševanja sistema informacijskega varovanja morajo biti zastavljene tako, da so aktivnosti odvisne od potreb in ciljev organizacije, od varnostnih zahtev, poslovnih procesov ter od velikosti in strukture same organizacije. Pri tem moramo upoštevati, da se sistemi, ki podpirajo poslovanje, skozi čas pričakovano dinamično spreminjajo skupaj s potrebami in cilji. Pomembno je, da je obseg varovanja skladen s potrebami organizacije in da jih ne presega.

1.2.2 Informacijski viri

Tisto, kar imamo v informatiki na razpolago za zagotavljanje zahtevane informacijske varnosti, so informacijski viri. To je tisto, s čimer v informatiki delamo, kar upravljamo in kar "nas obdaja", kar je "naše okolje". To je tudi tisto, kar ščitimo, da bi zagotovili celovitost, razpoložljivost in zaupnost informacij prek izvajanja IT procesov.

Informacijski viri so:

1. *Informacije* – informacijska sredstva: baze podatkov in datoteke, dokumentacija sistema, uporabniški priročniki, gradivo za usposabljanje, operativna navodila in podobno.

2. *Aplikacije* – sredstva programske opreme: uporabniške rešitve, temeljna programska oprema, razvojna orodja, podporni programi in podobno.

3. *IT infrastruktura* – fizična sredstva: računalniška in komunikacijska oprema, magnetni nosilci podatkov ter druga tehnična oprema (ključi, štampiljke, ...).

4. *Osebe* in ostala nematerialna sredstva: gesla, zaupne informacije, do katerih imajo dostop pooblaščene osebe za opravljanje poslovnih procesov, storitve računalniških obdelav, tehnične in komunikacijske storitve ter podobno.

1.2.3 Informacijska varnostna politika

Informacijska varnostna politika je strateški dokument organizacije, ki ga narekujejo poslovne potrebe organizacije. Vsi, ki zagotavljajo informacije, jih upravljajo in/ali obdelujejo, ga morajo v celoti upoštevati. Glavni namen informacijske varnostne politike je, da s preprečevanjem in zmanjševanjem učinkov varnostnih dogodkov ali incidentov omejimo poslovno škodo na najmanjšo možno mero ter vzpostavimo osnovna varnostna načela in izhodišča za zaščito informacij pred varnostnimi dogodki in incidenti. (ISO/IEC 27001:2005; Information technology - Security techniques - Information security management systems - Requirements; [12]). To storimo tako, da zagotavljamo razpoložljivost, celovitost in zaupnost informacij v pričakovanih okvirih.

Ker v organizacijah običajno že obstajajo utečeni postopki in modeli varovanja in iz njih izhajajoče politike, jih informacijska varnostna politika povzame in nadgradi. Bistvena sestavina vsake informacijske varnostne politike predstavlja učinkovito upravljanje tveganj. Na vsak način je informacijska varnostna politika predmet poslovanja in ne dokument, ki je uokvirjen s področjem IT, saj se ukvarja predvsem s tveganji pri doseganju poslovnih ciljev organizacije. V okviru modernejšega pristopa pa tudi z investicijami v informacijske vire.

1.2.4 Informacijski varnostni dogodek, incident in upravljanje neprekinjenega poslovanja

Informacijski varnostni dogodek Predstavlja identificiran pripetljaj v okviru računalniškega sistema, servisa ali mreže, ki kaže na to, da je bodisi kršena informacijska varnostna politika bodisi da gre za napako pri zaščiti informacijskega sistema, ali pa gre za neko neznano situacijo, ki se je pripetila v preteklosti in bi lahko imela vpliv na informacijsko varnost v bodoče.

V praksi se to manifestira kot odpoved delovanja ene ali več kritičnih poslovnih funkcij. V okviru plana neprekinjenega poslovanja običajno obstajajo predvideni postopki za odpravo prekinitve v predvidenem času. Poslovanje se običajno nadaljuje na isti lokaciji. Izvajati se začno predvideni postopki iz okrevalnega načrta – to so postopki za odpravo prekinitve.

Informacijski varnostni incident Predstavlja enega ali več (največkrat niz) nezaželenih ali nepričakovanih informacijskih varnostnih dogodkov, za katere velja, da bo njihov vpliv posledično zmanjšal ali celo onemogočil poslovne procese, aktivnosti ali opravila. Ti nezaželeni ali nepričakovani informacijski varnostni dogodki predstavljajo informacijsko varnostno grožnjo.

V praksi to pomeni odpoved delovanja ene ali več kritičnih poslovnih funkcij. V tem primeru gre za takšne odpovedi, da ne obstajajo predvideni postopki za odpravo prekinitve v predvidenem času. Poslovanje se lahko nadaljuje na isti lokaciji ali pa je potrebna delna ali popolna selitev na drugo lokacijo. Začnejo se izvajati postopki, predvideni v okrevalnem načrtu. V primeru nesreče se začne selitev dela sredstev in/ali ljudi, če je tako predvideno v planu neprekinjenega poslovanja.

Katastrofa Po informacijskem varnostnem incidentu, zagonu načrta za neprekinjeno poslovanje in po ostalih kriznih prijemih, se v organizaciji stanje lahko izboljša, ali pa gre za tako hude posledice incidenta, da organizacija ne preživi v približno obstoječi obliki ali pa sploh ne preživi. V slednjem primeru govorimo o katastrofi ali o incidentu s katastrofalnimi posledicami.

V praksi to predstavlja odpoved delovanja vseh kritičnih poslovnih funkcij na neki lokaciji. Za takšno stanje ne obstajajo predvideni postopki za odpravo prekinitve v predvidenem času. Poslovanje se dlje časa ne more nadaljevati na

isti lokaciji. Začne se reševanje ljudi in premoženja. Vzpostavitev delovanja ni predmet plana neprekinjenega poslovanja, temveč ostalih institucij in/ali javnosti.

V ameriški literaturi, ki se nekritično prevaja, se največkrat za katastrofalno stanje označuje že stanje incidenta.

Upravljanje neprekinjenega poslovanja Po standardu ISO 22301:2012 Societal security – Business continuity management systems — Requirements [11] gre pri upravljanju neprekinjenega poslovanja za holističen proces upravljanja, v katerem identificiramo:

- možne grožnje, s katerimi je organizacija soočena in
- vplive na poslovanje, ki so posledica realizacije groženj (samostojno ali v kombinaciji z ostalimi grožnjami).

Po drugi strani nam neprekinjeno poslovanje zagotavlja, da bodo ponovno vzpostavljeni za poslovanje bistveni procesi, aktivnosti in opravila, ki so bili okrnjeni ali povsem onemogočeni zaradi informacijskega varnostnega incidenta. Neprekinjeno poslovanje mora zagotavljati, da se ponovna vzpostavitev poslovnih procesov izvede na osnovi vnaprej definiranih prioritet in na osnovi vnaprej dorečene časovnice tako, da dosežemo normalno stanje vseh bistvenih elementov poslovanja.

Ključni element procesa neprekinjenega poslovanja je zagotovitev vseh potrebnih načrtov in ostalih, za vzpostavitev predvidenega obsega poslovanja potrebnih elementov. Tako načrte kot ostale potrebne elemente je potrebno testirati tako, da so pri tem vključeni vsi informacijski viri (informacije, aplikacije, infrastruktura in ljudje).

Za dosego vsega tega je potrebno vzpostaviti okvir, ki omogoča vzpostavitev sistema, ki napravi organizacijo odpornejšo na grožnje in na vplive realizacije teh groženj. To pomeni, da mora okvir zagotavljati učinkovit odziv, ki varuje interese posameznih deležnikov organizacije, njen ugled, blagovne znamke in izvajanje vseh aktivnosti, s katerimi organizacija pridobiva nove vrednosti. Poleg tega je pri upravljanju neprekinjenega poslovanja potrebno zagotavljati upravljanje okrevanja po incidentih. V to so vključeni tudi programi za treninge, vaje in preverjanje planov neprekinjenega poslovanja. Preveriti je potrebno izvedljivost

planov in jih sproti posodabljati na osnovi kritične analize izvedenih vaj in/ali incidentov v preteklosti.

Načrt neprekinjenega poslovanja je zbirka navodil in informacij, ki so bili razviti, zbrani in vzdrževani tako, da jih je mogoče uporabiti v primeru incidenta. Stopnja kompleksnosti samega plana in njegovega izvajanja v konkretnem primeru je sorazmerna z velikostjo in obsegom poslovanja organizacije. Kot takšen je predmet analize razmerja med stroški in koristmi organizacije.

Poglavje 2

Varnostno kopiranje

Eden najpogostejših varnostnih dogodkov, ki lahko ima, gledano z varnostnega vidika organizacije, celo katastrofalne posledice, je nezmožnost uporabe informacij. Največkrat je nezmožnost uporabe posledica informacijskega varnostnega dogodka ali incidenta, kot je odpovedi diska, namernega (kot posledica kriminalnega dejanja) ali nenamernega trajnega uničenja podatkov.

Najpreprostejša zaščita pred izgubo informacij je varnostno kopiranje (ang. "backup – back up"). Varnostno kopiranja uporabljamo pri zaščiti:

1. informacij in
2. programske opreme.

Oboje – informacije in programska oprema – so ključnega pomena pri zagotavljanju zahtevane razpoložljivosti in celovitosti informacij v primeru informacijskih varnostnih dogodkov ali incidentov. Pri varnostnem kopiranju tako informacije kot programsko opremo interpretiramo na enak način - oboje obravnavamo kot podatke.

Varnostno kopiranje uporabljamo zato, da imamo:

1. V primeru uničenja ali poškodovanja podatkov, rezervno kopijo. Izguba podatkov je namreč najpogostejša negativna izkušnja v IT.
2. Drug namen varnostnega kopiranja je povrnitev podatkovnega okolja v stanje, kot je bilo v nekem trenutku v zgodovini – torej pred nekim dolo-

čenim časom. Do kdaj v zgodovino se lahko vrnemo po želene podatke je določeno s tako imenovano politiko ohranjanja podatkov, ki je neposredno povezana s planom neprekinjenega poslovanja.

Varnostno kopiranje podatkov ima drugačen smisel in namen kot kopiranje podatkov za potrebe arhiviranja. Tehnologija in postopki so v veliki meri enaki ali podobni. Večkrat varnostno kopijo z dodatnimi postopki, jih predvideva predvsem organizacija dela in seveda zakonodaja, kategoriziramo kot arhivsko kopijo.

V primeru, da se original pokvari ali izgubi, lahko s pomočjo kopije restavriramo originalne podatke. Ta proces imenujemo restavracija ali vzpostavitev osnovnega stanja (ang. "restore"). Pri tem poznamo:

1. Restavracijo celotnega podatkovnega okolja in s tem celotnega računalniškega sistema v primeru informacijskega varnostnega incidenta. Pri tem želimo vzpostaviti stanje, ki je čim bolj podobno stanju tik pred informacijskim varnostnim incidentom. Doseganje tega cilja je še posebej pomembno v primeru računalniške podpore poslovnim procesom, za katere smo ugotovili, da potrebujejo plan neprekinjenega poslovanja.

2. Restavracijo manjšega števila datotek, ki so zbrisane, spremenjene ali poškodovane kot posledica informacijskega varnostnega incidenta ali zaradi siceršnje človeške napake.

Ker je za potrebe varnostnih kopij imeti eno ali več kopij podatkov v vsaj enem ali večih časovnih terminih, so zahteve v zvezi s shrambo podatkov osrednji izziv varnostnega kopiranja. Organizacija shrambe in njegovo upravljanje ter upravljanje samega procesa izdelave varnostnih kopij je zahtevno in zapleteno. Upoštevati je potrebno različne tipe naprav za shranjevanje podatkov, različne tipe geografske razpršenosti shramb, varnost podatkov in zmožnosti uporabe posameznih tehnologij in pristopov. Zelo pomembno je upoštevanje vseh omejitev – tudi zakonodajne – ki jih predpostavlja okolje in seveda človeški faktor in pričakovanja, ki jih subjektivno in objektovno postavljajo ljudje.

2.1 Informacije, ki jih upoštevamo ob vzpostavitvi in izvajanju varnostnega kopiranja

Nekatere pomembne informacije, ki so pogojene predvsem s tehniko in jih je potrebno upoštevati pri upravljanju procesa varnostnega kopiranja so:

1. Sklop informacij o podatkih, ki jih arhiviramo:
   (a) Naziv podatkov.
   (b) Lastnik in upravljavec(i) podatkov.
   (c) Pomembnost podatkov.
   (d) Velikost tolerirane podatkovne podatkovne luknje (koliko informacij lahko izgubimo).
   (e) Oblika podatkov, ki so predmet varnostne kopije (datoteka, slika diska („image“), boot sektor, blok podatkov, etc).
2. Sklop informacij o IT aktivnosti varnostnega kopiranja:
   (a) Lastnik in upravljavec(i) IT aktivnosti, ki izvaja varnostno kopiranje.
   (b) Perioda izdelave varnostnih kopij.
   (c) Število varnostnih kopij.
   (d) Čas hrambe varnostne kopije.
   (e) Obseg izdelave varnostne kopije (inkrementalni, popolni, etc).
   (f) Način izdelave varnostnih kopij (ročno, avtomatično, glede na nek dogodek, etc).
3. Sklop podatkov o orodjih, ki se uporabljajo pri varnostnem kopiranju:
   (a) Uporabljena strojna in programska oprema za izdelavo varnostnih kopij.
   (b) Lokacija orodja in uporabljene procedure, skripte in podobne informacije, ki so potrebne za uspešno uporabo orodja.
   (c) Uporabljeni standardi pri izdelavi varnostne kopije.
   (d) Uporabljeni algoritmi za kompresijo.

   (e) Uporabljeno algoritem določanja enolične označbe (po datumu in času, po zaporedni številki, etc).

4. Sklop podatkov o medijih, ki se uporabljajo pri varnostnem kopiranju:
   (a) Uporabljen medij za izdelavo varnostne kopije (disk, trak, CD, etc).
   (b) Lokacija(e) kjer se nahajajo mediji (varnostne kopije).
   (c) Kdo in na kakšen način ima dostop do medijev (varnostnih kopij).
   (d) Predpisani termini za delo z mediji (kdaj zamenjava, kdaj prepis, kdaj kopiranje in podobno).
5. Sklop podatkov o restavriranju podatkov:
   (a) Uporabljena strategija za restavracijo podatkov.
6. Revizijske sledi:
   (a) Naslov ali področje, kjer se nahajajo zapisi o vsakem posameznem izvajanju varnostnega kopiranja.
   (b) Podatki o lokaciji in načinu uporabe dnevnika, ki ga uporabljajo operaterji ob delu z mediji.

2.2 Shramba podatkov

Modeli podatkovnih shramb

V času, ko sistem ne deluje, kot posledica nekega varnostnega incidenta, lahko nastane vrzel pri procesiranju informacij. To vrzel imenujemo *podatkovna* ali *časovna luknja*. Primer: ob nekajurni prekinitvi delovanja računalnika, ki zajema podatke o številu vozil, ki so prepeljala prek nekega mostu, imamo opraviti s tako imenovano „podatkovno luknjo“ za čas, ko računalnik iz kakršnih koli vzrokov ni beležil prevozov. Predstavlja največji sprejemljivi čas ali največje število transakcij, katerih izgubo lahko toleriramo v primeru odpovedi delovanja sistema.

Pri načrtovanju izvajanja varnostnega kopiranja moramo poznati tolerirano podatkovno luknjo. V mnogih primerih sploh ne toleriramo podatkovne luknje. V tem primeru govorimo o nični podatkovni luknji. Takšni primerom smo običajno priča pri finančnih transakcijah - na primer dvigu gotovine na bankomatih, elektronskem nakazovanju in internem transakcijah v bankah.

Izvajanje varnostnega kopiranja je tudi eden od osnovnih pristopov pri neprekinjenem poslovanju. Običajno je del načrta neprekinjenega poslovanja.

Ker sistemi za varnostno kopiranje predvidevajo izdelavo vsaj ene kopije podatkov, ki jih želimo varovati, je treba računati na večje zahteve po dodatnih pomnilniških medijih.

Večkrat je pri varnostnih kopijah spregledana zaupnost. Varnostne kopije je potrebno glede zaupnosti varovati vsaj tako, kot je največja zahteva glede zaupnosti informacij, ki so predmet varnostne kopije.

Pri načrtovanju varnostnega kopiranja moramo upoštevati še časovno okno, v katerem se varnostno kopiranje izvaja v primeru, ko se predmet varnostnega kopiranja med samim kopiranjem spreminja.

Poleg podatkovne luknje moramo ob načrtovanju varnostnega kopiranja poznati več informacij o lastnostih tistega, kar je predmet varnostnega kopiranja. Ob vsakem posameznem izvajanju varnostnega kopiranja moramo beležiti:

1. Kaj vsebuje varnostna kopija (katere IT vire kopija vsebuje).
2. Točen čas začetka in konca izdelave kopije.
3. Enolično označbo kopije.
4. Zapis o uspešnosti ali neuspešnosti izdelave kopije.

Za nekatera varnostna kopiranja ni smiselno ali celo mogoče voditi vseh zgoraj navedenih evidenc. Ponavadi je za vodenje evidenc odgovoren lastnik aktivnosti varnostnega kopiranja.

Poleg tega je za potrebe verifikacije in validacije varnostnih kopij periodično (mesečno, vsake nekaj mesecev, letno, ...) izvesti popolno restavriranje naključno izbranega dela zadnje varnostne kopije. Ob verifikaciji in validaciji je potrebno napraviti zapisnik uspešnosti in se glede na uspešnost odločati o morebitnih spremembah in dopolnitvah IT procesa varnostnega kopiranja.

Poglavje 3

Računalniški vdori

V zadnjih letih je pomen informacijske varnosti pri poslovanju organizacij v izrednem porastu predvsem zaradi razširjenosti interneta. Z množično uporabo interneta se namreč informacijske varnostne grožnje vsakodnevno pojavljajo – največkrat v obliki vdorov v računalniške sisteme. Vdor v informacijski sistem organizacije lahko predstavlja samo bežen neljub dogodek, včasih pa nezgodo velikih razsežnosti, ki lahko povzroči krizno situacijo v organizaciji in navsezadnje celo pripelje do njene ukinitve.

Leta 2006 je na spletnih straneh mednarodne organizacije za standardizacijo ISO bil objavljen članek, v katerm piše: "Ocenjujemo, da mednarodni vdori v informacijske sisteme stanejo podjetja vsako leto okoli 15 milijard dolarjev in ta cena se strmo dviguje. Poleg tega gre pri vdorih še za škodo ugleda podjetij in njihovih blagovnih znamk, za kršitve in škodo pri intelektualni lastnini in avtorskih pravicah, za zaupanje kupcev in njihove lojalnosti in seveda na ceno delnic na borzah." [32]

Zaradi pereče problematike na tem področju so v okviru mednarodne organizacije za standardizacijo sprejeli standard ISO/IEC 18043:2006, Information technology – Security techniques – Selection, deployment and operations of intrusion detection system. Ta standard nudi okvir za pomoč pri detekciji vdorov v računalniške sisteme in neposredno dopolnjuje obstoječe in dobro poznane ISO/IEC 27001:2005 (glej podpoglavje "Varnostna politika"); Information technology – Security techniques – Information security management systems – Requirements

in ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management. Na ISO/IEC 18043:2006 se bodo sklicevali tudi nekateri novi standardi, predvsem standardi iz družine ISO/IEC 270xx.

Ted Humphreys, urednik skupine, ki je pripravila standard, pravi: "Eden od problemov, ki ga mnoga podjetja ne obvladujejo, je sposobnost detekcije vdora v njihov sistem. Le z detekcijo lahko začno izvajati učinkovite akcije za zaščito svojega premoženja". (Cel članek je na naslovu http://www.iso.org/iso/en/commcentre/pressreleases/2006/ref1017 .html).

Dandanes morajo organizacije poznati načine vdorov v njihova omrežja, sisteme ali aplikacije. Vedeti morajo, kakšna je njihova izpostavljenost in ranljivost, kako se zaščititi in sprejeti predvidena tveganja, da bo preprečevanje prihodnjih vdorov ustrezno in uspešno. To pomeni, da morajo v organizacijah znati razpoznati, kdaj in na kakšen način je prišlo do morebitnega vdora z ustreznim sprotnim analiziranjem strežnikov, mrežnega prometa in revizijskih sledi. Na osnovi analiz je mogoče razbrati specifične vzorce, ki so temelj za sum pojavljanja zlonamerne programske opreme. V te namene organizacije uporabljajo sisteme za detekcijo vdorov (SDV).

Če usposobljeni strokovnjaki dovolj poglobljeno in natančno izvajajo proces izbire, uvedbe in uporabe SDV, je mogoče pričakovati, da bo organizacija sistem izkoristila v največji možni meri. V tem primeru različni SDV omogočajo, da so informacije o vdoru na razpolago na ustrezen način in SDV tako postane pomemben člen v varovanju celotne informacijske in komunikacijske infrastrukture.

Znanje o vdorih je namenjeno predvsem odgovornim za IT, ki nameravajo vzpostaviti ali nadgraditi ustrezen SDV, da bo lahko deloval v kombinaciji z ostalimi SDV na nivoju posamezne organizacije ali med organizacijami. Dandanes je sodelovanje ali sočasno delovanje različnih SDV zaželeno in celo nujno, če želimo poskuse vdora učinkovito preprečevati. Standard, ki se ukvarja s problematiko vdorov, pa je pomemben tudi zato, ker njegova uporaba omogoča lažje sodelovanje med organizacijami.

3.1 Predstavitev sistema za detekcijo vdorov in njegove zmožnosti

SDV je pomemben element v mozaiku informacijske varnosti. To je orodje za upravljanje varnosti, ki ga uporabljamo za:

- napovedovanje in
- indentifikacijo vdorov

v računalniški sistem in za sprožitev ustreznega alarma med poskusom vdora.

Sistemi praviloma omogočajo še:

- lokalno zbiranje informacij o vdoru,
- konsolidacijo stanja po vdoru ter
- analize vzorcev običajnega obnašanja in uporabe informacijskega sistema.

Varnostni problemi, povzročeni z vdori, se največkrat izrazijo kot:

- neavtoriziran dostop do računalnikov,
- odpoved delovanja servisov ali
- splošno delovanje hekerjev.

Pri tem so za pojav vdora največkrat krivi:

- slaba konfiguracija sistemov,
- zanemarjanje in/ali slab nadzor nad uporabniki ter
- napake v programski opremi, uporabljenih protokolih in operacijskih sistemih, ki so posledice napačnega ali pomanjkljivega načrtovanja.

Te ranljivosti znajo uporabiti tako zunanji kot notranji uporabniki. Ko govorimo o notranjih uporabnikih, so pri tem mišljeni:

- samostojni in nepovezani uporabniki,
- povezani uporabniki, ki so udeleženci notranje "trgovine"uslug in poznanstev ter
- začasno zaposleni (pri nas gre največkrat za "študente").

3.2 Definicija sistema za detekcijo vdorov

Sistem za detekcijo vdorov (SDV) je informacijski sistem za identifikacijo:

- poskusa vdora,
- vdora, ki se izvaja, ali vdora, ki se je izvedel, in
- akcij, ki so se izvedle kot posledica vdora v širšem informacijskem sistemu ali na računalniški mreži.

Sistem za zaščito pred vdori je posebna nadgradnja sistema za detekcijo vdorov, ki je namenjena aktivnemu odzivu na zaznani vdor.

3.3 Pomen vdorov in sistemov za detekcijo in zaščito pred vdori za posamezno organizacijo

Za neko organizacijo je pri zaščiti pred vdori ključnega pomena, da zazna:

- ali je prišlo do vdora,
- kdaj je prišlo do vdora in
- kako je prišlo do vdora.

Vedeti mora, ali se je vdor izvršil prek:

- omrežja,
- sistema in/ali
- aplikacij.

Poleg tega si mora organizacija znati odgovoriti na naslednja vprašanja:

- Kolikšna in kakšna je izpostavljenost (ranljivost) organizacije?
- Kakšna je zaščita?
- Kako so tveganja obvladljiva (prenos tveganja, sprejemljivost tveganj, izogibanje tveganjem)?

Glede na naravo vdorov in težave, povezane z vdori, ter glede na zgoraj zapisano lahko zaključimo:

1. Organizacija se ščiti zato, da si zagotovi normalno poslovanje, ki izhaja iz njenega poslanstva.
2. Organizacija mora prepoznati vdore in mora se znati pred njimi zaščititi.
3. Organizacija v okviru splošnega poslovnega tveganja zagotavlja:
   (a) razpoložljivost,
   (b) celovitost in
   (c) zaupnost informacij.
4. Ob preverjanju smiselnosti dopolnitev in izboljšav organizacija upošteva oceno tveganja, stopnjo tveganja in stopnjo sprejemljivosti tveganja ter ocenjen denarni vložek za morebitno dopolnitev ali izboljšavo njene varnostne politike.

3.4 Namen in delovanje SDV

Sistem za detekcijo vdorov je namenjen pasivnemu opazovanju, detekciji in beleženju sumljivih, neustreznih, nenavadnih aktivnosti, ki kažejo na verjetnost vdora. V primeru zaznave takšnih aktivnosti SDV sproži ustrezne alarme.

Za aktivno pregledovanje zabeleženih zapisov o vdorih, izvajanje akcij kot odziv na alarmiranje in izvajanje študij izvajanj preteklih akcij v primeru vdorov mora biti v organizaciji odgovoren strokovnjak, zaposlen na področju informacijske varnosti.

3.5 Vrste SDV

Poznamo dve poglavitni vrsti SDV:

1. SDV, ki bazira na računalniku ali na računalniškem sistemu.
2. SDV, ki bazira na računalniški mreži.

Glede na različni vrsti SDV poznamo detekcijo vdora, ki opazuje in nadzira:

1. Računalnik (ali računalniški sistem) za izvor informacij o morebitnem vdoru in ki ga opazuje.

2. Promet na poljubnem segmentu računalniške mreže.

Največkrat uporabljamo kombinacijo obeh vrst SDV.

3.6 Generičen model sistema za detekcijo vdorov

SDV je sestavljen iz množice programskih in strojnih izdelkov, ki avtomatično opazujejo, zbirajo in analizirajo sumljive dogodke v informacijskem sistemu ali na mreži. Generičen model SDV je mogoče predstaviti kot množico spodnjih funkcionalnosti:

1. Izvor ali vir (šurovih") podatkov, ki so predmet pregleda s strani SDV.
2. Detekcija dogodkov.
3. Analiza dogodkov.
4. Shramba podatkov.
5. Odziv.

Navedene funkcionalnosti so realizirane v posameznih komponentah programskega paketa, ki so lahko del večjega programskega paketa, ali pa predstavljajo samostojen programski paket SDV.

3.6.1 Vir podatkov

Uspešnost delovanja SDV je v veliki meri odvisna od virov podatkov, iz katerih je mogoče pridobiti informacije o detektiranih poskusih vdorov. Standard predvideva naslednje podatkovne vire:

1. Revizijo različnih sistemskih zapisov in sporočil na različnih nivojih: od zelo abstraktnih do podrobnih pregledovanj kronološko urejenih zapisov o posameznih dogodkih v računalniškem sistemu.
2. Dodeljevanje sistemskih zmogljivosti s strani operacijskega sistema, ki vključuje množico različnih parametrov. Med njimi so zasedenost CPU, uporaba pomnilnika, pomanjkanje posameznih sistemskih zmogljivosti skozi daljša ali krajša časovna obdobja, promet prek V/I enot, število aktivnih mrežnih povezav in podobno.

3. Zapisi različnih orodij za upravljanje z mrežami. V teh zapisih so podatki o statusih na mreži in informacije o statusih prenosov.

4. Mrežni promet. Med temi informacijami so najpomembnejše informacije o izvorih in ponorih prometa na vseh mrežnih nivojih (ISO mrežni nivoji). Podatki o usmeritvah (routing) in posredovanju (proxy).

5. Ostali podatkovni viri, med katerimi so lahko na primer požarni zidovi (firewall) in seveda posebni agenti SDV, ki delujejo kot senzorji stanja na posameznih področjih računalniškega sistema.

V splošnem, tudi glede na vrsto SDV, je vir surovih podatkov računalnik ali računalniški sistem ali računalniška mreža.

3.6.2 Detekcija dogodkov

Detekcija dogodkov se uporablja v funkciji detekcije in pridobivanja za varnost relevantnih podatkov. Na osnovi opravljene analize podatkov lahko sklepamo o morebitnem varnostnem dogodku ali incidentu.

Detektirani dogodki so lahko preprosti posamični dogodki ali kombinacija posamičnih dogodkov, ki predstavljajo kompleksne dogodke. Na vsak način zaznava dogodkov ali sami podatki o teh dogodkih niso dovolj za detekcijo vdora. Potrebno je izvesti še vsaj analizo podatkov.

Detekcija dogodkov je največkrat realizirana s komponento monitoringa SDV tako, da je instalirana na mrežno napravo ali na specifičen računalnik ali računalniški sistem.

3.6.3 Analiza dogodkov

Osnovni namen SDV je analiza in procesiranje podatkov o detektiranih dogodkih na takšen način, da se pridobijo informacije o morebitnem poskusu vdora, ki se izvaja ali o že izvedenem vdoru.

Za potrebe analiziranja stanja se uporabljajo informacije iz zgoraj opisanih podatkovnih virov ter iz:

1. Podatkov, ki so rezultati predhodnih analiz in so del podatkovne baze SDV.

2. Informacij o tem, kako bi se moral obnašati sistem – tovrstni podatki predstavljajo bazo znanja o sistemu in njegovem obnašanju.

3. Informacij o tem, kako se nek sistem ne bi smel obnašati – tudi ti podatki so shranjeni v bazi znanja o sistemu in njegovem obnašanju.

4. Ostalih relevantnih informacij, ki predstavljajo morebitno informacijo o pričakovanem vdoru, o posameznikih ali lokacijah hekerjev in podobno.

Pri tem gre za dva splošna pristopa, ki jih SDV analizirajo:

1. Napačno uporabo nekega informacijskega vira.

2. Nenormalno obnašanje nekega informacijskega vira.

Fokus pri pristopu "napačne uporabe informacijskega vira"je v iskanju dokaza o vdoru med detektiranimi podatki o dogodkih, tako da se pri tem uporablja akumulirana baza znanja znanih napadov in o neavtoriziranih dostopih. Slaba stran tega pristopa je v tem, da vdora ni mogoče razpoznati, če ni razpoznan njegov "vzorec obnašanja"v obstoječi podatkovni bazi. Pri tem različni SDV uporabljajo znane tehnike kot so: analiza in primerjava sledi vdora, ekspertni sistem z vgrajenimi pravili in analize prehodov stanj v sistemu.

Pri analizi nenormalnega obnašanja nekega informacijskega vira skuša SDV najti neregularnosti pri obnašanju opazovanega dela sistema ali mreže in ga primerja s pričakovanim obnašanjem pri njegovem normalnem obratovanju. Profil normalnega pričakovanega obnašanja je del baze znanja SDV. Za analizo se uporabljajo poznane metode, kot so: identifikacija vzorcev nenavadnega obnašanja, ekspertni sistem z vgrajenimi pravili, statistične metode in nevronske mreže.

Sodobni SDV seveda različne metode medsebojno kombinirajo in analizirajo frekvenco vseh sumljivih dogodkov. Samih vdorov še posebej.

3.6.4 Podatkovna baza SDV

Podatkovna baza SDV je namenjena shranjevanju informacij, povezanih z varovanjem. Ti podatki so namenjeni analizam in izdelavi poročil.

V takšni bazi so shranjene informacije, kot so:

1. Detektirani dogodki in podatki, povezani s temi dogodki.

2. Rezultati analiz, detektiranih vdorov in ostalih sumljivih dogodkov, ki so uporabni za kasnejše analize v primeru sumljivih dogodkov.
3. Zbirka profilov poznanih vdorov in normalnega obnašanja.
4. Podrobni šurovi"podatki in zavarovane evidence (zapisi) v primeru, da je prišlo do alarmiranja.

3.6.5 Odziv

Namen funkcionalnosti odziva SDV je predstavitev odgovarjajočih rezultatov odgovornemu osebju (največkrat odgovorni dežurni osebi) v obliki alarma.

V primeru aktivnega odziva lahko SDV avtomatično kliče sistem za zaščito pred vdori, ki lahko začne takoj z izvajanjem nekaterih (ne vseh – večina je še vedno v domeni osebja) korektivnih ukrepov, kot so:

1. Re-konfiguracija sistema, v katerega je bil izvršen vdor.
2. Zaklepanje, odjava in zamrznitev računa (uporabniškega imena in področja), prek katerega se je vdor izvršil.
3. Ukinitev aplikacijske seje po predvidenem protokolu.

3.7 Opravila pri zaščiti pred vdori

Osnovni krog opravil, ki ga pri izvajanju zaščite pred vdori izvajamo, predstavlja:

1. Izbira strategije zaščite.
2. Implementacija strategije zaščite.
3. Izvajanje strategije zaščite.

3.7.1 Izbira strategij zaščite

Pri izbiri strategije zaščite upoštevamo naslednje dejavnike:

1. Ocena informacijskega varnostnega tveganja.
2. Izbira vrste SDV (na računalniku, na mreži, oboje).

3. Upoštevaje in ocena izbire glede na:
   (a) sistemsko okolje (operacijski sistemi, topologija mreže, ...);
   (b) obstoječe varnostne rešitve (DMZ, požarna pregrada, ...);
   (c) varnostna politika;
   (d) učinkovitost obstoječega informacijskega sistema in zahteve za učinkovitost SDV;
   (e) verificirane zmožnosti SDV;
   (f) ceno;
   (g) način osveževanj;
   (h) strategijo alarmiranja;
   (i) upravljanje z identitetami uporabnikov.
4. Implementacijo komplementaranih (dopolnjujočih) orodij in tehnik, med katerimi so:
   (a) preverjanje integritete datotek;
   (b) požarni zidovi in varnostna vrata;
   (c) medene vabe (honeypots);
   (d) orodja za upravljanje mrež;
   (e) orodja za upravljanje informacijske varnosti;
   (f) orodja za zaščito pred virusi;
   (g) orodja za oceno ogroženosti.
5. Zmožnost dopolnjevanja, dograjevanja in razširjanja (skalabilnost).
6. Tehnična podpora.
7. Usposabljanje in treningi.

3.7.2 Implementacija strategije zaščite

Vrsta vdora narekuje tudi naslednji vrsti implementacije strategije zaščite:

1. Izvedba na računalniški mreži. Zaščito na mreži umestimo za ali pred internetno požarno pregrado, na glavni hrbtenici notranje mreže ali na kritičnih notranjih delih interne mreže. Vsaka izmed lokacij ima svoje prednosti in slabosti, zato lokacije medsebojno kombiniramo.
2. Izvedba na računalnikih ali računalniškem sistemu

Obe izvedbi sta medsebojno dopolnjujoči in imata svoje prednosti in slabosti. Ustrezno zaščito največkrat dosežemo s kombinacijo zaščite na mreži in na računalnikih.

Posebno pozornost je potrebno posvetiti zaščiti podatkovno bazo SDV. Potrebno je zagotavljati njeno popolno integriteto, podatki morajo biti kriptirani, zagotovljeni morajo biti pravilni dostopi do baze in podobno. Z nepooblaščeno spremembo ali dostopom do podatkov SDV zmanjšamo ali celo popolnoma izničimo uspešno delovanje SDV.

3.7.3 Izvajanje strategije zaščite (obratovanje)

Opravila, ki jih opravljamo med izvajanjem ali obratovanjem sistema za detekcijo in zaščito pred vdori, so naslednja:

1. Izvajanje nastavitev SDV.
2. Ščitenje samega SDV pred informacijskimi varnostnimi grožnjami (predvsem zaščita podatkovne baze SDV).
3. Upravljanje alarmov SDV. V tem okviru moramo zagotoviti:
   (a) skupino za zaščito pred informacijskimi varnostnimi incidenti ali
   (b) imeti pogodbo z zunanjimi izvajalci s specialističnimi znanji.
4. Izvajati ustrezen odziv na incident. Odziv je lahko:
   (a) aktiven (akcije se avtomatično sprožajo kot odziv na alarm SDV) ali
   (b) pasiven (akcije so prepuščene osebi, ki se odloča na osnovi vrste alarma in obstoječih zabeležb).
5. Spremljanje in upoštevanje zakonodaje.

3.8 Izzivi, povezani s SDV

3.8.1 Koliko vlagati v SDV?

Z razvojem tehnologij se povečuje dostopnost do informacij, kar je dobro za organizacije, vendar se obenem povečujejo možnosti za vdore v njihove informacijske sisteme. Slednje je za organizacije neugodno. Vdori so postali običajni in njihovo število se iz meseca v mesec povečuje. Po drugi strani vemo, da vsega enostavno ni mogoče varovati, saj bi bili stroški previsoki. Podjetja varujejo svoje informacijske sisteme samo zaradi poslovnih motivov. Tudi nivo varovanja in s tem investirana sredstva narekujejo poslovni razlogi. Vprašanja, na katera si morajo podjetja znati odgovoriti, so:

1. Kakšen je želeni nivo celovitosti, zaupnosti in razpoložljivosti informacij?
2. Kolikšna je morebitna škoda, če zastavljenega nivoja ne dosega?
3. Kolikšno je sprejemljivo tveganje, ki še ne ogroža poslovanja?

Z drugimi besedami: organizacije morajo znati v okviru poslovnih in operativnih tveganj, poiskati tisto zdravo mejo kjer so vložki v varovanje informacijskih sistemov še smiselni. Če v varnost vlagajo preveč, po nepotrebnem izgubljajo sredstva, in če vlagajo premalo, je ogrožen njihov obstoj.

Pri odločanju, koliko vlagati v informacijsko varnost, podjetja izhajajo iz poslovnih tveganj, na osnovi katerih izdelajo operativna tveganja. Klasična formula za izračun tveganja je zmnožek verjetnosti za dogodek in ocenjena škoda v primeru dogodka. Pri ocenjevanju tveganj pa je potrebno biti posebno pozoren na tiste dogodke, ki v nobenem primeru niso sprejemljivi, četudi je verjetnost za dogodek prav majhna. Primer ocenjevanja tveganj je orkan Katrina. Odgovorni so bili mnenja, da se ne splača sprejeti posebnih (in dragih) varnostnih ukrepov, saj je verjetnost, da bi pot uničujočega orkana prečkala ravno veliko mesto New Orleans, izredno majhna. Tako je bil zmnožek verjetnosti z morebitno (visoko) ceno uničenja še vedno zelo majhen. V dogodku, ki je sledil, se je izkazalo, da je bila cena za neizvajanje posebnih varnostnih ukrepov nedopustno. Dejstvo, da ukrepov niso izvedli, se enostavno ne bi smelo zgoditi kljub ustrezno majhnemu zmnožku verjetnosti za dogodek s predvideno škodo.

Sistemi za detekcijo vdorov so tako samo del kolaža, ki ga tvori informacijska in siceršnja varnost podjetij. Tako se tudi podjetja o njihovi izbiri, implementaciji in izvajanju zaščite odločajo na osnovi ocene tveganj. V splošnem velja, da večji denarni vložki prinesejo kakovostnejšo zaščito in obratno.

3.8.2 Problem zasebnosti

Zasebnost pri uporabi SDV igra vse pomembnejšo vlogo, saj danes sistemi zbirajo in analizirajo navade uporabnikov in te podatke shranjujejo v svojih podatkovnih bazah. Pri tem gre za varovanje osebnih podatkov in problematiko, povezano z njimi. Še več, sisteme SDV je mogoče uporabiti za podroben nadzor posameznikov in njihovega obnašanja.

Že shranjevanje samega IP naslova je obdelava osebnega podatka. Informacijski pooblaščenec je podal naslednje mnenje: "IP številka je torej unikatna številka, s katero se vsak računalnik izkazuje v internet mreži kot naslov. V primerjavi z mobilno telefonijo je torej IP naslov to, kar pomeni telefonska številka za posameznika. Posameznika se da torej vsaj določljivo identificirati. V skladu z navedenim je torej IP naslov podatek, ki se nanaša na posameznika in tega sorazmerno enostavno določi. IP naslov je torej osebni podatek, ki se ga na podlagi 10. člena obdeluje zgolj, če obstaja zakonska podlaga ali osebna privolitev posameznika, v javnem sektorju pa zgolj, če obstaja za takšno ravnanje zakonska podlaga. Če takšne pravne podlage ni (z izjemo pogodbenega odnosa), je IP naslov varovani osebni podatek, katerega obdelava je prepovedana." [31]

Ker SDV shranjujejo več osebnih in občutljivih podatkov, standard predvideva upoštevanje naslednjih treh principov:

1. Detekcija vdorov naj služi samo zaščiti podatkov ali sistemov. To pomeni, da detekcija ne sme služiti kot instrument nadzora nad obnašanjem posameznikov.

2. Zbirka podatkov SDV mora biti uporabljena le za ustrezno (načrtovano) varovanje. S tem zagotavljamo, da se zbirajo in analizirajo le podatki, ki so nujno potrebni za zagotavljanje zaščite pred vdori. Tehnično to pomeni, da se podatki, ki so nastali na osnovi nekega dogodka zavržejo takoj, ko se primerjajo s "podpisom", ki ga za seboj pušča zlonamerna programska oprema; podatke ki so potrebni za nadzor nad vdori, pa moramo varno

shraniti. Ob tem moramo upoštevati, da je potrebno zagotoviti revizijske sledi za nadaljnje analize.

3. Politike, ki se nanašajo na zasebnost osebnih podatkov, je potrebno realizirati tudi v okviru SDV.

V tem času ni posebne zakonodaje, ki bi obravnavala problematiko detekcije vdorov.

3.8.3 Izzivi, povezani z izmenjavo podatkov o vdorih

Aktivna izmenjava podatkov o vdorih, izkušnjah in uporabi SDV je lahko velika prednost za vsa podjetja, ki so v takšno izmenjavo vključena. Tako je na primer zgodnje opozarjanje o možnostih vdora ali o novem tipu vdora za vsa podjetja dobrodošlo. Takšna opozorila so mogoča šele potem, ko se je neki nov tip "vdor-ažgodil in je bila izvedena analiza vdora. Tako podjetja po eni strani prispevajo podatke, po drugi strani pa so deležna opozoril in osveženih baz ali repozitorijev vzorcev, prek katerih je mogoče spoznati nove vdore.

Pri tem nastane vprašanje, koliko in kaj so podjetja pripravljena deliti s širšo skupnostjo. Ko podjetja delijo znanje, delijo tudi informacije o tem, ali so bila napadena ali ne, ali je bil vdor uspešen ali ne – iz informacij je mogoče razbrati notranjo organizacijo poslovanja in podobno. Tako gre po eni strani za za zelo občutljive informacije (na primer o banki), ki pa so za širšo skupnost dobrodošle, saj je mogoče na njihovi osnovi pripraviti boljšo zaščito za vnaprej. Tu se znova srečujemo s problemom anonimnosti pri posredovanju podatkov v skupno bazo znanja.

3.9 Učinkovitost

Pri ocenjevanju in izbiri SDV igra njihova učinkovitost osrednjo vlogo. Pri tem lahko merimo in ocenjujemo vsaj naslednje:

1. Točnost. Izvor netočnosti nastane v primeru, ko SDV identificira neko aktivnost kot vdor, pa čeprav ne gre za vdor (govorimo o pozitivni napaki). Po drugi strani lahko SDV vdora ne razpozna in ga identificira kot legalno

aktivnost (govorimo o negativni napaki). Količnik med posameznimi napakami glede na pravilno identificirane vdore je prvo merilo za točnost in dober parameter informacijske varnostne politike. Njegova nadgradnja je mogoča v smeri upoštevanja pomena posamezne napake.

2. Učinkovitost. Merimo jo kot razmerje porabljenih IT resursov s strani SDV pri pregledovanju posameznih dogodkov, procesiranju in uporabi lastne podatkovne baze glede na siceršnje zmogljivosti sistema. V primeru slabe učinkovitosti, je izvajanje SDV v realnem času vprašljivo. Podobno je pri mrežah, kjer SDV upočasnjujejo promet po mreži in povzročajo dodaten promet.

3. Popolnost. V primeru, da SDV ne zazna vdora, govorimo o nepopolnosti njegovega delovanja. Ta parameter je najtežje oceniti, saj je nemogoče vedeti, kakšni vdori vse so v nekem trenutku na svetu sploh mogoči.

4. Odpornost na napake. Sam SDV bi moral biti še posebno odporen na vdore in na grožnjo onemogočanja izvajanja storitve (DoS). Še posebej pereče je to zato, ker je večina sodobnih SDV izvedenih kot dodatek operacijskemu sistemu ali kakšnemu drugemu sistemskemu servisu, ki je predmet vdora ali druge informacijske grožnje.

5. Hitrost. Sam SDV mora čim hitreje izvesti vse potrebne analize in izvesti alarmiranje v primeru, da zazna vdor. Večkrat gre za sekunde, ko je potrebno zaščititi podatke, izvore podatkov ali sam SDV.

3.10 Osebje, odgovorno za implementacijo in obratovanje SDV

Izbira SDV je zelo zahtevno opravilo in mora upoštevati, kako se bo SDV lahko integriral v obstoječe IT podsisteme. Veliko funkcij SDV mora ostati takšnih, da jih lahko dobro usposobljeno osebje ročno upravlja. Osebje mora biti dobro podkovano na področju računalniških vdorov, informacijske varnosti (kamor je vključena tudi varnost omrežja) in organizacije IT v okolju, ki naj bi ga pokrival SDV.

Osebje mora, poleg uvedbe SDV, znati še:

- izvesti potrebne nastavitve SDV tako, da bo v nekem IT okolju mogoče zaznati morebitne vdore;
- hitro in pravilno interpretirati alarme, ki jih izvede SDV;
- izdelati politike in navodila za izvedbo odziva na realna opozorila s strani SDV;
- popraviti vso škodo, ki jo je povzročil vdor.

Vsa ta opravila in zadolžitve predstavljajo veliko več dela in zadolžitev, kot sama instalacija nekega SDV. So pa potrebna in morajo biti del celotnega procesa detekcije vdorov v nekem IT okolju.

Poglavje 4

Upravljanje informacijskih varnostnih incidentov

Popolne zaščite informacij, informacijskih sistemov, servisov in mrež ne zagotavlja nobena varnostna politika ali zaščita. Tudi po implementaciji predvidene zaščite še vedno ostajajo možnosti za informacijske varnostne incidente. Le ti pa direktno ali indirektno povzročajo poslovno škodo.

Vseskozi nastajajo tudi nove, še neodkrite možnosti za informacijske incidente. Nezadostna in ne dovolj kakovostna priprava na morebitne incidente lahko povzroči, da so odzivi nezadostni in ne odgovarjajo stopnji negativnega vpliva na poslovanje. Zato je za vsako organizacijo ključnega pomena, da ima strukturiran in planiran pristop k:

- detekciji, javljanju in ocenitvi informacijskih varnostnih incidentov;
- odgovarjajočemu odzivu na informacijske varnostne incidente, ki vključuje aktiviranje zaščite za preprečitev, zmanjšanje in ponovno vzpostavitev poslovanja v primeru vdora;
- učenju na osnovi preteklih informacijskih incidentov, ki omogočajo izboljšanje varnosti poslovanja.

ISO/IEC TR 18044:2004 [5] je tehnično poročilo, ki standardizira nekatere vidike upravljanja informacijskih incidentov. V nadaljevanju bodo predstavljene

ključne definicije, štirje procesi, ki jih predvideva tehnično poročilo ISO/IEC TR 18044:2004, opisani bodo nekateri ključni izzivi, s katerimi se srečujemo v primeru informacijskih incidentov in na koncu bo podana delna predloga poročila o incidentu s primerom ocenjevanja posameznih vplivov.

Reševanje situacije v primeru varnostnega incidenta rešuje posebna skupina – skupina za odziv na informacijski varnostni incident. V zgoraj omenjenem tehničnem poročilu in v nadaljevanju bo uporabljena kratica za to skupino ISIRT (Information Security Incident Response Team).

ISIRT je skupina ustrezno izkušenih in zaupanja vrednih oseb iz organizacije, ki upravlja z informacijskimi varnostnimi incidenti v času njihovega življenjskega cikla. Takšna skupina je v večini primerov virtualna in se po potrebi dopolnjuje z zunanjimi eksperti, njihovimi izkušnjami in znanjem.

4.1 Cilji in procesi, s katerimi dosegamo cilje

Ključni del informacijske varnostne strategije pri podjetjih je dobro strukturiran plan upravljanja z informacijskim incidenti. Poglavitni cilji takšne strategije so naslednji:

1. Informacijske varnostne dogodke je treba zaznati in jih učinkovito obdelati. Še posebej pomembna je hitra odločitev o tem, ali je nek informacijski varnostni dogodek tudi informacijski varnostni incident ali ne.

2. Informacijske varnostne dogodke je treba hitro oceniti in se učinkovito in na najbolj ustrezen način nanje odzvati.

3. Škodljive vplive informacijskih varnostnih incidentov na organizacijo in njene poslovne procese je treba minimizirati z ustreznimi zaščitami, ki so sestavni del odziva na incidente (po potrebi v skladu z ustreznimi načrti neprekinjenega poslovanja).

4. Poduk, ki ga lahko izluščimo iz vsakega posameznega informacijskega varnostnega incidenta in njegovega upravljanja, se mora čim hitreje odraziti v dopolnitvah obstoječe varnostne politike in varnostne prakse v neki organizaciji.

Po drugi strani pa z naslednjimi procesi:

1. Načrtovanje shem za upravljanje informacijskih varnostnih incidentov in izvedba priprav na incidente.
2. Uporaba pripravljenih shem za upravljanje informacijskih varnostnih incidentov.
3. Pregled in ocena preteklih dogodkov in ravnanj ob informacijskih varnostnih incidentih.
4. Korekture in izboljšave obstoječih načrtov in preteklih ravnanj ob informacijskih varnostnih incidentih (dosegamo v prejšnjem podpoglavju naštete cilje). Procesi so medsebojno odvisni in povezani.

4.2 Kratek opis procesov pri upravljanju z informacijskimi varnostnimi incidenti

Načrt in priprava

V okviru tega procesa je treba za potrebe učinkovitega in ustreznega odziva na informacijski varnostni incident izvesti naslednje aktivnosti:

1. Razviti in dokumentirati politiko upravljanja informacijskih varnostnih incidentov tako, da bo razvidno strinjanje z njeno vsebino s strani vseh ključnih deležnikov – še posebej najodgovornejših upravljavcev v organizaciji.
2. Razviti podrobno dokumentacijo o upravljanju informacijskih varnostnih incidentov na osnovi politike informacijskih varnostnih incidentov. Sem spadajo tudi: obrazci, procedure in posamezna potrebna orodja za detekcijo, poročanje, ocenjevanje in orodja za izvedbo odziva na incident, izdelana in dobro dokumentirana skala za ocenjevanje resnosti posledic incidenta in podobno.
3. Sprotno ažuriranje informacijske varnostne politike s pripadajočo politiko informacijskih varnostnih incidentov na vseh nivojih in pri vseh informacijskih sistemih, servisih in mrežah.
4. Vzpostavitev ustrezne organizacijske strukture za primere informacijskih varnostnih incidentov – ISIRT. V takšni strukturi morajo biti dobro definirane vloge in odgovornosti za vse mogoče tipe varnostnih incidentov.

V večini organizacij je ISIRT virtualna skupina, v kateri je tudi predstavnik vodstva in ostali strokovnjaki za posamezna (poslovna) področja ter seveda eksperti za posamezna področja računalništva, informatike, zlonamerne programske opreme in podobno.

5. Obveščati vse zaposlene o potencialni eksistenci nevarnosti za vdor, o zaščiti, o organizacijski shemi za ISIRT, prednostih, ki jih prinaša zaščita in o načinih poročanja v primeru informacijskega varnostnega dogodka. Poleg same obveščenosti morajo člani virtualne skupine opraviti tudi potrebne treninge, kjer se preizkusi delovanje organizacijske sheme ISIRT in njeno delovanje.

Uporaba

Pri procesu uporabe gre za izvajanje aktivnosti, ki so nujne v primeru informacijskega varnostnegadogodka ali incidenta. Aktivnosti so:

1. Detekcija in obveščanje o informacijskem varnostnem dogodku, ki ga izvede osebje, avtomatično nek sistem ali ga delno izvede osebje in delno avtomatično temu namenjen sistem.
2. Zbiranje informacij o informacijskem varnostnem dogodku in ocenjevanje dogodka za potrebe odločanja o tem, v katero kategorijo spada in ali gre za incident ali ne.
3. Izvajanje odgovarjajočih akcij v primeru incidenta, ki so:
   (a) takojšnje v realnem času ali skoraj v realnem času;
   (b) v primeru, da je incident pod kontrolo izvajanje potrebnih akcij za sanacijo stanja in vzpostavitev želenega stanja;
   (c) v primeru, da situacija ni pod kontrolo, začetek izvajanja kriznih aktivnosti po načrtu kriznega upravljanja (na primer izvajanje plana za neprekinjeno poslovanje);
   (d) izvajanje komunikacijskih aktivnosti o informacijskem varnostnem incidentu s predvidenimi javnostmi v skladu s komunikacijskim planom;
   (e) izvajanje forenzične analize;

(f) ustrezno zaznamovanje (logiranje) vseh ukrepov in odločitev, ki jih uporabimo v kasnejših analizah;

(g) zaključevanje akcij v zvezi z incidentom s posebnim dokumentom (ugotovitveni dokument).

Pregled

Ko je informacijski varnostni incident zaključen, je treba izvesti naslednje aktivnosti:

1. Voditi in spremljati potrebne forenzične analize.
2. Identificirati lekcijo, ki nam bo v pomoč v prihodnjih podobnih primerih.
3. Identificirati izboljšave pri implementaciji informacijske varnosti, ki so nastale na osnovi pridobljene lekcije ob preteklih incidentih.
4. Identificirati izboljšave pri organizaciji sheme za upravljanje v primeru informacijskih varnostnih incidentov.

Izboljšave

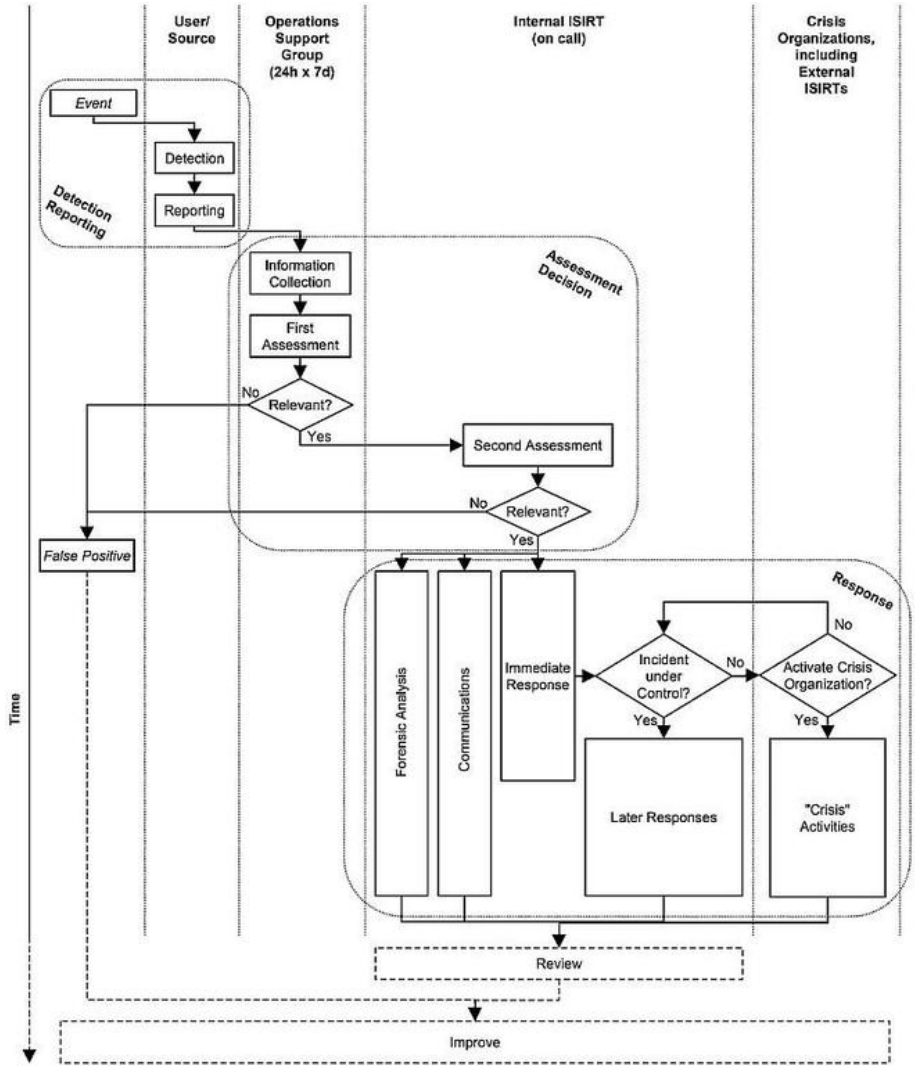
Poudarek mora biti na iteraktivnosti procesov informacijskih varnostnih incidentov z neprestanim dograjevanjem (izboljševanjem) posameznih informacijskih varnostnih elementov skozi čas. Izboljšave morajo nastati na osnovi pregledov podatkov o incidentih in morajo biti potrjene s strani ekspertov za posamezna področja.

Slika 4.1 prikazuje časovni diagram upravljanja z incidentom, v katerem so predstavljeni vsi štirje zgoraj opisani procesi in glavne aktivnosti.

4.3 Prednosti načrtovanja upravljanje informacijskih varnostnih incidentov

Pomembnejše prednosti so:

1. Izboljšanje splošne informacijske varnosti.



Slika 4.1: Časovni diagram izvajanja procesov upravljanja informacijskega varnostnega dogodka [5]

2. Zmanjšanje škodljivega vpliva na poslovanje, ki se odraža skozi prekinitve, finančne izgube in podobno in ki nastane kot posledica informacijskih varnostnih incidentov.

3. Izboljšan vpogled in pregled nad informacijskimi varnostnimi incidenti.

4. Izboljšane prioritete in evidence. S postavljenimi prioritetami se izognemo ukrepom na osnovi posameznih partikularnih interesov in trenutnega razmerja moči v organizaciji, medtem ko se z urejenimi evidencami izognemo zapletom, ki lahko sledijo po normalizaciji stanja – še posebej če smo po zakonodaji odgovorni sestavljati poročila o incidentih ali če sledijo obvezne revizije in siceršnji pregledi predvideni s strani zakonodaje.

5. Proračun in viri ter pripomočki. Z dobro strukturiranim pristopom pri informacijskih varnostnih incidentih je mogoče enostavneje in uspešneje upravičevati potrebe po proračunskih in ostalih sredstvih. Prav tako je vzorčenje in poročanje, ki podaja sliko stanja in uspešnosti pri preprečevanju incidentov (in posledično potrebe po denarju in ostalih virih), mogoče le z omenjenim dobro strukturiranim pristopom.

4.4 Ključni izzivi upravljanja informacijskih varnostnih incidentov

Odzivi o načinu upravljanja informacijskih varnostnih incidentov predstavljajo vodilo organizacijam, da se lahko osredotočijo na realna tveganja, ki izhajajo iz njihovih IT sistemov, servisov in mrež. Na ta način je mogoče veliko uspešneje, ob zagotovljenem denarju in ostalih resursih, zagotavljati zahtevano varnost, kot je to v primeru "ad hoc"pristopa. Rezultati so boljši in zaupanje v sitem varovanja se poveča. Tako vodstvo, zaposleni in ostale javnosti potrebujejo zaupanje v pravočasnost opozoril in alarmov, v njihovo relevantnost, točnost, natančnost in celovitost.

Tako je za kakovostno shemo informacijskih varnostnih incidentov treba vzpostaviti okolje, ki vključuje predvsem:

1. Strinjanje, podporo in zavezanost poslovodstva, ki omogoča strukturirano shemo za upravljanje z informacijskimi varnostnimi incidenti. Glavno

orodje pri tem so komunikacijske strategije.

2. Zavedanje vseh uporabnikov IT, da je njihovo sodelovanje pri izvajanju zaščite nujno. Zavedati se morajo, da so del organizacije in da so del varnostne sheme. Poznati morajo prednosti in koristi, ki jih nudi varnostna shema ter svojo vlogo in zadolžitve v okviru te sheme. Poznati morajo tudi osnove strategije za izvajanje sheme. Glavno orodje za doseganje potrebnega zavedanja so komunikacijske strategije

3. Pri doseganju pravnih in zakonodajnih zahtev je treba upoštevati:

   (a) zahtevano zaščito osebnih podatkov;

   (b) ustrezno vzdrževanje zapisov, ki so povezani z informacijskimi varnostnimi incidenti;

   (c) zaščito zapisov in informacij, ki izhajajo iz pogodbenih odnosov;

   (d) usklajenost politik in procedur s splošnimi pravnimi predpisi;

   (e) pregled pravne veljavnosti vseh izjem pri garancijah ("disclaimers");

   (f) pogodbe z zunanjimi izvajalci je treba preveriti z vseh vidikov;

   (g) treba je stalno preverjati, ali obstajajo vse potrebne izjave zaposlenih, ki se nanašajo na IT varovanje in preveriti, ali so vsi zaposleni takšne izjave podpisali (glede na dostop do posameznih IT virov);

   (h) zagotavljanje zakonodajnih zahtev glede dokumentiranja in upravljanja v primeru incidentov;

   (i) vsi vidiki vseh obveznosti morajo biti povsem nedvoumni (obveznosti do: ostalih organizacij, ažuriranje baze nezaželene programske opreme, poročanje o vdoru izbranemu ponudniku programske opreme, poročanje ostalim, zainteresiranim javnostim in podobno);

   (j) preučiti je treba specifične pravne zahteve;

   (k) zagotoviti je treba izvajanje vseh procedur za prijavo in preiskavo v zvezi z organi pregona;

   (l) zagotoviti je treba, da so vse vrste monitoringa usklajene s pravnimi predpisi;

(m) zagotoviti je treba izvajanje vseh politik pri izvajanju komuniciranja v primeru incidenta.

4. Učinkovito obratovanje (izvajanje) in zagotavljanje kakovosti s strukturiranim pristopom, ki zagotavlja zavezanost k zaznavanju incidentov, kakovosti obveščanja, dogovorjeni (in enostavni) uporabi, hitrosti ter učenju.
5. Anonimnost in zaupnost, ki sta dogovorjeni in dokumentirani z možnostjo preverjanja.
6. Kredibilnost v okolju, kjer se izvaja detekcija vdorov.
7. Zagotovljena je kompatibilnost s siceršnjo informacijsko varnostno politiko, kar zagotavljamo z ustrezno tipologijo.

4.5 Elementi poročila o informacijskem varnostnem incidentu

Datum

Šifra

Poslovni proces :: Podatki o kontaktni osebi

1. Ime
2. Naslov
3. Telefon
4. E-pošta

Skupina za odziv na informacijski varnostni incident :: Podatki o kontaktni osebi

1. Ime
2. Naslov
3. Telefon
4. E-pošta

Opis informacijskega varnostnega incidenta

1. Kaj se je zgodilo?
2. Kako se je zgodilo?
3. Zakaj se je zgodilo?
4. Kateri IT viri so bili prizadeti?
5. Poslovna škoda in negativni vplivi na poslovanje
6. Identificirane ranljivosti

Podrobni opisi informacijskega varnostnega incidenta

1. Datum in čas incidenta
2. Datum in čas, ko je bil incident odkrit
3. Datum in čas obvestila o incidentu
4. Je incident končan (Da/Ne)
5. Koliko časa je trajal (če je zgoraj DA) ali koliko časa že traja (če je zgoraj NE)

Tip informacijskega incidenta: Realizacija (izberi in obkroži)

1. Dejanski
2. Poskus
3. Sum na incident

Tip informacijskega incidenta: Način (izberi in obkroži)

1. Premišljen
   (a) Kraja
   (b) Prevara
   (c) Sabotaža ali fizična škoda
   (d) Zlonamerna koda

   (e) Hekanje ali infiltracija
   (f) Napačna uporaba IT virov
   (g) Ostalo
2. Nesreča
   (a) Napaka na strojni opremi
   (b) Napaka pri programski opremi
   (c) Napaka pri komunikacijski opremi
   (d) Ogenj
   (e) Poplava
   (f) Ostale naravne nesreče
   (g) Izguba kritičnih servisov
   (h) Primanjkljaj osebja
   (i) Ostalo
3. Napaka
   (a) Napaka pri obratovanju
   (b) Napaka pri vzdrževanju strojne opreme
   (c) Napaka pri vzdrževanju programske opreme
   (d) Uporabniška napaka
   (e) Napaka v dizajnu
   (f) Ostalo
4. Neznano

Prizadetost IT virov

1. Informacije ali podatki
2. Strojna oprema
3. Programska oprema
4. Komunikacijska oprema
5. Dokumentacija

	Stopnja (1-10)	Vrednost (€)
Finančna izguba ali prekinitev poslovanja		
Komercialni in ekonomski pomen		
Osebni podatki		
Zakonske in pravne obveznosti		
Opravila vodenja in poslovanja		
Izguba premoženja		

Tabela 4.1: Ocenjevanje poslovne škode v primeru informacijskega varnostnega incidenta

Poslovna škoda in identificirani negativni vplivi na poslovanje

Pri ocenjevanju poslovne škode je treba identificirati negativne vplive na naslednje elemente varnostne politike:

1. Zaupnost.
2. Integriteta.
3. Razpoložljivost.
4. Ugled.
5. Uničenje.

Za vsakega izmed elementov varnostne politike je treba izpolniti tabelo 4.1:

Konec incidenta

1. Začetek preiskave
2. Osebe, vključene v preiskavo
3. Datum zaključka incidenta
4. Datum zaključka vpliva, ki ga je imel incident
5. Datum zaključka preiskave o incidentu
6. Reference o preiskovalnih poročilih

Osebe, ki so bile vključene v izvedbo incidenta

1. Posamezniki (naštej)
2. Organizirane skupine (naštej)
3. Legalne ustanovljene organizacije ali inštitucije (naštej)
4. Nesreča
5. Brez krivcev (naravna nesreča, človeška napaka, etc)

Opis krivcev

Dejanski in predvideni motivi

1. Kriminalni in/ali motiv okoriščanja
2. Politični
3. Zabava in/ali hekanje
4. Maščevanje
5. Ostalo

Akcije, ki so bile izvedene za razrešitev incidenta

1. Brez
2. V ožji organizaciji (naštej)
3. V širši organizaciji (naštej)
4. Zunanja (povej s kom, kako, etc)

Akcije, ki so predvidene za razrešitev incidenta

1. Brez
2. V ožji organizaciji (naštej)
3. V širši organizaciji (naštej)
4. Zunanja (povej s kom, kako, etc)

Akcije, ki se izvajajo za razrešitev incidenta

1. Brez
2. V ožji organizaciji (naštej)
3. V širši organizaciji (naštej)
4. Zunanja (povej s kom, kako, etc)

Zaključek

1. Manjši vpliv in razlaga
2. Večji vpliv in razlaga

Obveščeni posamezniki

1. Vodja informacijske varnosti
2. Vodja skupine za odziv na informacijski varnostni incident
3. Vodja organizacijske enote, kjer se izvaja poslovni proces, na katerega je vplival incident (naštej)
4. Oseba odgovorna za izvajanje poslovnega procesa, na katerega je vplival incident (naštej)
5. Vodja IT informacijske enote
6. Oseba, ki je prijavila incident
7. Vodja osebe, ki je prijavila incident
8. Policija
9. Ostali (naštej)

Vključeni posamezniki

1. Avtor tega poročila (podpis, datum)
2. Pregledal 1 (podpis, datum, vloga)
3. Pregledal 1 (podpis, datum, vloga)
4. Etc

4.6 Nekateri primeri določanja stopenj negativnih vplivov na poslovanje

Finančna izguba ali prekinitev poslovanja

Stopnje:

1. Finančna izguba/stroški velikosti x1 ali manj
2. Finančna izguba/stroški velikosti med x1 +1 in x2
3. Finančna izguba/stroški velikosti med x2 +1 in x3
4. Finančna izguba/stroški velikosti med x3 +1 in x4
5. Finančna izguba/stroški velikosti med x4 +1 in x5
6. Finančna izguba/stroški velikosti med x5 +1 in x6
7. Finančna izguba/stroški velikosti med x6 +1 in x7
8. Finančna izguba/stroški velikosti med x7 +1 in x8
9. Finančna izguba/stroški velikosti x8 ali več
10. Organizacija ne preživi finančne izgube ali stroškov

Komercialni in ekonomski pomen

Stopnje:

1. Konkurenca je pridobila, vendar sami nismo utrpeli komercialne škode
2. Konkurenca je na naš račun pridobila y1 prometa ali manj
3. etc

Osebni podatki

Stopnje:

1. Manjši problemi s posamezniki (jeza, nestrinjanje, frustracije), vendar do kršitve predpisov ali zakonodaje ni prišlo.
2. Problemi s posamezniki (jeza, nestrinjanje, frustracije), vendar do kršitve predpisov ali zakonodaje ni prišlo.

3. Kršitev predpisov, zakonodaje ali etičnih zahtev ali namen publiciranja zaščitenih informacij, ki bi lahko škodovale posamezniku v manjši meri.
4. Kršitev predpisov, zakonodaje ali etičnih zahtev ali namen publiciranja zaščitenih informacij, ki mečejo slabo luč na posameznika ali skupini posameznikov.
5. Kršitev predpisov, zakonodaje ali etičnih zahtev ali namen publiciranja zaščitenih informacij, ki resno škodujejo posamezniku.
6. Kršitev predpisov, zakonodaje ali etičnih zahtev ali namen publiciranja zaščitenih informacij, ki resno škodujejo posamezniku ali skupini posameznikov.
7. Ni vrednosti.
8. Ni vrednosti.
9. Ni vrednosti.
10. Ni vrednosti.

Zakonske in pravne obveznosti

Stopnje:

1. Ni vrednosti.
2. Ni vrednosti.
3. Uveljavljanje opozorila, civilne tožbe ali kriminalnega postopka, ki ima za posledico finančno škodo/kazen v višini z1 ali manj.
4. Uveljavljanje opozorila, civilne tožbe ali kriminalnega postopka, ki ima za posledico finančno škodo/kazen v višini med z1 +1 in z2.
5. Uveljavljanje opozorila, civilne tožbe ali kriminalnega postopka, ki ima za posledico finančno škodo/kazen v višini med z2 +1 in z3 ali zaporno kazen manjšo od dveh let.
6. Uveljavljanje opozorila, civilne tožbe ali kriminalnega postopka, ki ima za posledico finančno škodo/kazen v višini med z3 +1 in z4 ali zaporno kazen večjo od dveh let in manjšo od deset let.

7. Uveljavljanje opozorila, civilne tožbe ali kriminalnega postopka, ki ima za posledico navzgor neomejeno finančno škodo/kazen ali zaporno kazen večjo od deset let.
8. Ni vrednosti.
9. Ni vrednosti.
10. Ni vrednosti.

Poglavje 5

Standardi

Po ocenah strokovnjakov kar 95 odstotkov svetovnega gospodarstva predstavljajo majhna in srednje velika podjetja. Njihova gospodarska moč in vpliv sta manjša od njihovega deleža zaradi njihove razdrobljenosti, vendar se s časom, predvsem s pomočjo različnih vrst standardizacije, njihov vpliv veča. Standardizacija namreč omogoča, da se v svetovne globalne verige za preskrbo z dobrinami, vključujejo tudi manjša podjetja. Eden izmed primerov standardizacije je ravno uporaba telekomunikacijskih storitev z internetom na čelu, prek katerega se majhni sistemi kosajo z velikimi precej bolj enakopravno, kot je to bilo v preteklosti. Standardizirana podpora digitaliziranim vsebinam, procesom kontrole kvalitete in finančnih transakcij je velikim podjetjem odvzela monopole. Zadnji primer je standard, ki standardizira zapis dokumentov ISO/IEC 26300; Open Document Format for Office Applications (OpenDocument) v1.0. Temu standardu se je navsezadnje uklonil tudi Microsoft (najverjetneje zaradi novega vodstva) in tako omogočil ostalim ponudnikom programske opreme za pisarniško poslovanje bolj enakopravno nastopanje na tržišču.

Standardi organizacije ISO so bili in so še pri standardizaciji vodilni v svetovnem merilu. S svojimi praktičnimi rešitvami in neodvisnostjo od tehničnega, gospodarskega in političnega okolja podajajo praktične rešitve – predvsem majhnim podjetjem, ki si ne morejo privoščiti velikih razvojnih vlaganj.

V mesecu avgustu leta 2006 smo se spominjali stoletnice začetka mednarodne standardizacije z ustanovitvijo International Electrotechnical Commission

(IEC), ki je delovala na področju elektrotehnike. Leta 1926, dvajset let za ustanovitvijo mednarodne standardizacije, se je začelo pionirsko delo standardizacije še na ostalih področjih v okviru National Standardizing Associations (ISA), ki je delovala predvsem na področju strojništva. Leta 1946 so se delegati iz 25 držav v Londonu odločili, da ustanovijo mednarodno organizacijo s ciljem "pospeševanja mednarodne koordinacije in združevanja industrijskih standardov". Tedaj je bila rojena organizacija ISO, ki je uradno začela svoje delovanje 23. februarja 1947, in je do danes objavila več kot 15.000 mednarodnih standardov.

ISO deluje tudi (na osnovi mednarodnega političnega konsenza) skupaj z že omenjeno IEC in z ITU (International Telecommunication Union) v okviru WTO (World Trade Organization). S tem prispeva k cilju WTO, ki je promocija proste in pravične svetovne trgovine in naj bi omogočil rast svetovne trgovine.

ISO standardi se razvijajo v okviru tehničnih odborov. Eden izmed njih je odbor z imenom *Information Technology* in z oznako JTC 1, v okviru katerega delujejo pododbori, ki so navedeni v spodnji tabeli – tabeli 21.

Za industrijo IT sta še posebej zanimiva

- pododbor za programsko opremo in sistemski inženiring z oznako SC 7 zaradi svojega širokega vpliva na industrijo IT in
- pododbor za področje varnosti z oznako SC 27.

Spiska standardov iz obeh pododborov, ki so že sprejeti in tistih, ki so še v razvoju sta na naslovih:

1. http://www.iso.ch/iso/en/CatalogueListPage.CatalogueList?COMMID=40&-scopelist=ALL in
2. http://www.iso.ch/iso/en/CatalogueListPage.CatalogueList?COMMID=143&-scopelist=ALL

Primera dveh standardov iz pododbora SC 27 sta:

1. Na novo objavljeni standard ISO/IEC 18043:2006, Information technology – Security techniques – Selection, deployment and operations of intrusion detection system), ki je v pomoč pri detekciji vdorov v računalniške sisteme.
2. ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management, ki je na petem mestu najbolj uporabljanih ISO standardov.

Oznaka	Pododbor
JTC 1SC 2	Coded character sets
JTC 1/SC 6	Telecommunications and information exchange between systems
JTC 1/SC 7	Software and system engineering
JTC 1/SC 17	Cards and personal identification
JTC 1/SC 22	Programming languages, their environments and system software interfaces
JTC 1/SC 23	Digital storage media for information interchange
JTC 1/SC 24	Computer graphics, image processing and environmental data representation
JTC 1/SC 25	Interconnection of information technology equipment
JTC 1/SC 27	IT Security techniques
JTC 1/SC 28	Office equipment
JTC 1/SC 29	Coding of audio, picture, multimedia and hypermedia information
JTC 1/SC 31	Automatic identification and data capture techniques
JTC 1/SC 32	Data management and interchange
JTC 1/SC 34	Document description and processing languages
JTC 1/SC 35	User interfaces
JTC 1/SC 36	Information technology for learning, education and training
JTC 1/SC 37	Biometrics

Tabela 5.1: Pododbori odbora Informacijska tehnologija JTC1

Vsak standard se sprejema po vnaprej načrtovanem postopku in vsak standard ima označbo stanja, v katerem se trenutno nahaja. Spodnja tabela (tabela 5.3) prikazuje vsa stanja, v katerih se lahko nek standard nahaja. Iz stanj je mogoče razbrati njegov življenjski cikel, postopek njegovega sprejemanja in dopolnjevanja. Ko govorimo o standardih, je pomembno, da vzamemo v obzir poleg njegove siceršnje označbe (številka in letnica) tudi njegovo označbo stanja. Postopek sprejemanja in ukinjanja standardov je uporaben tudi za sprejemanje dokumentov v drugih primerih in okoljih – na primer pri sprejemanju ISMS dokumentacije.

V nadaljevanju poglavja bodo podrobneje opisani naslednji temeljni standardi iz pododbora 7 (Software and system engineering):

1. ISO/IEC 12207:1995; Information technology – Software life cycle processes z amadmajem ISO/IEC 12207:1995/Amd 1:2002 in ISO/IEC 12207:1995/Amd 2:2004.

2. ISO/IEC 90003:2004; Software engineering – Guidelines for the application of ISO 9001:2000 to computer software.

3. ISO/IEC 25000:2005; Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE.

4. ISO/IEC 25051:2006; Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing.

5. ISO/IEC 25062:2006; Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Common Industry Format (CIF) for usability test reports.

in iz pododbora 27 (IT Security techniques):

1. ISO/IEC 27001:2005; Information technology – Security techniques – Information security management systems – Requirements Pri standardu ISO/IEC 27001:2005 gre za standard iz okvira standardov

STAGE	SUB-STAGE						
	00	20	60	90 Decision			
	Registration	Start of main action	Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary stage	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Review summary circulated			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal stage	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Voting summary circulated	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 Preparatory stage	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Comments summary circulated			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee stage	30.00 Committee draft (CD) registered	30.20 CD study/ ballot initiated	30.60 Comments/ voting summary circulated	30.92 CD referred back to Working Group		30.98 Project deleted	30.99 CD approved for registration as DIS
40 Enquiry stage	40.00 DIS registered	40.20 DIS ballot initiated: 5 months	40.60 Voting summary dispatched	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project deleted	40.99 Full report circulated: DIS approved for registration as FDIS

Tabela 5.2: Stanja in življenjski cikel ISO standardov - 1. del

STAGE	SUB-STAGE						
	00	20	60	90 Decision			
	Registration	Start of main action	Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
50 Approval stage	50.00 FDIS registered for formal approval	50.20 FDIS ballot initiated: 2 months. Proof sent to secretariat	50.60 Voting summary dispatched. Proof returned by secretariat	50.92 FDIS referred back to TC or SC		50.98 Project deleted	50.99 FDIS approved for publication
60 Publication stage	60.00 International Standard under publication		60.60 International Standard published				
90 Review stage		90.20 International Standard under periodical review	90.60 Review summary dispatched	90.92 International Standard to be revised	90.93 International Standard confirmed		90.99 Withdrawal of International Standard proposed by TC or SC
95 Withdrawal stage		95.20 Withdrawal ballot initiated	95.60 Voting summary dispatched	95.92 Decision not to withdraw International Standard			95.99 Withdrawal of International Standard

Tabela 5.3: Stanja in življenjski cikel ISO standardov - 2. del

ISO/IEC 2700x, ki so v tem trenutku (avgust 2006) še v fazi usklajevanja in sprejemanja. V okvir 2700x bodo sodili še naslednji standardi: 1. ISO/IEC NP 27000; Information technology – Information security management – fundamentals and vocabulary; stanje 10.99.

2. ISO/IEC NP 27004; Information technology – Information security management measurements;stanje 10.99.

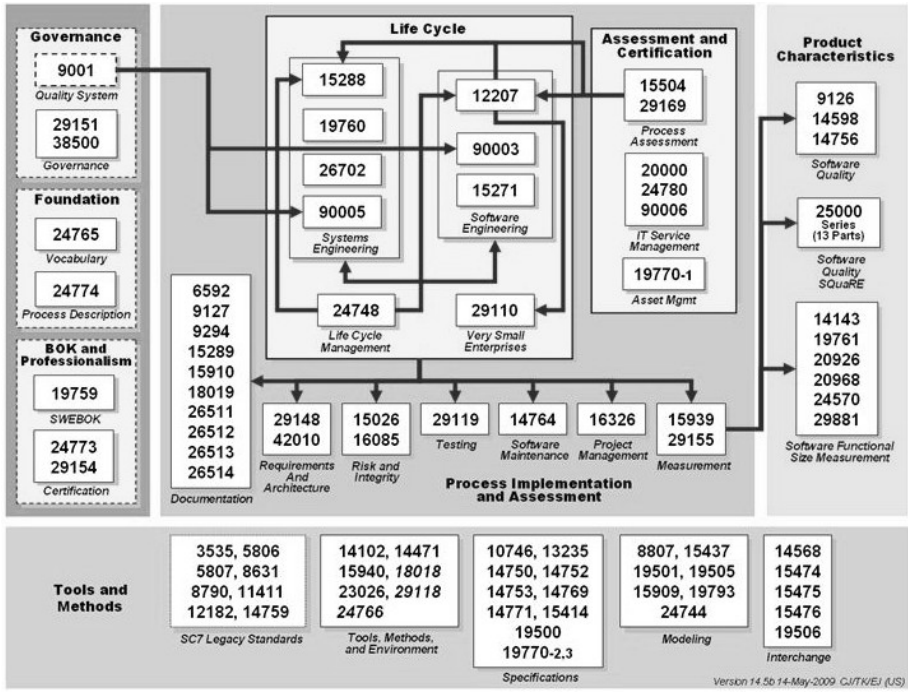
3. ISO/IEC CD 27005; Information technology – Information security risk management; stanje 30.20.

4. ISO/IEC FCD 27006; Information technology – Security techniques – Requirements for the accreditation of bodies providing certification of information security management systems; stanje 40.20.

5.1 Programska oprema in sistemski inženiring (JTC 1/SC 7 Software and system engineering)

Slika **??** prikazuje relacije med posameznimi standardi pododbora SC7. Iz te slike je razvidna osrednja vloga standarda 12207 (15271 je tehnično poročilo, ki razlaga kako uporabljati 12207) in 90003.

V prihodnje v pododboru načrtujejo delo na poenotenju standardov tako, da bodo temeljili na poenotenih procesih. Najprej je predvsem potrebno poenotiti procese med 12207 in 15288, zato sta že odprta projekta za revizijo obeh standardov (trenutno sta v fazi 10.99). Glede na ostale nove standarde in predvsem na standard 90003 je mogoče zaključiti, da je temeljni opis procesov v 12207.



Slika 5.1: Okvir standardov pododbora *Programska oprema in sistemski inženiring* [24]

5.1.1 Standard ISO/IEC 12207:1995 z amandmaji

Namen

ISO/IEC 12207 [14] vzpostavlja vzpostavitev okvira, v katerem povezujemo procese, ki jih določajo specifičnosti:

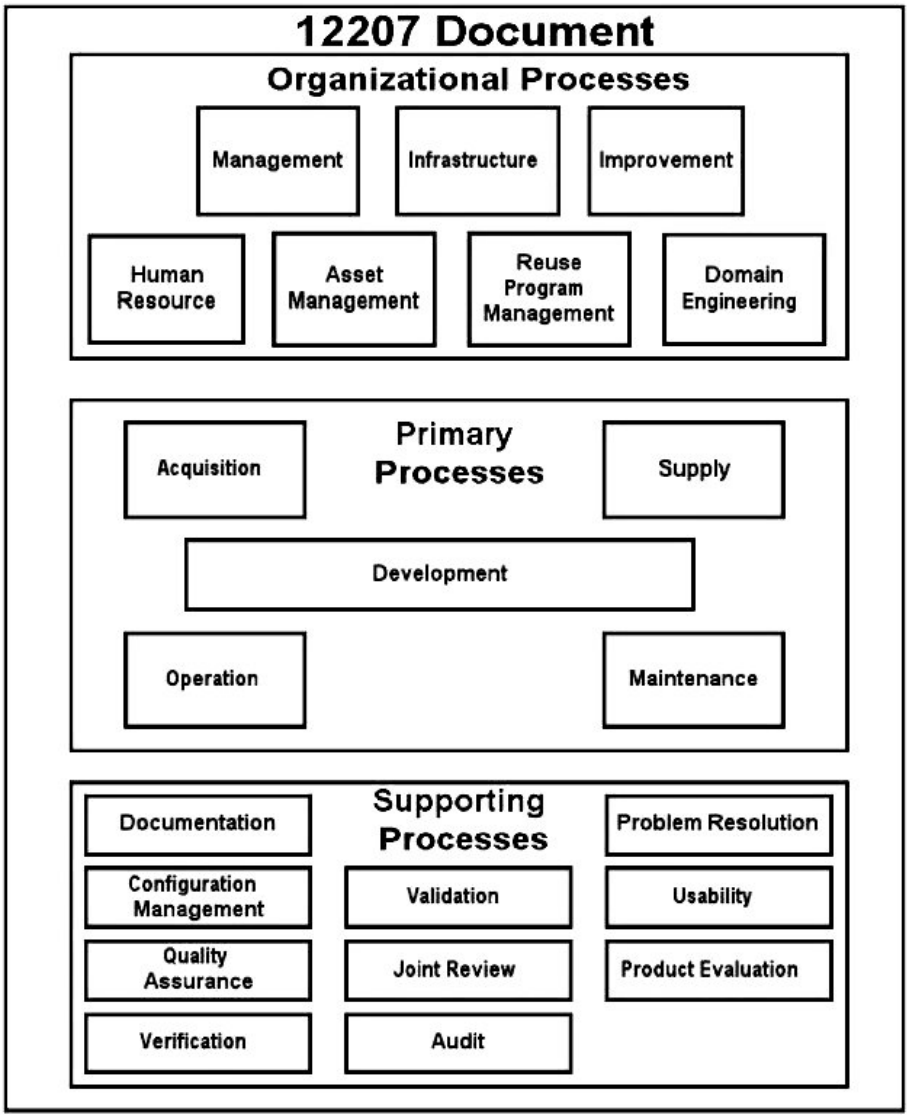
1. strojne opreme,
2. programske opreme,
3. ljudi in
4. poslovne prakse.

Uporaba

Standard predvideva običajne procese, kot so povpraševanje, nabava, razvoj, vodenje, podporna opravila, vzdrževanje in obratovanje programske opreme. Čeprav v svoji zasnovi ni namenjen neposredni uporabi pri delu s projekti ali pri rednem delu, ponuja sistem za postavitev podrejenih standardov, ki so uporabni v posameznih konkretnih primerih. Z njim opisujemo procese v življenjskem ciklu programske opreme od njenega nastanka do njene ukinitve. Svojo ustreznost še posebej izkazuje pri podpori prodajnim aktivnostim, saj zelo dobro razlikuje in definira vlogi naročnika (v standardu preveden kot »odjemalec«) in ponudnika (v standardu preveden kot »dobavitelj«).

V ta namen definira:

1. procese (22), ki jih prikazuje slika 5.2,
2. aktivnosti (95),
3. opravila (325) in
4. cilje (254) pri življenjskem ciklu programske opreme.



Slika 5.2: Shema procesov ISO/IEC 12207 [14]

Lastnosti

Nekatere pomembnejše lastnosti:

1. Definira procese, ki so povezani s programsko opremo in je tako namenjen podpori sporazumevanju in koordinaciji pri odnosu dveh strank, kjer dogovor ali pogodba določata razvoj, vzdrževanje ali upravljanje programskih sistemov.

2. Ne podpira procesa prodaje končnih množičnih komercialnih programskih izdelkov (ki jih kupujemo na policah prodajaln).

3. Je neodvisen od izbranega posameznega modela življenjskega cikla ali metode za razvoj programske opreme in jih ne predpisuje.

4. Ne določa detajlov o tem, kako izpeljati neko aktivnost ali opravilo, ki sestavljata proces. To je prepuščeno dodatnim standardom in definicijam postopkov.

5. Je zelo "varčen"pri zahtevani dokumentaciji. V tem se razlikuje od ostalih primerljivih standardov pri uporabi CASE orodij in pri RAD. Pri tem:

   (a) Ne predpisuje oblike in vsebine dokumentov.

   (b) Zahteva, da je inženirsko delo napravljeno in dokumentirano, ne glede na to, kdaj bodo dokumenti nastali.

   (c) Je povsem nevtralen do CASE orodij, ki prevzamejo funkcijo tradicionalno predpisane dokumentacije.

Predvideva skupno upravljanje projektov, v katerem sodelujeta naročnik in dobavitelj, ter skupnega revidiranja, kar je alternativa tradicionalnemu ciklu dokumentiranja in revidiranja.

Ostalo

Z amandmaji 1 k 12207 so dodali ali zamenjali nekatere procese obstoječemu standardu in za potrebe skladnosti z ISO/IEC 15504 dodali cilje, ki jih v okviru posameznega procesa želimo doseči. S tem je omogočen proces ocenjevanja in izboljševanja procesov. ISO/IEC 12207 sicer definira procese, vendar si z njim ne moremo pomagati pri izboljševanju procesov. To ni njegov domet. Za upravljanje kakovosti je treba uporabljati druge standarde ali modele. Standard, ki definira kakovost, (to je ISO/IEC 90003 na primer) pa po drugi strani ne definira procesov. Torej lahko pri slednjem premlevamo in se pogovarjamo o nekih generičnih procesih – govorimo o njihovih izboljšavah, vendar ne vemo, kateri ti procesi so. Kateri so procesi, ki definirajo programsko opremo v celoti. Postavlja se vprašanje, ali so standardi, ki definirajo kakovost, uporabni brez standardov, ki definirajo procese. Odgovor je: niso uporabni, ker definirajo modele nepoznanih procesov. Od tega ni veliko koristi. Sklepamo lahko, da se presoja poslovanja po 90003 ali 15504 (CMM) mora najprej opraviti z definicijo procesov.

5.1.2 Standard ISO/IEC 90003:2004

Namen

ISO/IEC 90003 uporabljamo za podajanje navodil o tem, kako uporabljati sistema vodenja kakovosti po ISO 9001:2000 v postopku:

- nakupa,
- prodaje,
- razvoja,
- obratovanja in
- vzdrževanja

programske opreme ter pri opravilih, si so s temi fazami povezana.

Uporaba

Primeren je za programsko opremo, ki:

- je del komercialne pogodbe z drugo organizacijo (podjetjem);
- je izdelek namenjen tržišču;
- se uporablja za podporo procesov neke organizacije (podjetja);
- je vsebovani del v strojni opremi; ali pa
- se nanaša na servisiranje programske opreme.

Pri tem so nekatere organizacije (podjetja) vključena v vse zgoraj opisane aktivnosti, spet druga so specializirana na eno ali več od zgoraj naštetih področij.

Nekateri primeri uporabe so naslednji:

1. V osnovi gre za navodila za interpretacijo ISO 9001:2000.
2. Je osnova za izdelavo programske opreme, ki podpira sistem kvalitete programske opreme.
3. Zmanjševanje rizikov pri vseh zgoraj naštetih fazah (nakup, prodaja, razvoj, vzdrževanje in obratovanje), v katerih se nahaja programska oprema ali pri opravilih, povezanih s temi fazami.
4. Pri programu za izboljševanje kvalitete v organizaciji (podjetju) je nepogrešljiv takoj, ko ima organizacija na kakršenkoli način opraviti s programsko opremo.
5. Je v pomoč pri načrtovanju in razvoju organizacije (podjetja).
6. Predstavlja podporo in prispeva k razvoju profesionalnosti.
7. Je osnova za sporazumevanje in koordinacijo dela.

Lastnosti

Nekatere pomembnejše lastnosti so:

- Standard ne dodaja ali na kakršen koli način spreminja zahteve, ki jih podaja ISO 9001:2000.
- Pri uporabi standarda ISO/IEC 90003 je potrebno vse termine in definicije iskati v standardu ISO/IEC 12207.
- V vsaki točki standarda ISO/IEC 90003 so napisani kazalci za nadaljnja navodila v ostalih ISO/IEC standardih. V več kot 90 odstotkih se kazalec nanaša na ISO/IEC 12207 in na amandmaje 1:2002 k ISO/IEC 12207.
- Identificira področja in teme, na katere je potrebno biti pozoren in ki jih je potrebno upoštevati.

Ob tem je neodvisen od:

- tehnologije,
- modela življenjskega cikla,
- razvojnih procesov,
- sekvenc aktivnosti in od
- organizacijske strukture podjetja.

Ostalo

Standard ima dva dodatka.

1. Dodatek A v ISO/IEC 90003 vsebuje kazalce na navodila za implementacijo ISO/IEC 9001:2000 tako, da uporabljamo ostale ISO/IEC

standarde in tehnična poročila s področja IT (dokumentiranje, testiranje, ...). Število različnih kazalcev je 16. Dva najpogosteje uporabljana sta omenjena že zoraj (kazalca na ISO/IEC 12207 in na njegove amandmaje). Med ostalimi pomembnejšimi sta tudi kazalca na:

(a) Guide for the application of ISO/IEC 12207 to project management in

(b) Guide for ISO/IEC 12207 – Software Life Cycle Processes

2. V dodatku B v ISO/IEC 90003 je povezovalna tabela med aktivnostmi za planiranje kvalitete (ISO/IEC 90003) in med aktivnostmi pri razvoju programske opreme (ISO/IEC 12207 z amandmaji k ISO/IEC 12207) tako, da s strani vodenja projekta lahko uporabljamo enovite aktivnosti pri razvoju projektnega plana.

Drugih dodatkov v standardu ISO/IEC 90003 ni.

Na osnovi zgoščene predstavitve ISO/IEC 90003 lahko sklepamo, da morajo podjetja v primeru, ko želijo vzpostaviti sistem kvalitete, ki bo skladen z zahtevami ISO 9001:2001 na področju programske opreme, uporabiti vsaj še tri dokumente (standarde), ki so:

- ISO/IEC 90003,
- ISO/IEC 12207 in
- amandmaji 1 k ISO/IEC 12207

Vsi trije predstavljajo minimum dokumentov, ki so pomembni in potrebni za celotno razumevanje vodil in zahtev, ki jih podaja ISO/IEC 9001:2000.

5.1.3 Standard ISO/IEC 25000:2005

Standard ISO/IEC 25000:2005 [13] podaja navodila za uporabo povsem nove skupine mednarodnih standardov, namenjenih ocenjevanju kakovosti programske opreme. Skupina je imenovana Quality Requirements and Evaluation – SQuaRE.

Namen

SQuaRE podaja:

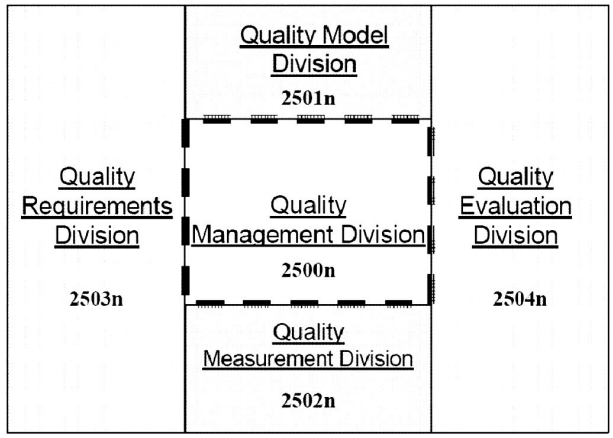
- termine in definicije,
- referenčne modele,
- splošna navodila,
- posamična navodila in
- standarde za:
  - specifikacijo zahtev,
  - načrtovanje in upravljanje ter
  - merjenje in ocenjevanje.

Organizacijo skupine predvidenih 14 standardov SQuaRE, organiziranih v 5 področij, prikazuje slika 5.3.

Lastnosti

SQuaRE nadomešča (bo nadomestil, ko bo popoln) dve skupini predhodnih skupin standardov: 9126 in 14598. Nekatere pomembnejše značilnosti obeh predhodnikov so naslednje:

1. Oba imata skupne normativne, referenčne in funkcionalne korenine.



Slika 5.3: Področja skupine standardov *SQuaRE (ISO/IEC 250xx)* [13]

2. Sta medsebojno komplementarna in dopolnjujoča standarda.

3. Kot posledica medsebojno neodvisnega razvoja sta na mnogih področjih medsebojno nekonsistentna.

Po drugi strani pa so pomembne naslednje značilnosti SQuaRE:

1. Uvaja novi, splošen referenčni model.

2. Uvaja posamezna in podrobna navodila za vsako področje, ki ga pokriva, posebej.

3. Uvaja novo področje Merjenje kakovosti z merami kakovosti.

4. Uvaja novo področje Zahteve za kakovost.

5. Na novo definira proces ocenjevanja.

6. Uvaja navodila uporabe, ki so podkrepljena s primeri praktične uporabe.

7. Standardi so koordinirani in harmonizirani z vsebino ISO/IEC 15939 (Proces merjenja programske opreme).

Uporaba

Model kakovosti predpostavlja naslednje vidike kakovosti programske opreme, ki jih prikazuje slika 5.4:

1. Notranja kakovost, ki jo ocenjujemo na ravni posameznega izdelka ali modula.

2. Zunanja kakovost, ki jo ocenjujemo na ravni informacijskega sistema. Kakovost posamičnega izdelka ali modula ocenjujemo v okviru večjega večjega sistema (programske opreme).

3. Kakovost programske opreme v uporabi predstavlja vidik na ravni ocenjevanja kakovosti na ravni poslovnega sistema. Kakovost posamičnega izdelka ali modula ocenjujemo v okviru poslovnega sistema.

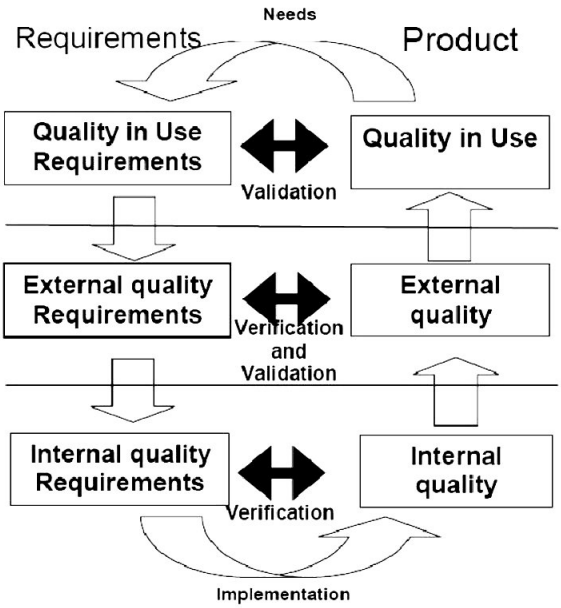
Skupina mednarodnih standardov SQuaRE je namenjena izključno ocenjevanju kakovosti programske opreme in ob tem specifikacijam zahtev, meritev in ocenjevanj. Pri tem je ločena od vodenja kakovosti v skladu z družino standardov ISO/IEC 90003.

Snovalci SQuaRE so želeli doseči izdelavo logično organizirane, bogatejše in poenotene množice standardov, ki pokrivajo naslednja glavna procesa:

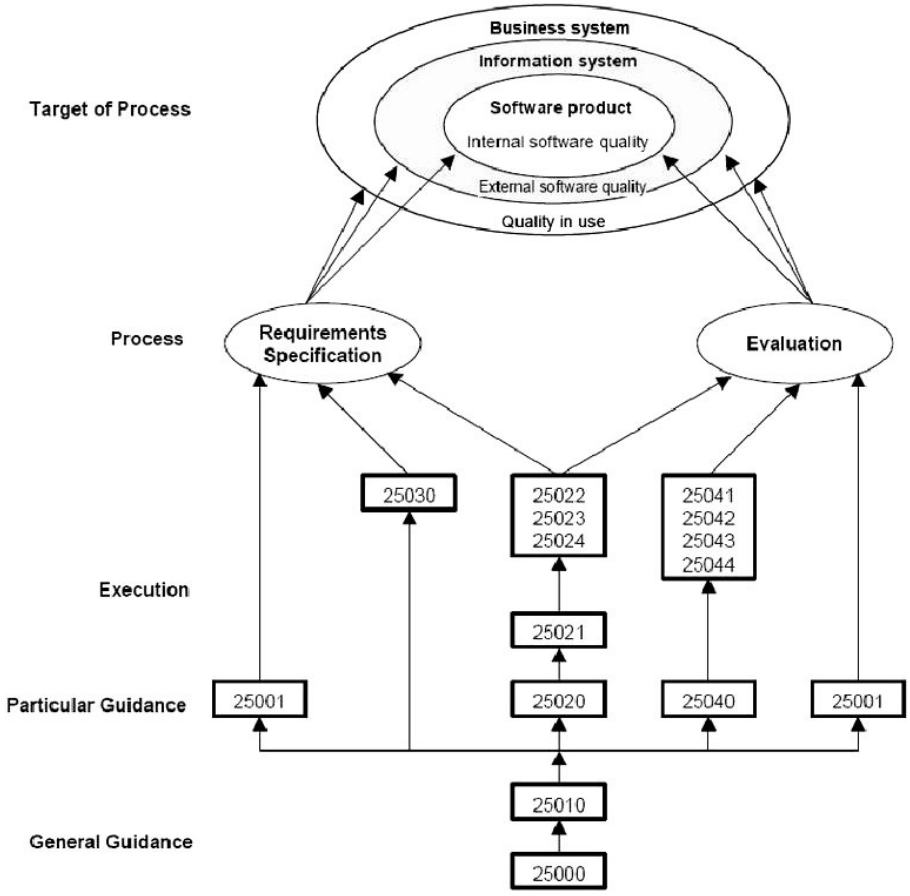
1. Specifikacijo zahtev za kakovost programske opreme.

2. Ocenjevanje kakovosti programske opreme, ki je podprta s procesom merjenja.

Slika 5.5 prikazuje oba glavna procesa.
Definiran model kakovosti vsebuje vidik:



Slika 5.4: Model življenjskega cikla kakovosti programske opreme [13]



Slika 5.5: Splošni referenčni model SQuaRE [13]

- kupca (naročnika) in
- vidik razvoja.

S kupčevo definicijo zahtev za kakovost so podani parametri kakovosti za proces razvoja. S tem standardi predlagajo mere za kakovost programske opreme, ki jih uporabljamo kot:

- razvijalci,
- kupci ali
- ocenjevalci.

Ostalo

Področje merjenja kakovosti programske opreme je izziv domala za vsako podjetje pri nakupu programske opreme, njenem razvoju za lastne potrebe ali razvoju za naročnika. S problemom ocenjevanja, merjenja in podajanja zahtev za kakovost se stalno srečujemo v vlogi vodje poslovnega procesa, IT procesa ali uporabnika, in vendar šele sedaj skupina standardov 250xx ali SQuaRE obljublja dovolj kakovostno pomoč. Da gre za široko problematiko, je razvidno že iz tega, da so si snovalci zamislili že na samem začetku 14 standardov in nekaj tehničnih poročil, ki bodo pojasnjevala uporabo standardov. Verjetno bo ta skupina standardov postala ena temeljnih standardov v IT industriji ob boku njenih temeljnih standardov, kot so: 12207, 90003 in 15504

5.1.4 Standard ISO/IEC 25051:2006

Namen

Standard je namenjen ocenjevanju kakovosti komercialnih programskih izdelkov, namenjenih neznanemu kupcu (COTS).

Standard 25051 vzpostavlja:

1. Kakovostne zahteve za COTS programske izdelke.
2. Zahteve za testno dokumentacijo s katero testiramo COTS izdelke, ki vključuje tudi testne zahteve, testne primere in testna poročila
3. Navodila za ocenjevanje ustreznosti

Iz tega lahko razberemo, da se standard ne ukvarja s kakovostjo programske opreme v fazi razvoja (na primer kakovost specifikacije, razvoja, ...).

Lastnosti

Osrednji del standarda tvorijo tri poglavja:

1. Zahteve za COTS programski izdelek (5. poglavje standarda), ki predvideva zahteve za:
   (a) opis izdelka,
   (b) uporabniško dokumentacijo in
   (c) kakovost programskega izdelka.
2. Zahteve za testno dokumentacijo (6. poglavje standarda), kjer so opisane:
   (a) splošne zahteve,
   (b) zahteve za načrt testiranja,
   (c) zahteve za opis testiranja in
   (d) zahteve za predstavitev rezultatov testiranja.
3. Navodila za ocenjevanje skladnosti (7. poglavje standarda) z zahtevami iz prejšnjih dveh poglavij, kamor sodi:
   (a) opis splošnih principov, ki jim COST izdelek mora zadostiti,

(b) prisotnost vnaprej znanih pogojev,

(c) prisotnost vseh potrebnih aktivnosti za ocenjevanje,

(d) ocenjevanje skladnosti s strani tretje osebe,

(e) poročilo o ocenjevanju in

(f) ponovno ocenjevanje skladnosti.

Uporaba

COST se množično uporabljajo na skoraj vseh področjih poslovanja in so nemalokrat vitalnega pomena za poslovanje, za varnost ali za osebno uporabo. Osnovna značilnost COST je ta, da kupec nima vpliva na njene zmožnosti ali na njeno kakovost. Tipično so tovrstni izdelki prodani skupaj z uporabniško dokumentacijo, ki je na voljo le, ko odpremo že kupljeno embalažo. Tako so informacije, ki so na sami embalaži, edine informacije na voljo kupcu pred nakupom in edino okno do najnujnejših informacij, ki omogoča kupcu, da oceni kakovost programskega izdelka in se odloči za morebiten nakup.

Za kupca je izbira visoko kakovostnih COTS izdelkov še posebej pomembna, saj morajo ti izdelki delovati v zelo različnih okoljih in praviloma ni možnosti primerjave s podobnimi izdelki.

Po drugi strani tudi izdelovalci potrebujejo način za zagotavljanje zaupanja v svoj izdelek in v storitve povezane z njim. Nekateri izdelovalci izberejo ocenjevanje nekoga tretjega ali zagotovijo overovitev, da zagotovijo potrebno zaupanje. COTS programska oprema je skladna s tem standardom če:

- ima lastnosti, kot jih določa 5. poglavje standarda;
- je ob testiranju nastala dokumentacija, kot jo določa 6. poglavje standarda;

- so morebitne anomalije odkrite med testiranjem dokumentirane in rešene še preden je izdelek kupljen. Rešene so, če so anomalije odpravljene ali pa je umaknjena zahteva lastnosti, pri kateri se je anomalija pokazala. Anomalija je tudi sprejemljiva, če:
  - zaradi nje ni ogrožena kakšna zahtevana lastnost ali
  - je izdelovalec primerno pregledal naravo in posledice anomalije pri potencialnih kupcih ter ugotovil, da je zanemarljiva in anomalijo dokumentiral za potrebe bodočih izboljšav.

Ostalo

Med uporabniki standarda so:

1. Izdelovalci.
2. Organizacije za certifikacijo programske opreme.
3. Laboratoriji za testiranje.
4. Organizacije za akreditacijo programske opreme.
5. Potencialni kupci.
6. Končni uporabniki.
7. Organizacije, ki uporabljajo COTS programsko opremo.
8. Organizacije za regulacijo, ki podajajo zahteve in izdajajo priporočila.

5.1.5 Standard ISO/IEC 25062/2006

Namen

Standard je namenjen izdelavi standardiziranega poročila in predstavitvi rezultatov o testiranju uporabnosti programske opreme s tako imenovanim

Common Industry Format (CIF) dokumentom (poročilom). To pomeni, da je predpisan format poročil, ki so namenjena kupcem in jih pripravljajo izdelovalci tako, da so v poročilu zabeležene uporabljene metode testiranja in rezultati opravljenih testov. CIF standardizira tipe informacij, ki jih pridobivamo pri uporabniškem testiranju. S tem omogoča izmenjavo poročil o rezultatih testiranja med različnimi organizacijami, ne glede na to ali gre za izdelovalce ali kupce programske opreme.

Lastnosti

Do pred kratkim namreč ni bilo standarda za izmenjavo poročil o testiranju in z uporabo standardiziranih poročil se nadejamo naslednjih prednosti:

1. Zmanjšanje potrebnega časa za učenje in za pripravo testiranja uporabnosti s strani osebja, ki pripravlja in izvaja testiranje, saj se osebje v vseh primerih ravna podobno in pripravlja poročila na enak način, ne glede na to, v koliko različnih organizacijah izvajajo testiranja, za koliko različnih primerov programske opreme gre in za koliko različnih naročnikov testiranja.

2. Poenostavitev in izboljšanje komunikacije med izdelovalci in kupci programske opreme, saj uporabniki standardiziranih poročil uporabljajo skupen jezik in izkušnje.

Uporaba

S standardiziranim poročilom je omogočena avtomatizacija odločanja o tem, ali so cilji uporabnosti neke programske opreme doseženi ali ne. Potrebe po odločanju se pojavljajo predvsem ob nakupih in nadgradnjah programske opreme. Predloga poročila je na spletnem naslovu http://www.ncits.org/ref-docs/CIF/CIF_template.dot.

Ostalo

Uporabnost programske opreme je ključen faktor, na osnovi katerega lahko predvidevamo njeno uspešnost. Pri programski opremi izvajamo testiranje njene uporabnosti v različnih fazah njenega življenjskega cikla. Še posebej v fazi razvoja in nakupa. Takšno testiranje običajno vključuje:

- osebe, ki predstavljajo tipično ciljno populacijo uporabnikov,
- tipična opravila, kjer programsko opremo uporabljamo ter
- mere učinkovitosti, uspešnosti in subjektivnega zadovoljstva.

5.1.6 Standard ISO/IEC 27001:2005

Namen

ISO/IEC 27001:2005 daje model za:

- vzpostavitev,
- izvedbo,
- obratovanje,
- spremljanje,
- pregledovanje z ocenjevanjem,
- vzdrževanje in
- izboljševanje.

sistema za upravljanje informacijskega varovanja (Information Security Management System – ISMS). Pri tem velja, da naj bi za organizacije bil sistem ISMS del njihovih strateških usmeritev. Načrt in implementacija modela ISMS je odvisna od potreb in ciljev podjetja, varnostnih zahtev,

dejavnosti, ki jo podjetje izvaja ter od njegove strukture in velikosti. Vse, od česar je ISMS odvisen, se s časom spreminja. Zato predpostavljamo, da mora model ISMS omogočati spremembe. ISMS je potrebno po potrebi dopolnjevati ali klestiti glede na specifičnosti in zahteve organizacije.

Lastnosti

Standard predpostavlja procesni pristop za izvedbo ISMS. To pomeni, da je organizacija predstavljena kot skupek procesov, ki imajo svoje vhode in izhode, ki so po potrebi medsebojno povezani. Ker vsak proces potrebuje po eni strani svoje vire, po drugi strani pa mora biti upravljan, spremljamo tako štiri množice dejavnikov, ki so lahko varnostno občutljivi:

- vhodi,
- izhodi,
- različni viri, ki jih za izvajanje procesa potrebujemo in
- realizacija, način ali postopki upravljanja procesa.

Pri tem standard daje poseben pomen:

- razumevanju informacijskih varnostnih zahtev in pomena vzpostavitve informacijske varnostne politike s svojimi cilji,
- implementaciji in realizaciji kontrol, ki upravljajo z informacijskimi varnostnimi tveganji v kontekstu doseganja poslovnih ciljev organizacije,
- spremljanju in pregledovanju z ocenjevanjem uspešnosti in učinkovitosti uporabljenega ISMS in
- talnemu izboljševanju, ki temelji na objektivnem merjenju uspešnosti in učinkovitosti.

Iz zgornjega je razvidno, da standard temelji na preizkušenem in vsesplošno uporabljanem modelu „Plan-Izvedba-Presoja-Ukrep“ („Plan-Do-Check-Act“), ki je vgrajen v vse procese ISMS.

Uporaba

Standard BS7799 iz leta 1995 je definiral razvoj in implementacijo sistema za upravljanje informacijskega varovanja (ISMS). Standard je usmerjen na varovanje razpoložljivosti, zaupnosti in integriteto informacijskih virov tako, da upošteva cilje organizacije. To pomeni, da je uporabil pristop ocenjevanja varnostnih tveganj skozi optiko poslovnih tveganj.

Na začetku je bil to standard, ki je imel status dokumenta "dobre prakse". Kot takšen je dajal vodilo za izvedbo ISMS posamezne organizacije, vendar ni nudil sheme verificiranja in certificiranja s strani tretje organizacije. Zaradi potreb po pridobitvi certifikata, ki ga podeljujejo organizacije, usposobljene za presojo skladnosti, so razvili drugi del standarda BS7799-2 (imenovan tudi drugi del BS7799), ki se ukvarja z zahtevanimi specifikacijami kontrol in ne z ISMS.

Z internacionalizacijo in revizijami standarda BS7799 je nastal ISO/IEC 17799:2005 in podobno je na osnovi standarda BS7799-2 nastal ISO/IEC 27001:2005. Tako je danes govorimo o certificiranju po standardu ISO/IEC 27001:2005, ki za vir, iz katerega izbiramo in nato izvajamo kontrole, uporablja ISO/IEC 17799:2005. V bistvu je 17799 drugi del 27001.

Poglavje 6

Upravljanje tveganj

Organizacije, katerih delovanje je zelo regulirano, kot je to v primeru finančnih institucij, telekomunikacijskih podjetij, energetskega sektorja, zdravstva in farmacevtske industrije ter podobnih, je upravljenje tveganj v veliki meri vpeto v njihovo vsakodnevno poslovanje že mnogo let. Pri mnogih organizacijah pa se šele v zadnjem času stanje spreminja v smeri zavedanja pomena učinkovitega upravljanja tveganj. Praksa kaže, da se vrh upravljavske piramide v organizacijah začenja zavedati pomena upravljanja tveganj, ob tem pa se večje število zaposlenih v poslovnem svetu začenja ukvarjati s tveganji. Upravljanje tveganj se s časom prenese povsem na operativni nivo in od tam nazaj na poslovni nivo upravljanja, saj se tveganja prenašajo iz nivoja na nivo in jih ne moremo upravljati izolirano, vsako zase. Prenašajo se tudi po horizontali med samimi oddelki. Največkrat se organizacija zave upravljanja tveganj kot samostojnega področja delovanja v času priprave načrtov za neprekinjeno poslovanje.

Ne glede na dobrodošle spremembe, upravljanje s specifičnimi tveganji, kot so tveganja v IT ali logistiki, običajno še vedno niso sestavni del strateškega načrtovanja v organizacijah. IT, logističnih in drugih specifičnih tveganj v vrhu upravljavske piramide organizacije še vedno ne zaznavajo

kot področja, ki bi zahtevalo predstavnika "tveganj" (to je lastnika "tveganj") v vodstvu. Seveda smo tudi pri srednjem upravljavskem nivoju daleč od idealnih razmer: četudi upravljavci tveganj igrajo osrednjo vlogo pri analizi in obravnavi tveganj v organizaciji, še vedno kronično primanjkuje osebja in znanja.

V praksi se pojavlja tudi problem pri učinkoviti in pragmatični realizaciji upravljanja tveganj po tem, ko je že opravljena korektna ocena tveganja, saj ne pride do premišljene odločitve, kaj s tveganjem napraviti – pa čeprav bi to pomenilo odločitev, da glede nekega tveganja ne naredimo ničesar. V takšnem okolju je nastal standard ISO 31000, ki je nevtralen do kakršnega koli poslovanja organizacije. Predstavlja dobro izhodišče za vse, ki se šele začenjajo ukvarjati z tveganji, in za tiste, ki iščejo nekaj več.

ISO 31000 je pisan v poslovnem jeziku z namenom razumevanja ključnih konceptov in terminologije pri upravljanju tveganj. Prispeva h konsistentnosti upravljanja tveganj s pregledom tehnik in metod. Definira izrazoslovje in tako rešuje pereče probleme uporabe skupnega jezika za opisovanje tveganja, merjenja vplivov, verjetnosti, negotovosti ter ostalih dimenzij upravljanja tveganj med tehnološko in poslovno usmerjenim kadrom v organizaciji in med organizacijami.

Nek vsesplošno priznan standard ali okvir za upravljanje tveganj je namreč potreben, saj mora vsaka organizacija vsaj:

1. poenotiti jezik za delo s tveganji;
2. uporabiti skupno metriko za delo s tveganji ne glede na področje uporabe (poslovno, tehnološko, itd);
3. zagotoviti varnost na vsakem področju delovanja (tudi na področju IT in logistike, na primer) ter jo integrirati v splošno varnost organizacije;
4. tveganja vsakega področja je potrebno znati predstaviti v kontekstu ali jih prevesti v poslovna tveganja; in navsezadnje

5. vsa tveganja prevesti v jasno sliko investicij.

ISO 31010 podpira standard ISO 31000 v tistem delu, ki se ukvarja s prepoznavanjem in ocenjevanjem tveganj. Oboje je sestavni del upravljanja tveganj. Standard je podlaga za odločanje o najustreznejšem pristopu za obvladovanje posameznega tveganja, je pomoč pri implementaciji principov obvladovanja tveganj (iz ISO 31000).

ISO/IEC 27005 opisuje proces upravljanja tveganj in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost. Ne določa, ne predlaga, ne imenuje kakršne koli metode za analizo tveganj. Določa pa strukturirane, sistematične in natančno določene procese (od analize do izdelave načrtov upravljanja).

ISO/IEC 27001 je mednarodni standard, ki podaja model za vzpostavitev, izvajanje, upravljanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema informacijske varnosti. Učinkovit sistem upravljanja informacijske varnosti predpostavlja sistematično upravljanje informacijskih tveganj, ki mora biti skladno s potrebami, usmeritvami in okoljem v katerem organizacija deluje. Navsezadnje mora biti upravljanje informacijskih tveganj v skladu z upravljanjem vseh tveganj, s katerimi se organizacija srečuje. Varnostne usmeritve se nanašajo na pravočasno in učinkovito upravljanje tveganj na področjih in v času, kjer in ko je to potrebno. Gre za proces, ki ga je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

Pomembnejši standard s področja varnosti v logistiki, ki se neposredno nanašajo tudi na upravljanje tveganj, je ISO 28000, katerega namen je izboljšanje varnosti oskrbovalne verige. Namenjen je upravljavskemu nivoju organizacije, ki je v pomoč pri vzpostavitvi celovitega sistema upravljanja varnosti oskrbovalne verige tako, da organizacija oceni okolje v katerem deluje in ugotovi, ali so vzpostavljeni ustrezni varnostni ukrepi, in ali organizacija izpolnjuje vse zakonske zahteve.

V tem poglavju bo še opisan model tveganj, ki temelji na segmentaciji

javnosti. V tem modelu je bistvena predpostavka, da so tveganja lastna ljudem in ne stvarem ali pojmom. Princip modeliranja tveganj predvideva, da moramo model sistema procesov ter vhode in izhode v procese segmentirati prav tako kakor javnost, pri kateri želimo tveganja modelirati in simulirati. Tovrstni pristop zahteva bistveno kompleksnejše modeliranje tveganj kot je danes najpogosteje v uporabi, vendar po drugi strani prinaša večjo zaupanje v modeliranje, saj je bliže realnosti življenja.

Na koncu poglavja bo opisan še primer kataloga tveganj, kot rezultat konvencionalnega prepoznavanja in ocenjevanja tveganj, ki vsebuje vsa prepoznana in opisana tveganja s področja oskrbovalne verige. Proces upravljanja tveganj je zahteven in zato velikokrat počasen in ne dovolj natančen. Ideja prosto dostopnega kataloga vseh do sedaj prepoznanih tveganj pa organizacijam nudi možnost, da pri procesu uporabijo tudi zunanja znanja, ko se lotevajo upravljanja tveganj. Katalog tveganj vsebuje tveganja v oskrbovalni verigi, ki so bila prepoznana v organizacijah z različnih področij delovanja. Zato je lahko odličen vir informacij za širok spekter organizacij, ki pristopajo k upravljanju tveganj, saj ga lahko uporabljajo kot smernice za prepoznavanje tveganj in kot opomnik, s katerim ugotovijo, katera od že identificiranih tveganj iz kataloga lahko prepoznajo tudi znotraj svoje organizacije.

Problem definicije in razumevanja pojma tveganje Tveganja so del našega bivanja in videti je, kot da se ljudje še nikoli do sedaj nismo toliko ukvarjali z izzivi tveganj kot ravno v današnjem času. Tveganja so predmet obravnave v številnih člankih, komentarjih in pogovorih. Prav tako obstaja veliko različnih dojemanj in definicij tega pojma. Tudi če se neka javnost uskladi glede definicije tveganja, še ne jamči mnenjske usklajenosti: Kako tveganja zaznati? Kako jih meriti? Katerim tveganjem smo v katerem trenutku izpostavljeni? Kolikšne so posledice izpostavljenosti tveganjem – kakšen je njihov vpliv? Katera in kako velika tveganja so

sprejemljiva? Za koga so sprejemljiva in za koga ne? Kako se tveganja spreminjajo skozi čas? Kako vplivajo posamezno, kako združeno? Kakšen je njihov medsebojni vpliv in kakšne so posledice teh interakcij? Kako jih upravljati? Kako ovrednotiti potrebna sredstva za zmanjšanje tveganj? Odprtih vprašanj je še veliko in dajejo slutiti kompleksnost problema, na katerega naletimo, ko skušamo tveganja celovito obravnavati in jih upravljati.

Kaj pomeni pojem tveganje razumemo, vendar ima ta pojem številne različne interpretacije. Poglejmo si nekatere izmed njih:

1. V spletnem slovarju BusinessDictionary.com [1] je podanih šest definicij z različnih področij. Prva definicija je splošna in pravi, da je tveganje: "Verjetnost ali nevarnost za nastanek škode, poškodbe, izgube, kršenja obveznosti ali kakšen drug negativen dogodek, ki ima zunanje ali notranje vzroke in ga je mogoče vnaprej nevtralizirati z zaščitnimi akcijami." Druga definicija je s finančnega področja in opisuje sedemnajst različnih kombinacij in pomenov besede tveganje. Sledijo še definicije s področja prehrambene industrije, zavarovalništva, trgovine in navsezadnje delovnega mesta. Slednja pravi, da je tveganje: "Produkt resnosti posledic in vpliva verjetnosti nekega tveganega dogodka ali fenomena."

2. V spletnem slovarju InvestorWords.com [3] je tveganje opisano kot: "... merljiva verjetnost za izgubo ali izgubo zaradi zmanjšanja ..." Tudi tu ponujajo definicije v dvajsetih kombinacijah besede tveganje s kakšno drugo besedo.

3. Na Wikipediji [34] je v članku o pojmu tveganje napisano, da definicija besede potrebuje dodatno pozornost ekspertov, kar kaže na to, da obstaja mnenje, da beseda ni dovolj dobro definirana, kljub temu, da je prispevek nadpovprečno dolg in upošteva mnoge vidike. Med drugim je v prispevku zapisano, da je tveganje koncept, ki natančno

opisuje verjetnosti za posamezne možne izzide. V nadaljevanju je opisano, da je tveganje potrebno opisati kvalitativno in kvantitativno. Citirajo tudi Franka Knighta, ki je v svojem delu [6] razmeji tveganje in negotovost.

4. Adam Green [2] v svojem članku pravi, da vsaka definicija tveganja prinaša subjektiven pogled na to, kaj tveganje je, glede na področje in način uporabe. V svojem delu, ki govori o vodenju projektov, predstavi tudi definicijo, kjer je tveganje enako produktu med nevarnostjo in izpostavljenostjo in je izpostavljenost enaka vplivu škode na tisto ali tistega, na katerega škoda vpliva. Na vsak način je zanj osrednji pojem nevarnost, da se zgodi slučajni dogodek (hazard).

5. Po Johnathanu Munu [23] sta pojma negotovost in tveganje različna, vendar povezana. Tveganja so nekaj, kar je nekomu ali nečemu lastno in je posledica negotovosti. Isti avtor pravi, da je na začetku vedno negotovost in z njo povezana tveganja, ki s časom, v katerem se izvajajo neke akcije in dogajajo dogodki, preidejo v dejstvo. Mun tudi trdi, da se lahko soočimo z negotovostjo, ki sploh nima tveganja. To opisuje na primeru strmoglavljenja letala, na katerem sta dve osebi in eno staro padalo, za katerega ne vemo, ali se bo ob uporabi sploh odprlo ali ne. Obe osebi sta v enaki negotovosti glede tega, ali se bo padalo odprlo ali ne. Če je objekt negotovosti staro padalo in se obe osebi dogovorita, kdo bo uporabil padalo, potem bo oseba s padalom prevzela vso tveganje glede odprtja padala od trenutka, ko bo oseba izskočila iz padajočega letala, pa do trenutka, ko se bo padalo odprlo oziroma bo ostalo zaprto. Medtem druga oseba, ki nima padala, ne bo v ničemer tvegala glede delovanja padala, obenem pa nima možnosti, da preživi.

Iz različnosti zgornjih definicij je mogoče sklepati, da vsako področje pojem tveganje opredeljuje drugače; tudi v okviru področij se krešejo

mnenja o različnih interpretacijah in celo pri posameznem primeru imamo opraviti z različnimi, nemalokrat nasprotujočimi mnenji o tveganjih.

Vsako področje ima tako svojo definicijo tveganj ali prevzame eno od obstoječih. Te definicije niso popolne, saj gre za kompleksen pojem, kar potrjuje že njihova številnost. Uporaba posameznih definicij, ki reducirajo kompleksnost tveganj, je verjetno nujna, da v eksaktnih znanstvenih disciplinah sploh lahko uporabljamo ta pojem. Zavedati se moramo, da so tveganja zanimiva aktualna problematika. Veliko ljudi se ukvarja z modeli tveganj (VaR, SARA, SPRINT), ki so vedno bolj kompleksni in upoštevajo vse več lastnosti tveganj oziroma parametrov. Tu so še standardi in ogrodja za upravljanje tveganj (ISO 31000, AS/NZ 4360 COSO ERM, IT Risk Management Framework).

Pri iskanju definicije tveganja smo v bližnji preteklosti prišli do točke, ko se v okviru mednarodne institucije ISO niso mogli poenotiti glede ključne opredelitve glede definicije tveganja. Tako v standardu ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management manjkala natančna definicija terminov, kot so: nevarnost (grožnja), ranljivost, verjetnost (likelihood), kot je v uporabi pri študiju tveganj ter predstavlja kombinacijo grožnje in ranljivosti, ter navsezadnje tveganje [22]. Kmalu po izidu standarda je v članku na ta problem opozoril Steven J. Ross [25]. V tem primeru, ki pa zdaleč ni edini, smo se soočali z vprašanjem natančne in jasne obravnave problematike, ko osnovni pojmi problematike niso bili nedefinirani. O čem je govoril ISO/IEC 27005 (v stari verziji), če ne vemo, kaj tveganje je? Standard je bil napisan tako splošno, da bi se ga dalo verjetno uporabiti tudi na drugih področjih (na primer na področju logistike). Vsekakor pa so ostajala odprta vprašanja, kaj tveganja so, kako jih določiti in upravljati. Standard je govoril tudi o tem, da tveganja ocenjujemo s splošnega in podrobnega nivoja. Torej smo se lotevali delitve tveganj na splošen in podroben nivo, a še vedno nismo vedeli, kaj tveganje točno je. Takšnemu stanju smo bili

priča do nove verzije standarda, ki nosi oznako ISO/IEC 27005:2011 (izšel je leta 2011) in je bila sinhronizirana z ISO 31000. Nedorečena pa ostajajo še številna področja, kjer se pogovarjamo o tveganjih, ne da bi bil sam pojem, za potrebe področja, definiran.

6.1 Standard ISO 31000:2009

ISO 31000:2009 [7] določa načela in splošne smernice za upravljanje tveganj. Uporablja se za vse vrste tveganj, ne glede na njihovo naravo, in predvideva tako pozitivne kakor tudi negativne posledice. Namenjen je organizacijam vseh vrst, ne glede na njihovo specifičnost. Čeprav določa splošne smernice, pri tem ne zahteva enotnosti pri upravljanju tveganj. Pri vzpostavitvi in implementaciji načrtov in okvirov za upravljanja tveganj upošteva različnost potreb v organizacijah, posebnosti njihovih ciljev, kontekst, strukturo, načina delovanja, procese, funkcije, projekte, izdelke, storitve in sredstva ter specifičnosti obstoječih praks.

Zaradi splošnega konteksta omogoča celovita navodila za upravljanje tveganj na različnih področjih in je tako namenjen organizacijam vseh velikosti in vseh vrst, ne glede na njihovo specifičnost (organizacijam s področja financ, inženirstva, varnosti, in ostalim).

Namenjen je uporabi skozi celotno življenjsko dobo organizacije z najširšim razponom dejavnosti, ki vključuje tudi vzpostavitev strategij, odločanje, poslovanje, izvajanje projektov, izvajanje ostalih funkcij organizacije, proizvodnjo in upravljanje z izdelki, storitvami in sredstvi ter podobnim.

Standard že takoj na začetku definira tveganje, ko pravi: Organizacije različnih tipov in velikosti so soočene z notranjimi in zunanjimi faktorji in vplivi, ki povzročajo negotovost glede časa, v katerem bo organizacija dosegla svoje cilje in glede tega, če jih sploh bo dosegla. Učinek negotovosti glede doseganja ciljev organizacije je "tveganje”.

Standard ni namenjen temu, da bi se organizacije v skladu z njim certificirale.

Proces upravljanja tveganj v organizaciji ali v celotni oskrbni verigi je priporočljivo zastaviti v okviru cikla Plan-Do-Check-Act (PDCA), ki je že uveljavljen procesni cikel, tudi v okviru standarda ISO 9001. Osnovna ideja cikla je, da proces najprej zasnujemo in načrtujemo (Plan), nato ga uvedemo oziroma izvedemo (Do), ga preverjamo in nadzorujemo (Check) ter na podlagi ugotovitev prilagajamo, spreminjamo in dopolnjujemo, ter stalno izboljšujemo (Act). Standard ISO 31000 pri svojem okvirju za upravljanje tveganj uporablja cikel PDCA, prirejen za namene upravljanja tveganj. Slika 6.1 prikazuje relacije med principi, okvirom in procesom upravljanja tveganj po ISO 31000. V splošnem standard določa arhitekturo za učinkovito upravljanje tveganj. Gradniki te arhitekture pa so principi, okvir in proces.

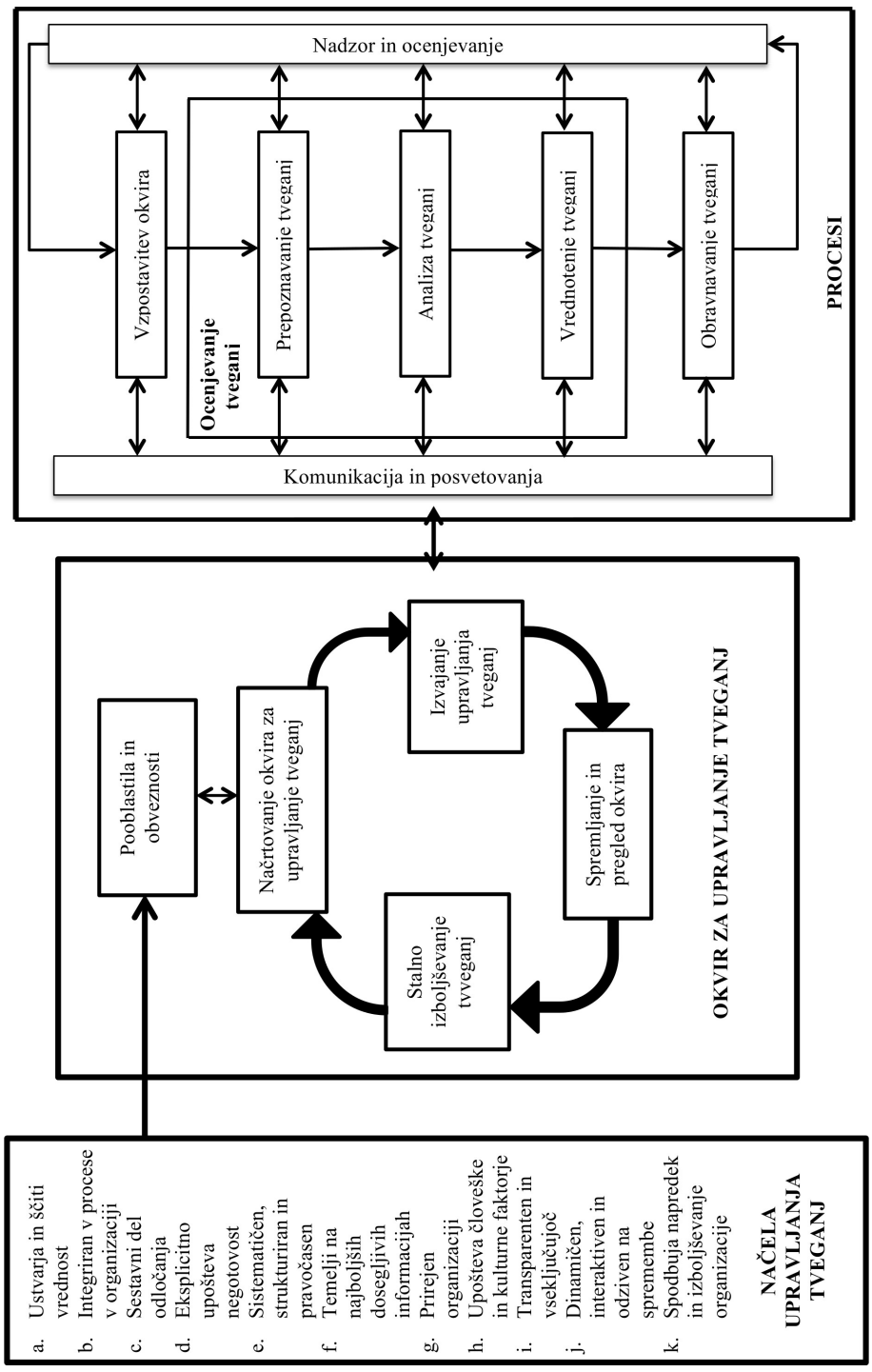
6.1.1 Struktura dokumenta ISO 31000

Standard sestavlja pet poglavij in dodatek – skupaj 23 strani.

Po uvodu sledi pomembno poglavje z definicijami in opisom posameznih terminov. Gre za povzetek dokumenta ISO Guide 73:2009, Risk Management – Vocabulary [9]. To poglavje je za razumevanje celotnega standarda nepogrešljivo in zavzema polnih šest strani.

Tretje poglavje predstavi ključnih enajst principov uspešnega upravljanja tveganj v neki organizaciji. Za predstavitev teh principov porabi dobro stran. V dodatku je opisanih nekaj nadaljnjih usmeritev za organizacije, ki si želijo učinkoviteje upravljati tveganja.

Četrto poglavje opisuje okvir za učinkovito upravljanje tveganj, ki naj bi bil vsebovan na vseh nivojih organizacije. Okvir zagotavlja, da se o tveganjih ustrezno poroča tako, da je mogoče na osnovi informacij (informacije nastanejo v procesu upravljanja tveganj) sprejemati ustrezne odločitve – seveda na vseh nivojih vodenja organizacije. Okvir je opisan na petih



Slika 6.1: Relacije med principi, okvirom in procesom standarda ISO 31000 [18]

straneh.

Zadnje poglavje na osmih straneh podrobno opisuje proces upravljanja tveganj. Sestavljen je iz petih glavnih aktivnosti. Osrednja aktivnost je ocenjevanje tveganj, ki ga pa podrobneje opisuje ISO/IEC 31000, in je skupno ime za (pod)aktivnosti identifikacije, analize in vrednotenje tveganj.

6.1.2 Termini in definicije po ISO 31000

Tveganje

Učinek negotovosti pri doseganju ciljev.

Opomba 1 Negotovost je odklon od pričakovanega (pozitiven in/ali negativen).

Opomba 2 Cilji organizacije lahko imajo različne vidike (kot npr. finančni, vidik zdravja in varnosti te okoljevarstveni) in se lahko upoštevajo na različnih nivojih (kot npr. strateški, nivo celotne organizacije, nivo izdelkov in procesov).

Opomba 3 Tveganje je pogosto opisano kot referenca morebitnim *dogodkom* in *posledicam* oziroma kombinacij obeh.

Opomba 4 Tveganje je pogosto izraženo kot kombinacija posledic nekega dogodka (tukaj so vštete tudi možne spremembe okoliščin) in s tem povezane *verjetnosti* določenega pojava.

Opomba 5 Negotovost je stanje, ki se delno pojavi takrat, ko se zgodi pomanjkanje informacij in/ali znanj, povezanih z razumevanjem oziroma poznavanjem dogodka, njegovih posledic ali verjetnosti.

Upravljanje tveganj

Koordinirane aktivnosti upravljanja in kontroliranja organizacije v povezavi s tveganjem, ki dajejo okvir za učinkovito upravljanje *tveganj*.

Okvir za učinkovito upravljanje tveganj

Gre za sklop sestavin, ki zagotavljajo temeljne in organizacijske ureditve za oblikovanje, vpeljavo, *nadzorovanje*, poročanje in nenehno izboljšavo *upravljanje tveganj* celotne organizacije.

Opomba 1 Temelji, ki vključujejo politiko, cilje, pooblastila in zavzetost upravljanju *tveganj*;

Opomba 2 Organizacijski dogovori, ki vključujejo plane, razmerja, odgovornosti, sredstva, procese in aktivnosti; ter

Opomba 3 Okvir za učinkovito upravljanje tveganj, ki sovpada s splošno organizacijsko strategijo in aktivnostmi te organizacije.

Politika ukvarjanja s tveganji

Izjava, ki zajema splošne namene in usmeritve organizacije v povezavi z *upravljanjem tveganj.*

Odnos do tveganja

Odnos do *tveganja* pomeni pristop organizacije, s katerim ta tveganja oceni ter jim posledično sledi oziroma se jim izogne.

Planiranje upravljanja tveganj

Shema znotraj *okvira za učinkovito upravljanje tveganj*, ki navaja pristop, komponente upravljanja in sredstva, ki so dodeljena upravljanju *tveganj.*

Opomba 1 Komponente upravljanja ponavadi vključujejo postopke, prakse, dodeljevanja odgovornosti, zaporedja in tempiranje aktivnosti.

Opomba 2 Plan upravljanja tveganj se lahko nanaša na določen produkt, proces in projekt ter lahko zajema le del organizacije ali pa celotno.

Lastnik tveganja

Oseba ali subjekt z odgovornostjo in pooblastili za upravljanje *tveganja*.

Proces upravljanja tveganj

Sistematična uporaba politike upravljanja, postopkov in praks v zvezi z aktivnostmi komuniciranja, svetovanja, identificiranja, analiziranja, ocenjevanja in opazovanja *tveganj* ter ravnanja z njimi.

Vzpostavitev okvirov

Definiranje zunanjih in notranjih parametrov, ki jih je treba vzeti v ozir pri upravljanju tveganj, ter določitve obsega in *kriterijev tveganja* za politiko *upravljanja tveganj*.

Zunanji okvir

Zunanje okolje, v katerem si organizacija prizadeva izpolniti zadane cilje. Pod zunanje okolje lahko spada:

- kulturno, socialno, politično, pravno, regulativno, finančno, tehnološko, naravno in konkurenčno okolje, ne glede na to ali je mednarodno, državno, regionalno ali lokalno;
- ključni dejavniki in trendi, ki imajo vpliv na cilje organizacije; ter
- odnosi, dojemanje in vrednotenje zunanjih zainteresiranih strani (deležniki itd.).

Notranji okvir

Notranje okolje, v katerem si organizacija prizadeva izpolniti zadane cilje. Pod notranje okolje lahko spada:

- vodstvo, organizacijska struktura, vloge in odgovornosti posameznikov;
- politika, cilji in strategije ki so realno zastavljene;
- zmogljivosti, ki se razumejo pod pojmom sredstev in znanja (npr. kapital, čas, ljudje, procesi, sistemi in tehnologije);
- informacijski sistemi, pretok informacij in procesi odločanja (formalni in neformalni);
- odnosi, dojemanje in vrednotenje notranjih zainteresiranih strani;
- organizacijska kultura;
- standardi, navodila in modeli privzeti s strani organizacije; ter
- oblika in obseg pogodbenih razmerij.

Komunikacija in posvetovanje

Stalni in ponavljajoči se procesi, ki jih vodi organizacija, da zagotavlja, deli in pridobiva informacije, ter da se vključi v dialog z *deležniki* v zvezi z obvladovanjem *tveganj*.

Opomba 1 Informacije se lahko nanašajo na obstoj tveganj, njihovo naravo, obliko, *verjetnost*, pomen, vrednost, sprejemljivost ter na siceršnjo obravnavo tveganj.

Opomba 2 Posvetovanje je dvosmerni proces informirane komunikacije med organizacijo in zunanjimi vlagatelji v zvezi z odločitvijo ali determiniranjem usmerjenosti glede te odločitve.

Posvetovanje je:

- proces, ki vpliva na odločitev s pomočjo vpliva (raje kot moči) in
- prispevek k odločanju (vendar pa to ni skupno odločanje).

Interesna skupina

Oseba ali organizacija, ki lahko vpliva, sama čuti vpliv, ali pa sama zazna odločitev ali aktivnost.

Deležnik je lahko tisti, ki sprejema odločitve.

Ocenjevanje tveganja (Risk Assesment)

Proces, ki združuje *prepoznavanje* (Risk Identification), *analizo* (Risk Analysis) in *vrednotenje* (Risk Evaluation) tveganj.

Prepoznavanje tveganja (Risk Identification)

Proces iskanja, prepoznavanja in opisovanja *tveganja*.

Opomba 1 Identifikacija tveganja vključuje identifikacijo *virov tveganja*, *dogodkov*, njihovih namenov in potencialnih *posledic*.

Opomba 2 Identifikacija tveganja lahko vključuje zgodovinske podatke, teoretične analize, informacijska mnenja in mnenja specialistov ter potrebe *vlagateljev*.

Vir tveganja

Element, ki lahko sam ali v kombinaciji z drugimi določi od kod izvira *tveganje*. Vir tveganja je lahko oprijemljiv ali neoprijemljiv.

Dogodek

Pojav ali sprememba določenega sklopa okoliščin.

Opomba 1 Dogodek je lahko en ali več pojavov, in lahko ima več namenov.

Opomba 2 Dogodek je lahko sestavljen iz nečesa, kar se dejansko ne dogaja.

Opomba 3 Dogodek je lahko včasih naslovljen kot "incident" ali "nesreča".

Opomba 4 Dogodek brez *posledic* se lahko imenuje tudi, "nevaren pojav", "incident", škorajšnji zadetek", "tesen izid".

Posledice

Rezultat *dogodka*, ki vpliva na cilje.

Opomba 1 Dogodek lahko privede do različnih posledic.

Opomba 2 Posledice so lahko določene ali nedoločene in imajo pozitivne ali negativne učinke na cilje.

Opomba 3 Posledice so lahko izražene kvalitativno ali kvantitativno.

Opomba 4 Začetne posledice se lahko stopnjujejo do verižne reakcije.

Verjetnost (Likelihood)

Verjetnost, da se bo nekaj zgodilo.

Opomba 1 V terminologiji upravljanja tveganj je beseda verjetnost (likelihood) uporabljena kot možnost, da se nekaj zgodi, kar je lahko definirano, izmerjeno, determinirano, subjektivno ali objektivno, kvalitativno ali kvantitativno. Opisana je z uporabo splošnih matematičnih terminov.

Opomba 2 »Likelihood« v drugih jezikih nima sopomenke, zato se uporablja tudi »probability«. V angleščini je »probability« dostikrat uporabljan kot ozek matematični pojem. V tej terminologiji je torej »likelihood« izraz, ki zajema enako obsežnost kot »probability« v drugih jezikih.

Profil tveganja

Opisi celote *tveganj*.

Opomba Celota tveganj zajema tista tveganja, ki se nanašajo na celotno organizacijo, del organizacije ali je definirana kako drugače.

Analiza tveganja (Risk Analysis)

Proces razumevanja narave *tveganja* in določitve *stopnje tveganja*.

Opomba 1 Analiza tveganja predstavlja osnovo za *vrednotenje tveganja*, na tej podlagi pa odločitev glede morebitnega *obravnavanja tveganja*.

Opomba 2 Analiza tveganja se zaključi z vrednotenjem tveganja.

Vrednotenje tveganja (Risk Evaluation)

Naloge, s katerimi ocenimo pomen *tveganja*.

Opomba 1 Vrednotenje tveganja temelji na osnovi organizacijskih ciljev in *notranjega* ter *zunanjega okvira*.

Opomba 2 Vrednotenje tveganja mora izhajati iz standardov, zakonov, politike in drugih zahtev.

Nivo tveganja

Obseg *tveganja* ali kombinacije tveganj, izražene v kombinacijah *posledic* in njihovih *verjetnosti*.

Ocena tveganja (Risk Assesment)

Proces primerjanja rezultatov z *analizo tveganja* in *vrednotenjem tveganja*, da ugotovimo ali je *tveganje* in njegov obseg sprejemljiv.

Opomba Ocena tveganja pomaga pri odločitvi glede obravnavanja tveganja.

Obravnava tveganja (Risk Treatment)

Proces za modificiranje *tveganj*.

Opomba 1 Obravnava tveganj lahko pomeni:

- izogniti se tveganju tako, da ne začnemo ali ne nadaljujemo aktivnosti, ki tveganje povzroča;
- povečanje tveganja za priložnost;
- odpraviti *vir tveganja*;
- spremeniti *verjetnost* dogodka;
- spremeniti *posledice* dogodka;
- deliti tveganje z drugimi pogodbeniki (vključujoč pogodbe in rizično financiranje); in/ali
- s premišljenimi odločitvami ohraniti tveganje.

Opomba 2 Obravnave tveganj, ki se ukvarjajo z negativnimi posledicami, se včasih nanašajo na blaženje tveganja, odpravljanje tveganja in zmanjšanje tveganja.

Opomba 3 Obravnava tveganj lahko ustvari tudi nova tveganja ali modificira obstoječa tveganja.

Nadzor (Supervision)

Ukrep, ki spreminja/modificira *tveganje*.

Opomba 1 Nadzor vključuje vse procese, politiko, naprave, prakse in druge akcije za modificiranje tveganja.

Opomba 2 Nadzor ne izvaja vedno namenjenega modifikacijskega učinka.

Preostalo tveganje (Residual Risk)

Tveganje, ki ostane po *obravnavi tveganja*.

Opomba 1 Preostalo tveganje lahko vsebuje nedefinirano tveganje.

Opomba 2 Preostalo tveganje je lahko znano kot zadržano tveganje.

Spremljanje (Monitoring)

Konstantno preverjanje, nadzor, kritično opazovanje in definiranje statusa, da bi se definirala pričakovana in želena sprememba.

Opomba Spremljanje/monitoring se lahko aplicira v *okvir upravljanja tveganja*, v *proces upravljanja tveganja*, v *tveganje* ali v *kontrolo*.

Pregled (Review)

Dejavnost za zagotavljanje primernosti, učinkovitosti in ustreznosti predmeta za dosego postavljenih ciljev.

Opomba Pregled se lahko aplicira v *okvir upravljanja tveganja*, v *proces upravljanja tveganja*, v *tveganje* ali v *kontrolo*.

6.1.3 Principi

Organizacija naj bi za učinkovito upravljanje tveganj na vseh nivojih upoštevala naslednje principe:

1. **Upravljanje tveganj ustvarja in ščiti vrednost.** Dokazljivo prispeva k doseganju ciljev in izboljšanju učinkovitosti, kot je to v primeru človeškega zdravja in varnosti, zaščiti vseh vrst, pri usklajevanju s pravnimi predpisi, javnemu odobravanju, zaščiti okolja, kvaliteti proizvodov, projektnemu managementu, učinkovitosti pri poslovanju, upravljanju in ugledu.

2. **Upravljanje tveganj je sestavni del vseh procesov v organizaciji.** Upravljanje tveganj ne predstavlja samostojne aktivnosti, ki je ločena od glavnih aktivnosti in procesov organizacije. Upravljanje tveganj je del odgovornosti celotnega managementa in glavni del vseh organizacijskih procesov, vključno s strateškim planiranjem ter s procesi upravljanja projektov in procesi uvajanja sprememb.

3. **Upravljanje tveganj je sestavni del odločanja.** Upravljanje tveganj pomaga odločevalcem, da se ozaveščeno odločajo glede ukrepov in razlikujejo med alternativnimi postopki načinov delovanja.

4. **Upravljanje tveganj izrecno obravnava negotovost.** Upravljanje tveganj izrecno upošteva negotovost, naravo negotovosti in način, s katerim jo je mogoče obravnavati.

5. **Upravljanje tveganj je sistematično, strukturirano in pravočasno.** Sistematičen, pravočasen in strukturiran pristop k upravljanju tveganj prispeva k učinkovitosti in doslednim, primerljivim in zanesljivim rezultatom.

6. **Upravljanje tveganj temelji na najboljših informacijah, ki jih je mogoče pridobiti.** Vložek v proces upravljanja tveganj temelji na informacijskih virih kot so: zgodovinski podatki, izkušnje, odziv deležnikov, opazovanja, napovedi in strokovna presoja. Vendar pa bi se morali odločevalci pozanimati glede dostopnosti in primernosti podatkov ter upoštevati morebitne omejitve glede te dostopnosti, načina modeliranja ali možnosti razhajanja mnenj različnih strokovnjakov.

7. **Upravljanje tveganj je prilagojeno.** Upravljanje tveganj je potrebno prirediti glede na notranji in zunanji kontekst organizacije ter glede na vrsto tveganj.

8. **Upravljanje tveganj upošteva kulturne in človeške faktorje.** Z upravljanjem tveganj prepoznamo sposobnost, dojemanje in namene zunanjih in notranjih ljudi, ki lahko pospešijo ali zavirajo doseganje ciljev organizacije.

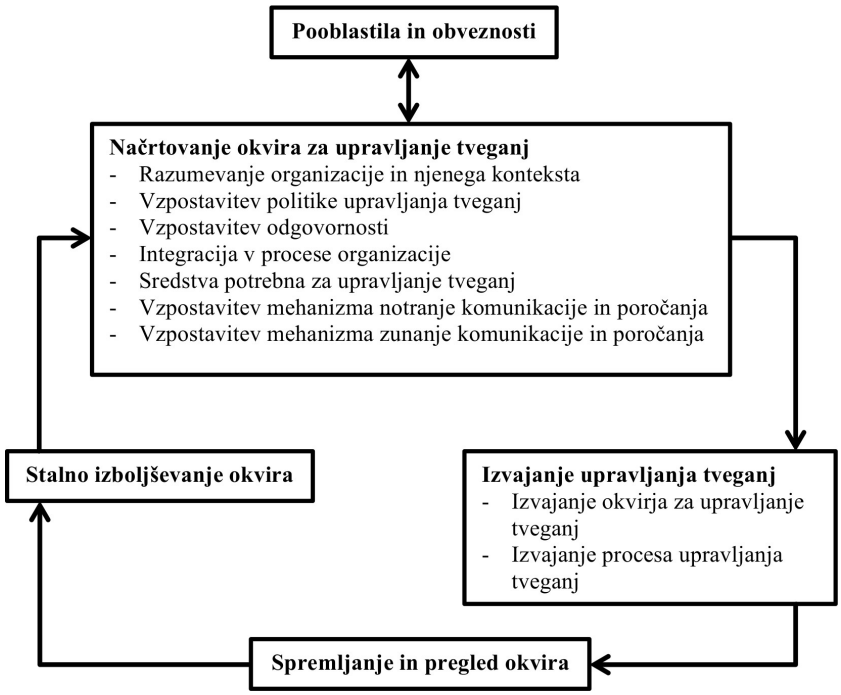
9. **Upravljanje tveganj je pregledno in neizključujoče.** Upravljanje tveganj vključuje različne deležnike in upravljavce na vseh nivojih organizacije. Primerna in pravočasna vključitev deležnikov in še posebej odločevalcev na vseh nivojih organizacije zagotavlja, da upravljanje tveganj ostaja vselej pomembno in posodobljeno. Vključitev deležnikov dovoljuje, da so primerno zastopani in da so njihova mnenja upoštevana pri določanju kriterijev glede tveganj.

10. **Upravljanje tveganj je dinamično, ponavljajoče se in sposobno odziva na spremembe.** Upravljanje tveganj nenehno zaznava in se odziva na spremembe. Ko se zgodijo zunanji in notranji dogodki, se spremeni kontekst in znanje, potekata spremljanje in pregled tveganja, lahko se pojavi novo tveganje, lahko se neko tveganje spremeni, lahko pa celo izgine.

11. **Upravljanje tveganj spodbuja in omogoča neprestano izboljševanje organizacije.** Organizacija bi morala razviti in izvajati strategije za izboljševanje zrelosti upravljanja tveganj, vzporedno z vsemi ostalimi vidiki v organizaciji.

6.1.4 Okvir

Uspeh obvladovanja tveganja je odvisen od učinkovitosti okvira upravljanja, ki zagotavlja temelje in ureditve, ki so vgrajeni v celotno organizacijo na vseh ravneh. Poleg tega okvir zagotavlja, da se informacije o tveganjih, ki nastanejo v procesu upravljanja tveganj, ustrezno sporočajo in uporabljajo kot osnova za odločanje in vzpostavitev odgovornosti na vseh ravneh



Slika 6.2: Relacije med komponentami okvira upravljanja tveganj [18]

organizacije. Slika 6.2 prikazuje okvir, iz katerega je mogoče razbrati, da se njegovi posamezni deli povezujejo na interaktiven način. Elementi slike 6.2 so zajeti tudi v sliki 6.1.

Okvir ni namenjen temu, da bi predpisoval samostojen sistem upravljanja, temveč je bolj v pomoč organizaciji pri integraciji sistema upravljanja tveganj v vsesplošen sistem upravljanja neke organizacije.

Pooblastila in obveznosti

Za vzpostavitev upravljanja tveganj in za zagotavljanje stalne učinkovitosti tega upravljanja so potrebna trdna in trajna prizadevanja vodstva organizacije kot tudi strateško in dosledno načrtovanje za doseganje zavezanosti

na vseh ravneh organizacije. Vodstvo organizacije naj bi:

1. definiralo in podpiralo politiko upravljanja tveganj;
2. zagotovilo, da je politika upravljanja tveganj v sozvočju z organizacijsko kulturo;
3. določilo kazalnike uspešnosti upravljanja tveganj, ki so v sozvočju s kazalniki uspešnosti organizacije;
4. uskladilo cilje upravljanja tveganj s cilji in strategijami organizacije;
5. zagotovilo skladnost z zakoni;
6. dodelilo pooblastila in odgovornosti na vseh ravneh organizacije;
7. zagotovilo potrebna sredstva za upravljanje tveganj;
8. izmenjevalo informacije o novostih, idejah in prednostih obvladovanja tveganj z vsemi deležniki; in
9. zagotovljalo primernost in učinkovitost okvira za upravljanje tveganj.

Oblikovanje okvira za upravljanje tveganj

Razumevanje organizacije in njenega konteksta Še pred začetkom načrtovanja in implementacijo okvira za upravljanje tveganj je pomembno oceniti in razumeti notranji in zunanji kontekst, v katerem organizacija živi. Oboje lahko pomembno vpliva na oblikovanje okvira.

Ocenjevanje organizacijskega zunanjega konteksta lahko vključuje, ni pa nujno omejeno na:

1. socialno in kulturno, politično, pravno, finančno, tehnološko, ekonomično, naravno in konkurenčno okolje, bodisi internacionalno, nacionalno, regionalno ali lokalno okolje;

2. ključne dejavnike in trende, ki vplivajo na cilje organizacije; in
3. odnose z zunanjimi deležniki, njihovo dojemanje ter vrednote.

Ocenjevanje organizacijskega notranjega konteksta lahko vključuje, ni pa nujno omejeno na:

1. upravljanje, organizacijsko strukturo, vloge in odgovornosti;
2. politiko, cilje in strategije, ki so namenjene za doseganje le-teh;
3. zmogljivosti v smislu virov in znanja (kapital, čas, ljudje, procesi, sistemi in tehnologije);
4. informacijske sisteme, informacijske tokove in odločitvene procese (formalne in neformalne);
5. odnos z notranjimi deležniki, njihovo dojemanje ter vrednote;
6. organizacijsko kulturo;
7. standarde, navodila in modele, ki jih organizacija uporablja; ter
8. oblikovanje in razširitev pogodbenih odnosov.

Vzpostavitev politike upravljanja tveganj Politika upravljanja tveganj mora jasno opredeliti cilje organizacije in njeno zavezanost k politiki upravljanja tveganj, ki običajno vključuje:

1. organizacijsko utemeljitev glede obvladovanja tveganj;
2. povezave med organizacijskimi cilji in politiko ter politiko upravljanja tveganj;
3. obveznosti in odgovornosti glede upravljanja tveganj;

4. način, ki ga organizacija uporablja pri reševanju navzkrižnih interesov;

5. prizadevanje za omogočanje potrebnih virov oziroma informacij tistim, ki so odgovorni za upravljanje tveganj;

6. definiranje načina, s katerim bo tveganje izmerjeno in sporočeno; ter

7. stremljenje k temu, da se bo politika upravljanja tveganj ves čas razvijala ter da bo ta politika vedno odgovorila na nek dogodek oziroma spremembo okoliščin.

Politiko obvladovanj tveganj je treba sporočati ustrezno.

Odgovornost Organizacija mora zagotoviti odgovornost, potrebno avtoriteto in kompetence za upravljanje tveganj ter vzpostavitev in vzdrževanje procesa upravljanja tveganj. Vzpostavitev odgovornosti vključuje tudi ustrezne in učinkovite kontrole. Pri tem je med najpomembnejšimi:

1. identificiranje lastnikov tveganja, ki imajo odgovornost in ustrezno avtoriteto, potrebno pri obvladovanju tveganj;

2. identificiranje odgovornih za razvoj, izvedbo in trajnost okvira za upravljanje tveganj;

3. identificiranje vseh ostalih odgovornosti posameznikov v organizaciji, saj lahko to pomaga pri obvladovanju tveganj;

4. vzpostavitev meritev učinkovitosti ter zunanjih in/ali notranjih procesov poročanja; in

5. zagotavljanje ustrezne ravni priznavanja.

Integracija v vse procese organizacije Integracija v procese organizacije mora biti izvedena tako, da je upravljanje tveganj ustrezno, učinkovito in uspešno. Upravljanje tveganj mora biti del posameznih procesov in ne sme biti od njih oddvojeno. Zlasti je treba upravljanje tveganj integrirati v razvoj politik, v poslovno in strateško načrtovanje in pregled, ter v postopke uvajanja sprememb.

Potreben je načrt za upravljanje tveganj celotne organizacije, da se zagotovi, da se politika upravljanja tveganj izvaja in je vgrajena v vse postopke in procese organizacije. Načrt za upravljanje tveganj se lahko vključi v druge organizacijske načrte podobno kot strateški načrt.

Sredstva Organizacija mora zagotoviti potrebna sredstva za upravljanje tveganj. Med temi sredstvi so:

1. ljudje, znanje, veščine, izkušnje in kompetence;
2. sredstva, potrebna za vsak korak v procesu upravljanja tveganj;
3. postopki, orodja in metode organizacije, ki se uporabljajo za upravljanje tveganj;
4. dokumentirani procesi in postopki;
5. informacijski sistemi in sistemi za upravljanje znanja; ter
6. programi izobraževanj oziroma usposabljanj.

Vzpostavitev sistema notranje komunikacije in mehanizmov poročanja Organizacija bi morala v podporo in povečanje odgovornosti ter lastništva tveganja vzpostaviti notranje komuniciranje in poročevalne mehanizme. Ti mehanizmi naj bi zagotavljali, da:

1. so glavne komponente okvira upravljanja tveganj in vse nadaljnje modifikacije tega okvira ustrezno posredovane;

2. obstaja ustrezno notranje poročanje glede okvira, predvsem glede njegove učinkovitosti in rezultatov;

3. so vse relevantne informacije, ki izhajajo iz upravljanja tevganj, na voljo na primernem nivoju in pravočasno; ter da

4. so vzpostavljeni procesi za posvetovanje z notranjimi deležniki.

Ti mehanizmi bi morali, kjer je to primerno, vključevati procese za utrditev informacij glede tveganj, ki prihajajo iz različnih virov, ter po potrebi obravnavati njihovo občutljivost.

Vzpostavitev sistema zunanje komunikacije in mehanizmov poročanja Organizacija bi morala razviti in implementirati načrt, kako bo komunicirala z zunanjimi deležniki. To vključuje:

1. vključevanje primernih zunanjih deležnikov in zagotavljanje učinkovite izmenjave informacij;

2. zunanje poročanje v skladu z zakonskimi in regulativnimi zahtevami;

3. zagotavljanje povratnih informacij in poročanje o komunikaciji in posvetovanju;

4. uporabljanje komunikacije za izgradnjo zaupanja v organizaciji; in

5. komuniciranje z deležniki v primeru nepredvidene krize.

Ti mehanizmi bi morali, kjer je to primerno, vključevati procese za utrditev informacij glede tveganj, ki prihajajo iz različnih virov, ter po potrebi obravnavati njihovo občutljivost.

Implementacija upravljanja tveganj

Implementacija okvira upravljanja tveganj Implementacja okvira za upravljanje tveganj pomeni, da mora organizacija predvsem:

1. določiti pravilen rok in strategijo za izvedbo;
2. uporabjati politiko in proces upravljanja tveganj vzporedno s procesi organizacije;
3. izpolniti zakonske in regulativne zahteve;
4. zagotoviti, da so odločitve, vključno z razvojem in določanjem ciljev, usklajene z rezultati procesov upravljanja tveganj;
5. imeti informacije in zagotavljati izobraževanja in usposabljanja; ter
6. razpravljati in se posvetovati z deležniki, da ostane okvir upravljanja tveganj primeren.

Implementacija procesa upravljanja tveganj Upravljanje tveganj je potrebno izvesti z zagotovilom, da se proces upravljanja tveganj uresničuje preko načrta za upravljanje tveganj na vseh ustreznih ravneh in funkcijah organizacije kot del njenih standardnih postopkov in procesov. Proces bo podrobneje opisan v naslednjem razdelku.

Spremljanje in pregled okvira

Za zagotavljanje učinkovitega upravljanja tveganj, ki vseskozi prispeva k učinkovitosti organizacije, je potrebno spremljanje in pregled okvira. V ta namen mora organizacija:

1. meriti prisotnost upravljanja tveganj s pomočjo kazalnikov ter redno pregledovati njihovo ustreznost;
2. redno meriti napredek v smislu približevanja ali odklona od načrta upravljanja tveganj;
3. redno pregledovati, ali so okvir upravljanja tveganj, politika in načrt še vedno ustrezni glede na zunanji in notranji kontekst organizacije;

4. poročati o tveganjih, napredku glede uresničevanja načrta upravljanja tveganj ter o tem, kako dosledno se politika upravljanja tveganj zpolnjuje; in

5. pregledati učinkovitost okvira upravljanja tveganj.

Nenehno izboljševanje okvira

Rezultat spremljanja in pregledovanja okvira je stalno izboljševanje okvira, politik in načrta upravljanja tveganj. Odločitve glede tega se izvajajo zato, da se upravljanje tveganj organizacije izboljšuje, prav tako pa tudi njena kultura upravljanja tveganj.

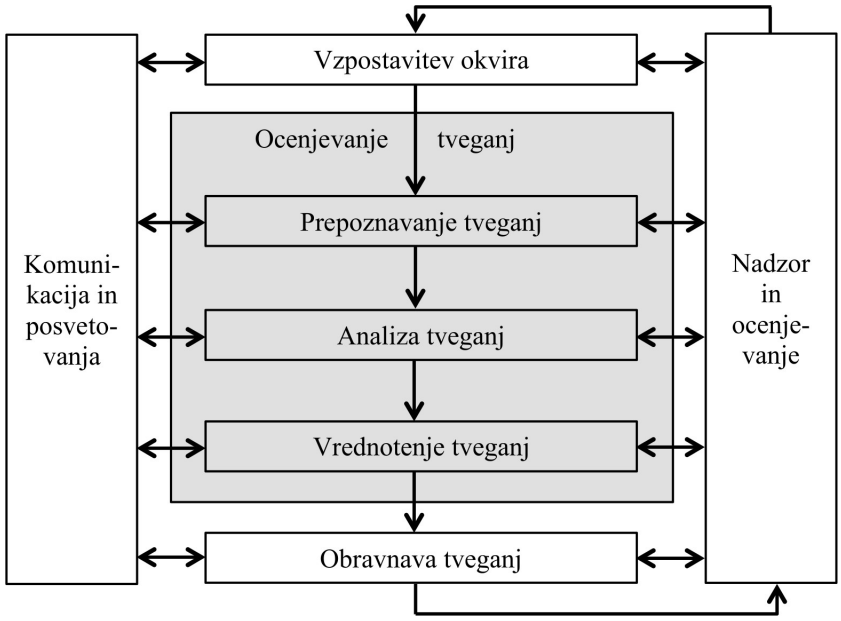
6.1.5 Proces

Proces sestavljajo aktivnosti, ki jih prikazuje slika 6.3. Za proces veljajo naslednje tri splošne usmeritve, ki jih moramo upoštevati pri vseh aktivnostih procesa. Te usmeritve so:

1. Upravljanje tveganj mora biti sestavni del upravljanja organizacije. To pomeni, da tveganja ne zahtevajo niti ne smejo biti posebni del upravljanja, s katerim se poslovodstvo ukvarja ob posebnih priložnostih (na primer enkrat letno).

2. Upravljanje tveganj mora biti del vsesplošne kulture v organizaciji in v praksah, ki se dnevno izvajajo. Seveda pa je prejšnja alineja predpogoj za doseganje te usmeritve.

3. Ker je vsaka organizacija posebna in unikatna, in ker se s časom vsaka organizacija tudi spreminja, je potrebno upravljanje tveganj prilagoditi posebnostim organizacije in ga s časom tudi dodatno dopolnjevati ali kako drugače spreminjati.



Slika 6.3: Aktivnosti procesa upravljanja tveganj in njihove medsebojne relacije [18]

Komunikacija in posvetovanje

Ker sta komunikacija in posvetovanje z notranjimi in zunanjimi deležniki organizacije nujno potrebnI aktivnosti skozi celoten proces upravljanja tveganj, je potrebno razviti načrte za te aktivnosti in vzpostaviti mehanizme za delo v skladu s temi načrti že povsem na začetku. Posvetovalni timski pristop lahko pomaga:

1. vzpostaviti ustrezen okvir;
2. zagotoviti, da so interesi razumljeni in upoštevani;
3. pripeljati strokovnjake za analizo tveganj;
4. zagotoviti različne poglede, katere je potrebno ustrezno razumeti;
5. zagotoviti potrditev in podporo; ter
6. izboljšati ustrezno uvajanje sprememb v proces upravljanja tveganj.

Komunikacija je pomembna, saj se tako presojajo možnosti tveganj glede na njihovo percepcijo. Te zaznave pa so lahko različne in odvisne od vrednot, potreb, predpostavk, konceptov itd. deležnikov. Ker imajo njihova stališča pomemben vpliv na odločitve, morajo biti vse te zaznave deležnikov prepoznane, evidentirane ter upoštevane pri procesu odločanja.

Vzpostavitev okvira

Z vzpostavitvijo okvira organizacija artikulira svoje cilje, definira notranje in zunanje parametre, ki jih je potrebno upoštevati med upravljanjem tveganj, ter definira obseg in kriterije za preostali del procesa upravljanja tveganj. Pri tem ločimo med vzpostavitvijo notranjega in zunanjega okvira ter vzpostavitvijo okvira za sam proces upravljanja tveganj.

Zunanji kontekst predstavlja zunanje okolje, v katerem organizacija skuša dosegati svoje cilje. Ta kontekst je pomemben zato, da lahko upoštevamo cilje zunanjih deležnikov pri razvoju kriterijev za tveganja. Temelji na kontekstu celotne organizacije, vendar s posebnimi podrobnostmi glede zakonskih in regulativnih zahtev, dojemanjem deležnikov in drugih vidikov tveganj, ki so značilna za področje procesa upravljanja tveganj. Vsebuje pa lahko:

1. socialno, kulturno, politično, finančno, tehnološko, ekonomsko in naravno okolje, bodisi internacionalno, nacionalno, regionalno ali lokalno okolje;
2. ključne dejavnike in trende, ki vplivajo na cilje organizacije; ter
3. odnose z zunanjimi deležniki, njihovo dojemanje ter vrednote.

Po drugi strani notranji kontekst predstavlja notranje okolje, v katerem organizacija skuša dosegati svoje cilje. Proces upravljanja tveganj mora biti skladen s kulturo organizacije, ostalimi procesi, strukturo in strategijo. Notranji kontekst je vse tisto znotraj organizacije, kar vpliva na način upravljanja tveganj. Vzpostaviti ga je potrebno ker:

1. upravljanje tveganja poteka v okviru ciljev organizacije;
2. je potrebno cilje in merila določenega projekta, procesa ali dejavnosti obravnavati v luči ciljev organizacije kot celote; in ker
3. nekatere organizacije ne morejo prepoznati priložnosti, da dosežejo svoje strateške, projektne ali poslovne cilje, kar vpliva na organizacijsko pripadnost, verodostojnost, zaupanje in vrednost.

Notranji kontekst je potrebno razumeti, to razumevanje pa lahko vključuje:

1. upravljanje, organizacijske strukture, vloge in odgovornosti;

2. usmeritve, cilje in strategije, ki so na voljo za njihovo doseganje;
3. zmogljivosti v smislu virov in znanja (npr. kapitala, časa, ljudi, procesov, sistemov in tehnologij);
4. odnos z notranjimi deležniki, njihovo dojemanje ter vrednote;
5. organizacijsko kulturo;
6. informacijske sisteme, informacijske tokove in odločitvene procese (formalne in neformalne);
7. standarde, navodila in modele, ki jih organizacija uporablja; ter
8. oblikovanje in razširitev pogodbenih odnosov.

Vzpostaviti oziroma določiti je potrebno cilje, strategije, področja uporabe in parametre dejavnosti organizacije, ali tiste dele organizacije, kjer se uporablja postopek upravljanja tveganja. Upravljanje tveganj je treba opraviti na način, da bi upravičili sredstva, ki so namenjena upravljanju tveganj. Prav tako je potrebno opredeliti sredstva, odgovornosti in pooblastila ter evidence, ki se vodijo.

Kontekst procesa upravljanja tveganj se lahko tudi spremeni glede na potrebe organizacije. Ta sprememba lahko vključuje:

1. opredelitev ciljev in dejavnosti upravljanja tveganj;
2. opredelitev odgovornosti v procesu upravljanja tveganj;
3. opredelitvi področja, kot tudi obseg aktivnosti za upravljanje tveganj, ki se izvajajo;
4. opredelitev dejavnosti, procesa, funkcije, projekta, izdelka, storitve ali sredstev v smislu časa in lokacije;

5. opredelitev odnosov med konkretnimi projekti, procesi ali dejavnostmi in drugimi projekti, procesi ali dejavnostmi organizacije;
6. opredelitev metodologij za oceno tveganja;
7. opredelitev načinov ocenjevanja uspešnosti in učinkovitosti znotraj upravljanja tveganja;
8. prepoznavanje in določanje odločitev, ki jih je potrebno sprejeti; ter
9. ugotavljanje potreb po študijah, določanje njihovega obsega in ciljev ter sredstev, potrebnih za takšne študije.

Organizacija mora definirati tudi kriterije, ki jih uporabljamo pri ovrednotenju pomembnosti posameznih tveganj. Ti kriteriji odsevajo vrednostne sisteme, cilje in vire neke organizacije. Nekateri od teh kriterijev so lahko pridobljeni na osnovi zakonskih, drugih regulativih in pogodbenih zahtev. Kriteriji tveganja bi morali biti v skladu s politiko upravljanja tveganj v organizaciji, opredeljeni na začetku vsakega procesa upravljanja tveganj ter jih je potrebno nenehno pregledovati. Pri določanju kriterijev tveganj, je treba upoštevati dejavnike, ki vključujejo:

1. naravo in vrsto vzrokov ter posledic, ki se lahko pojavijo, in način, kako se merijo;
2. inforamcijo, kako bo definirana verjetnost;
3. časovni(e) rok/e verjetnosti in/ali posledica(e);
4. informacijo, kako naj bo določena stopnja tveganja,
5. stališča deležnikov;
6. raven, do katere je tveganje sprejemljivo oziroma dopustno; ter
7. informacijo, ali je potrebno upoštevati kombinacije različnih tveganj, in če je tako, kako in katere kombinacije je potrebno upoštevati.

Ocenjevanje tveganj

Aktivnost ocenjevanja tveganj predstavlja srčiko upravljanja tveganj in predstavlja skupno ime za aktivnosti prepoznavanja, analizo in vrednotenje tveganj.

Pri ocenjevanju tveganj skušamo med drugim odgovoriti na naslednja temeljna vprašanja, ki se zastavljajo v zvezi tveganj:

1. Kaj se lahko zgodi in zakaj?
2. Kakšne so posledice?
3. Kakšna je verjetnost, da se tveganje pojavi v prihodnosti?
4. Ali obstajajo kakšni dejavniki, ki omogočajo, da se nekemu tveganju izognemo ali da zmanjšamo verjetnost, da se sploh pojavi?

Prepoznavanje/identificiranje tveganj

Organizacija mora opredeliti vire tveganj, področja vplivov, dogodke, ki so posledica nekega pojava ali spremembe določenega položaja, z vzroki in s potencialnimi posledicami, ki se lahko s časom tudi spreminjajo. Osnovni namen te aktivnosti (ali koraka v procesu) je ustvariti celovit seznam tveganj, ki bazira na tistih dogodkih, ki lahko ustvarijo, povečajo, onemogočijo, zmanjšajo, pospešijo ali upočasnijo doseganje ciljev. Celovito prepoznavanje je kritično, saj tveganje, ki ni identificirano v tem koraku, ne bo del nadaljnje analize. Zajeta morajo biti tudi tista tveganja, katerih vzrok ni nujno pod kontrolo organizacije, ali pa sploh ni znan. Upoštevati je potrebno tudi posebne učinke posledic (kumulativni učinki in kaskade) ter najrazličnejše možne vzroke in posledice, s pomočjo katerih se nato oblikujejo možni scenariji. Pri prepoznavanju tveganj si mora organizacija pomagati z različnimi orodji in tehnikami, vključene pa morajo biti tudi ustrezne podporne informacije ter ljudje z ustreznim znanjem.

Analiza tveganj

Pri analizi tveganj razvijemo razumevanje tveganja. Ta aktivnost je pogoj za vrednotenje tveganj in za odločitev o tem, ali naj se s tveganjem sploh ukvarjamo, in če se naj, katere najustreznejše strategije in metode bi bile primerne. Prav tako je ta aktivnost pogoj za odločanje o tem, kje v organizaciji se je potrebno posvetiti tveganjem in katere opcije (viri, področja vplivov, dogodki, posledice, itd.) vsebujejo različne vrste tveganj ter na kakšnem nivoju (poslovnem, tehničnem, itd.) je neko tveganje.

Pri analizi ugotavljamo vzroke in izvore tveganj, pozitivne in negativne posledice ter možnosti, da se zgodijo posledice (ponavadi predstavljene z verjetnostjo za dogodek). Iščemo faktorje, ki vplivajo na posledice, in možnosti za posledice. Upoštevamo, da lahko ima nek dogodek množico posledic, ki lahko vplivajo na množico ciljev organizacije. Upoštevamo pa tudi obstoječe kontrole in njihovo učinkovitost oziroma uspešnost.

S pomočjo načina, s katerim so posledice in verjetnosti izražene, in s pomočjo načina, ki določa stopnjo tveganja, se določi vrsta tveganja, informacije, ki so na voljo, ter namen, za katerega je rezultat ocenjevanja tveganja uporabljen. Vse pa mora biti v skladu s kriteriji tveganj.

Pri analizi tveganj je mogoče uporabiti različne stopnje podrobnosti, odvisno od tveganja, namena analize, ter informacij, podatkov in virov, ki so na voljo. Analiza je lahko kvalitativna, delno kvantitativna ali delno kvantitativna, ali pa kombinacija obeh načinov – odvisno od okoliščin.

Posledice in njihova verjetnost se lahko določijo z modeliranjem rezultatov dogodka ali niza dogodkov, z ekstrapolacijo iz eksperimentalnih študij, ali z analizo razpoložljivih podatkov. Posledice se lahko izrazi v smislu materialnih in nematerialnih učinkov. Lahko so izražene z večimi numeričnimi vrednostmi ali opisi, za različne čase, prostore, skupine in situacije.

Vrednotenje tveganj

Namen vrednotenja je pomoč pri sprejemanju odločitev. Temelji na analizi tveganj glede prioritet ravnanja s tveganji. Pri tem posamezno tveganje primerjamo s kriteriji sprejemljivosti, ki smo jih določili v aktivnosti vzpostavitve okvira, na podlagi rezultatov primerjave pa se nato določi način obravnave tveganja, ki mora biti v skladu z zakonskimi, regulativnimi in drugimi zahtevami.

V nekaterih primerih lahko ocena tveganja vodi v odločitev, da je potrebna dodatna analiza, ali pa v odločitev, da se tveganje obravnava samo zato, da se obdržijo obstoječe kontrole. Seveda pa je to odvisno od odnosa organizacije do tveganja ter kriterijev tveganj.

Obravnava tveganj

V okviru obravnave tveganj (v dobesednem prevodu bi lahko rekli tudi v "okviru zdravljenja tveganj") izbiramo eno ali več možnosti za spreminjanje tveganj in te možnosti tudi implementiramo. Po implementaciji obravnave tveganj zagotovimo ali spremenimo kontrole.

Sama aktivnost vsebuje manjši cikličen proces, ki zajema:

1. ocenjevanje tveganja;
2. odločanje o sprejemljivosti preostalega (residual risk) tveganja;
3. ponovno obravnavavo tveganja, če preostanek ni sprejemljiv; in
4. ocenjevanje uspešnosti te obravnave.

Možnosti obravnave tveganj niso nujno medsebojno izključujoče ali ustrezne v vseh okoliščinah. Možnosti so lahko:

1. izogibati se tveganjem tako, da se organizacija odloči, da ne začne ali ne nadaljuje aktivnosti, ki bi povečala to tveganje;

2. tveganje sprejeti ali celo povečati, da bi izkoristili priložnost;
3. odstraniti vzrok tveganja;
4. spremeniti verjetnost;
5. spremeniti posledice;
6. deliti tveganje s partnerjem/i (pogodbe, finančna tveganja); ter
7. ohranjati tveganje na premišljen način s premišljenimi odločitvami.

Pri izbiri najustreznejših možnosti za obravnavo tveganj tehtamo med vloženimi stroški in napori glede na koristi, upoštevaje zakonske in druge predpise, kot so družbena odgovornost in varstvo okolja. Odločitev je odvisna tudi od tega, ali je obravnava finančno upravičena, kot je to v primeru visoke stopnje negativne/ih posledic(e) z nizko verjetnostjo pojava dogodka.

Med obravnavo se osredotočimo tako na posamezno možnost, kakor tudi na kombinacijo različnih možnosti, pri čemer lahko ima organizacija veliko koristi.

Pri izbiri možnosti obravnave tveganja, mora organizacija upoštevati vrednote in dojemanje deležnikov in najprimernejše načine za komunikacijo z njimi. Tu gre predvsem za diskusijo glede tega, kako lahko možnosti obravnave tveganja vplivajo na druga tveganja v organizaciji ali z deležniki. Nekatere obravnave tveganj so namreč lahko bolj sprejemljive za nekatere deležnike kot za druge.

V načrtu obravnave je potrebno jasno opredeliti prednostni vrstni red, v katerem naj bi se izvajale posamezne obravnave tveganj.

Obravnava tveganj sama po sebi vsebuje tveganja. Eno najpomembnejših tveganj je tveganje, da sprejmemo neučinkovite ukrepe, ali da ti odpovedo. Zato je potrebno obravnavo tveganj stalno spremljati in pregledovati, da na ta način zagotavimo učinkovitost ukrepov.

Obravnava tveganj lahko privede do sekundarnih tveganj, ki jih je treba oceniti, obravnavati, spremljati in pregledovati. Ta sekundarna tveganja je treba vključiti v isti načrt obravnave kot primarno tveganje in se ne obravnavajo kot nova tveganja, pri tem pa mora biti povezava med primarnim in sekundarnim tveganjem jasna in trajna.

Namen načrtovanja obravnave tveganj je dokumentirati, kako bo posamezna izbrana možnost obravnave izvedena. Informacije, navedene v načrtu obravnave, morajo vsebovati:

1. razlog izbora možnosti, vključno s pričakovanimi koristmi, ki jih prinaša ta možnost;

2. imena odgovornih za odobritev načrta, in imena odgovornih za njegovo izvedbo;

3. predlagane ukrepe;

4. zahteve za potrebne vire, vključno z nepredvidenimi;

5. merila za učinkovitost ukrepov ter omejitve;

6. zahteve glede poročanja in spremljanja; ter

7. roke in urnik.

Načrte obravnave tveganj bi bilo potrebno vključiti v procese upravljanja organizacije in glede njih tudi razpravljati z ustreznimi deležniki.

Odločevalci in drugi deležniki pa morajo biti seznanjeni tudi z naravo in obsegom preostalega tveganja, ki ostane kljub obravnavi tveganja. Preostalo tveganje je treba dokumentirati in nadzorovati, pregledati in po potrebi ponovno obravnavati.

Spremljanje in pregledovanje

Oba, nadzor in pregled, morata biti del načrta upravljanja tveganj, ki mora vsebovati redne in naključne preglede ali spremljanje. Pri tem so zelo pomembne jasno določene odgovornosti.

Procesi spremljanja in pregledovanja bi morali vključevati vse vidike upravljanja tveganj zato, da:

1. se zagotovi, da so kontrole učinkovite in uspešne tako pri zasnovi kot v izvedbi;
2. pridobivanju dodatnih informacij za izboljšanje ocene tveganja;
3. organizacija analizira in pridobiva izkušnje na podlagi dogodkov (vključno s tistimi, ki so se skoraj zgodili), sprememb, trendov, uspehov in napak;
4. se zaznajo spremembe v notranjem in zunanjem kontekstu, vključno s spremembami kriterija tveganj in tveganja samega, kar lahko zahteva revizijo obravnave tveganj in zastavljenih prioritet; ter da
5. se ugotavijo nastajajoča tveganja.

Napredek pri izvajanju načrtov za obravnavo tveganj omogoča merjenje uspešnosti. Rezultate spremljanja in pregledovanja je potrebno zabeležiti/evidentirati, nato pa o njih poročati ustreznim notranjim in zunanjim javnostim, prav tako pa jih je potrebno uporabiti pri pregledu okvira upravljanja tveganj.

Evidentiranje v procesu upravljanja tveganj

Aktivnosti upravljanja tveganj morajo biti sledljive. V procesu upravljanja tveganj evidence zagotavljajo temelje za izboljšanje metod in orodij, kot tudi v celotnem procesu.

Odločitve glede oblikovanja evidenc so povezane s/z:

1. potrebami organizacije po nenehnem učenju;
2. ugodnostmi, ki jih ponuja ponovna uporaba informacij za namene upravljanja;
3. stroški in prizadevanji, nastalimi pri ustvarjanju in vzdrževanju evidenc;
4. zakonskimi, regulativnimi in operativnimi potrebami po evidencah;
5. načini dostopa, dostopnostjo in enostavnostjo medija za hrambo;
6. obdobjem hrambe; ter
7. občutljivostjo informacij.

6.2 Nekateri drugi standardi povezani z upravljanjem tveganj

6.2.1 ISO 31010:2009

ISO/IEC 31010:2009 [8] podpira standard ISO 31000 in daje napotke o izbiri in uporabi sistematičnih metod za oceno tveganja, postopek ocenjevanja tveganja in izbiro metode za oceno tveganja.

Nastal je kot plod sodelovanja med organizacijama ISO in IEC in podpira standard ISO 31000 v tistem delu, ko se le ta ukvarja z ocenjevanjem tveganj. Ocena tveganja je sestavni del upravljanja tveganj, ki zagotavlja organizacijam strukturiran proces za identifikacijo vplivov pri doseganju ciljev organizacije.

Ocenjevanje tveganja zagotavlja boljše razumevanje tveganj in omogoča boljše vedenje o ustreznosti in učinkovitosti obstoječega nadzora nad tveganji. Standard je podlaga za odločanje o najustreznejšem pristopu za obvladovanje posameznega tveganja. Je v pomoč pri implementaciji principov obvladovanja tveganj, ki jih podaja ISO 31000. Podrobno podaja:

1. koncepte ocenjevanja tveganj,
2. proces ocenjevanja tveganja in
3. izbiro tehnike za ocenjevanje tveganj.

S tem standard povzema obstoječe dobre prakse in odgovarja na naslednja vprašanja:

1. Kaj se lahko zgodi in zakaj?
2. Kakšne so posledice?
3. Kakšna je verjetnost njihovega nastanka v bodoče?
4. Ali obstajajo kakršni koli dejavniki, ki lahko ublažijo posledice tveganja ali zmanjšajo verjetnost za tveganje?

Standard sestavlja šest poglavij in dva izčrpna dodatka – vsega skupaj 90 strani.

Po uvodnih kratkih poglavjih, ki opisujejo dokument, obrazložijo povezave z drugimi dokumenti in definirajo v standardu uporabljene termine, sledijo tri osrednja poglavja, ki podrobno definirajo aktivnost ocenjevanja tveganja. Ta tri poglavja obravnavajo koncepte ocenjevanja, samo ocenjevanje in izbiro tehnike za ocenjevanje tveganj. Sledi prvi dodatek, ki vsebuje primerjave enaintridesetih različnih tehnik, ki jih lahko uporabimo pri ocenjevanju tveganj, in drugi dodatek, ki te tehnike tudi na kratko predstavi in podaja reference za nadaljnji študij le teh.

Četrto poglavje ISO 31010 podrobneje predstavlja koncepte, ki naj bi jih upoštevali pri obravnavi tveganj (kar ne smemo zamenjevati s principi, ki jih opisuje ISO 31000). Ti koncepti predstavljajo zelo poučen seznam dejstev, ki jih je pri ocenjevanju smiselno upoštevati. Zapisani so v podpoglavjih, ki govorijo o:

1. namenu in prednostih ocenjevanja,

2. vlogi in pomenu ocenjevanja glede na okvir za upravljanje tveganj, ter

3. vlogi in pomenu ocenjevanja v procesu upravljanja tveganj, kjer je ta pomen posebej izpostavljen v luči izmenjave mnenj in komuniciranja, vzpostavitve okvirja za upravljanje tveganj, samega procesa ocenjevanja tveganj, obravnave tveganj in seveda nadzora ter ocenjevanja.

Pri tem ISO 31010 ne ponavlja, temveč smiselno nadgrajuje zapisano v ISO 31000.

Peto poglavje podrobneje opisuje proces ocenjevanja. Pri tem ne samo, da podrobneje nadgrajuje vse zapisano o procesu v ISO 31000, temveč za vse aktivnosti tudi podaja predloge za uporabo posameznih tehnik iz nabora enaintridesetih, ki jih podajata oba dodatka.

Šesto poglavje opisuje, kako je mogoče izbrati ustrezno tehniko pri ocenjevanju tveganj. Pri tem opozarja, da je večkrat potrebno izbrati več teh tehnik ali metod, saj je posamezna namenjena ali pa je v danem primeru ustrezna samo eni ali več aktivnostim procesa ocenjevanja, vendar ne vsem. Pri tem poglobljeno v posameznih podpoglavjih opisuje področja znanj, ki jih je potrebno pri uporabi tehnik upoštevati. Ta področja so: izbira tehnike, razpoložljivost virov, ki vplivajo na izbiro tehnike in kompleksnost tehnike. Obstajajo še tri podpoglavja, ki govorijo o naravi in lastnostih negotovosti, ki je sestavni del tveganj, o uporabi ocenjevanja tveganj v življenjskih procesih (predvsem projektov) ter o mogočih klasifikacijah tehnik za ocenjevanje tveganj. Kratki povzetki nekaterih podpoglavij sledijo v nadaljevanju.

V dodatku A so navedeni nekateri atributi posameznih metod, kot so zahtevana sredstva, stopnja negotovosti, kompleksnost in zmožnost podajanja kvantitativnega rezultata pri oceni tveganja.

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13

```
Legenda slike:
SA - Zelo uporabno
A  - Uporabno
NA - Neuporabno
```

Slika 6.4: Uporabnost posameznih metod pri ocenjevanju tveganj (izsek iz ISO 31010) [8]

Izbira tehnike

Ocenjevanje tveganj se lahko izvaja z različnimi zahtevnostmi glede podrobnosti ocenjevanja in tako uporablja eno ali več metod, ki se razlikujejo po svoji kompleksnosti. Rezultat ocenjevanja ima lahko različne oblike, ki morajo biti v skladu s kriteriji, ki smo jih postavili v aktivnosti "Vzpostavitev okvirja". Pri tem si pomagamo z vrednotenjem posameznih metod po kriterijih, ki jih prikazuje slika 6.4. Slika prikazuje izsek tabele iz dodatka A standarda ISO 31010, kjer so posamezne metode ovrednotene glede na uporabnost v posameznih aktivnostih procesa ocenjevanja tveganj.

Razpoložljivost virov

Viri in zmožnosti, ki lahko vplivajo na izbiro tehnike ocenjevanja, vsebujejo:

1. spretnosti, izkušnje in zmožnosti skupine, ki ocenjuje tveganje;
2. časovne in ostale omejitve, ki so pogojene s samo organizacijo, ki ocenjuje tveganja; ter
3. finančne okvire, ki so na voljo v primeru, da so potrebni zunanji viri.

Narava in stopnja negotovosti

Oboje, narava in stopnja negotovosti zahtevata razumevanje kvalitete, količine in celovitosti informacij o posameznih tveganjih. To vsebuje tudi zavedanje o pomanjkanju informacij o tveganjih samih, njihovih virih in vzrokih ter posledicah, ki jih imajo za doseganje ciljev organizacije. Negotovost lahko izhaja iz slabih podatkov ali iz pomanjkanja pomembnih in zaupanja vrednih podatkov. Negotovost je lahko prisotna tudi v eksternem ali internem kontekstu organizacije. Nekateri podatki na osnovi zgodovine niso dosegljivi ali jih ni mogoče pravilno interpretirati. Vse to zahteva razumevanje tipa in narave negotovosti, kar je potrebno posredovati vsem odločevalcem v organizaciji.

Kompleksnost

Kompleksnost je naslednji izziv pri obravnavi tveganj. Nekatera tveganja so kompleksna sama po sebi, nekatera pa enostavna, vendar je medsebojna interakcija med posameznimi (lahko tudi zelo enostavnimi) tveganji zelo kompleksen pojav, ki ga nikakor ne smemo zanemariti, čeprav bi lahko rekli, da je vsako posamezno tveganje zanemarljivo.

6.2.2 ISO/IEC 27005:2011

Za izvedbo učinkovitega sistema upravljanja varnosti morajo organizacije poskrbeti za sistematično upravljanje tveganj, ki mora biti skladno s potrebami, usmeritvami in okoljem, v katerem organizacija deluje. Navsezadnje mora biti upravljanje posameznih (operativnih, IT, tečajnih, itd) tveganj v skladu z upravljanjem vseh tveganj, s katerimi se organizacija srečuje. Varnostne usmeritve se nanašajo na pravočasno in učinkovito upravljanje tveganj na področjih, kjer in kadar je to potrebno. Gre za proces, ki ga je potrebno vzpostaviti in ga po vzpostavitvi stalno izvajati in dopolnjevati.

Standard ISO/IEC 27005:2011 (ISO/IEC 27005:2011; Information technology – Security techniques – Information security risk management, International organization for Standardization) [10] je standard, ki opisuje proces upravljanja tveganj in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost v okviru splošnih konceptov. Za razliko od prejšnje različice, ki je nosila oznako ISO/IEC 27005:2008, opisani v članku [22], je standard v tej različici sinhroniziran z zgoraj opisanim standardom ISO 31000. Tako je najnovejši ISO/IEC 27005 primer uporabe ali impelmentacije ISO 31000.

Opisuje proces upravljanja tveganj in njegove aktivnosti, s katerimi zagotavljamo informacijsko varnost v okviru splošnih konceptov, ki jih podaja ISO/IEC 27001:2013 [12]. ISO/IEC 27001:2013 sicer določa zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema vodenja varovanja informacij v okviru organizacije. To vključuje tudi zahteve za ocenjevanje in obravnavo informacijskih tveganj prilagojeno potrebam organizacije. Vendar ISO 27001 ni predmet te knjige, ker je področje tveganj, ki ga opisuje, že pokrito s standadi ISO 31000, ISO 31010 in ISO 27005.

Proces upravljanja tveganj, ki jih predvideva ISO 27005, je mogoče uporabiti pri:

1. celotni organizaciji ali samo v enem od njenih delov (kot je oddelek, fizična lokacija ali celo storitev);

2. katerem koli informacijskem sistemu; in

3. pri obstoječih, planiranih ali pri posameznih vrstah kontrol v organizaciji (na primer pri načrtovanju neprekinjenega poslovanja).

Upravljanje informacijskih tveganj zajema opravila, ki med drugim zajemajo:

1. prepoznavanje tveganj;

2. ocenjevanje tveganj prek vplivov na poslovanje podjetja in morebitne verjetnosti, da se pojavijo;

3. komuniciranje in razumevanje verjetnosti za tveganja in posledice tveganj;

4. vzpostavitev prioritetnega vrstnega reda ukvarjanja s tveganji;

5. vzpostavitev vrstnega reda akcij za zmanjševanje tveganj;

6. vključevanje vseh deležnikov organizacije v odločanje o upravljanju tveganj in o stalnem informiranju o stanju glede tveganj;

7. učinkovit nadzor in spremljanje tveganj in samega upravljanja tveganj;

8. zajemanje informacij, s katerimi lahko upravljanje tveganj izboljšujemo;

9. izobraževanje zaposlenih - še posebej vodij - glede tveganj in načinov za izogibanje tveganjem.

Seveda ISO/IEC predstavlja samo enega od pristopov k reševanju problematike ocenjevanja tveganj. Podaja splošna priporočila za analizo in ocenjevanje informacijskih tveganj tako, da ne predpisuje posamezne metode ali orodja, ki bi bilo primerno za uporabo v neki organizaciji.

ISO/IEC 27005 podaja splošen pregled aktivnosti za obvladovanje informacijskih tveganj pri varovanju informacij. Pri vsaki aktivnosti so opisane dejavnosti, ki so porazdeljene v naslednja področja:

1. Prispevek (Input): Določa vse potrebne informacije za izvedbo aktivnosti.

2. Ukrep (Action): Dejavnost opiše.

3. Navodila za vpeljavo (Implementation guidance): Navede smernice za izvedbo ukrepa. Pri tem standard opozarja, da nekatere od teh smernic niso primerne v vseh primerih in da imamo opraviti z izbiro smernic ali načinov za izvedbo ukrepa.

4. Rezultat (Output): Določa vse informacije, ki nastajajo po izvedbi aktivnosti.

Nekateri dodatni izkustveni napotki za obvladovanje tveganja pri varovanju informacij so predstavljeni v prilogah:

1. Priloga A. Podaja izkustvene napotke o določanju konteksta upravljanja informacijskih tveganj.

2. Priloga B. Na osnovi dobre prakse priporoča prepoznavanje in ocenjevanje sredstev.

3. Priloga C. Predstavlja primere tipičnih groženj.

4. Priloga D. Našteti so primeri tipičnih ranljivosti.

5. Priloga E. Gre za prilogo, ki opisuje primere pristopov ocenjevanja informacijskih tveganj. V tej prilogi je podana jasna razmejitev med ocenjevanjem tveganj na splošnem, to je višjem nivoju in med ocenjevanjem na podrobnejšem nivoju. Ocenjevanje tveganj je osrednji izziv vsakega upravljanja tveganj.

6. Priloga F. V tej prilogi je seznam splošnih omejitev za zmanjšanje tveganja, kot so časovne, tehnične, etične, okoljevarstvene in druge omejitve.

Proces upravljanja informacijskih tveganj

Proces je enak kot pri ISO 31000, ki je opisan zgoraj. Kljub temu, pa so tudi v najnovejši različici standarda ohranili bolj podrobno delitev procesa, kot ga prikazuje slika 6.5.

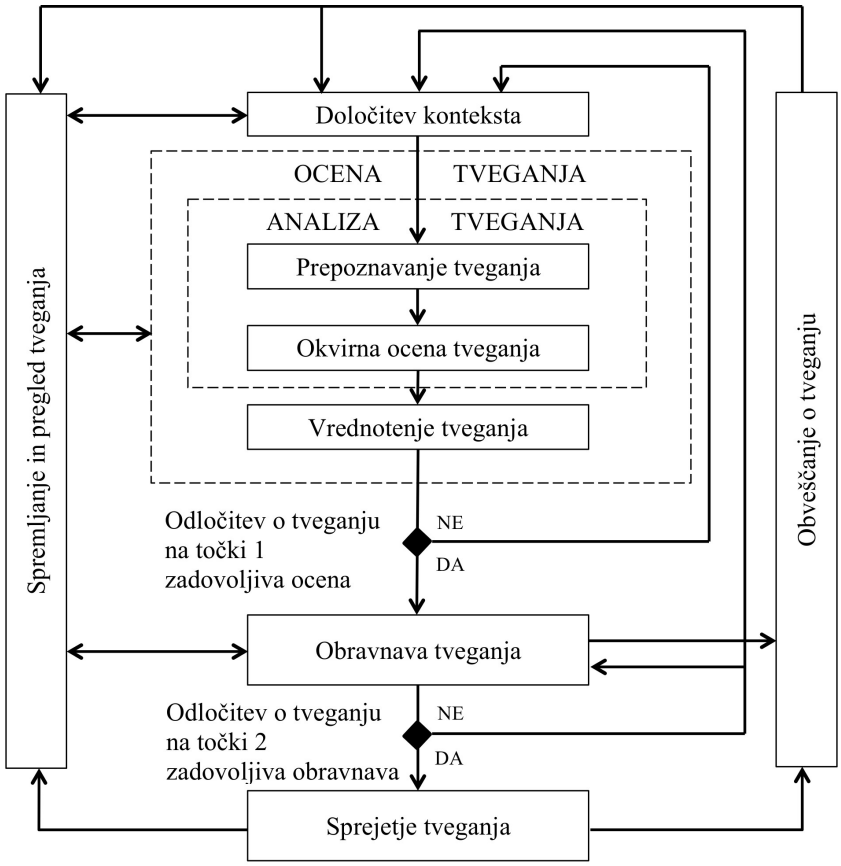
Pri sprejemanju tveganj moramo zagotoviti, da vodilni v organizaciji izrecno sprejmejo preostala tveganja. To pomeni, da sprejmejo vsa tveganja, ki niso bila predmet obravnave tveganj ali pa smo se pri obravnavi tveganj odločili, da jih v danem trenutku sprejmemo takšne, kot so.

Ker ISO 27001 predvideva cikel PDCA (Plan - Do - Check - Act) v okviru ISMS (Information Security Management System), je temu ciklu podvržen tudi ISO 27005. Spodnja tabela 6.1 povzema aktivnosti obvladovanja tveganja pri varovanju informacij.

V nadaljevanju branja bo mogoče razbrati, da ISO/IEC 27005 sledi ISO 31000, vendar ni povsem identičen – gre za primer njegove uporabe. Prav tako v nadaljevanju ni v celoti opisan ISO/IEC 27005, temveč predvsem tisti, del, ki sledi ISO 31000.

Določitev konteksta

Pri določanju konteksta zberemo informacije o organizaciji, ki so relevantne za obvladovanje tveganj v okviru informacijske varnosti. Sem spada:



Slika 6.5: Aktivnosti pri upravljanju informacijskih tveganj [18]

Proces ISMS	Aktivnost pri procesu obvladovanja tveganja pri varovanju informacij
Načrtuj (Plan)	Določitev konteksta Ocena tveganja Razvoj načrta za obravnavo tveganja Sprejetje tveganja
Stori (Do)	Vpeljava načrta za obravnavo tveganja
Preveri (Check)	Stalno spremljanje in pregledovanje tveganj
Ukrepaj (Act)	Vzdrževanje in izboljševanje procesa obvladovanja tveganja pri varovanju informacij

Tabela 6.1: Prekrivanje ISMS po ISO 27001 (Information Security Management System) procesov z aktivnostmi procesa obvladovanja informacijskih tveganj

1. **Določanje osnovnih meril**, potrebnih za varnost pri upravljanju informacijskih tveganj. Izbrati je potrebno ustrezen pristop k obvladovanju tveganja ali ga razviti. Razviti in določiti je potrebno merila za vrednotenje:

   (a) tveganja, ki ogroža varnost informacij organizacije;

   (b) učinka v smislu stopnje škode ali stroškov za organizacijo, ki jih povzroči informacijski varnostni dogodek; ter

   (c) sprejetja tveganja, ki so pogosto odvisna od politike in ciljev organizacije ter interesov interesnih skupin.

   Merila za sprejetje tveganja se lahko razlikujejo glede na to, kako dolgo pričakujemo obstoj tveganja. Poleg tega mora organizacija oceniti, ali so na voljo ustrezna sredstva.

2. **Opredelitev področja uporabe in mej** vseh ustreznih sredstev, poslovnih ciljev, poslovnih procesov, strategij, pravnih in regulativnih zahtev, ki veljajo za organizacijo, ter vmesnikov. Področje upo-

rabe procesa obvladovanja tveganja pri varovanju informacij mora biti opredeljeno za zagotovitev, da se pri oceni tveganja upoštevajo vsa sredstva. Poleg tega je treba določiti meje, da se lahko obravnavajo tveganja, ki lahko prestopijo meje. Informacije o organizaciji je treba zbrati za določitev okolja, v katerem deluje, in njegove pomembnosti pri procesih obvladovanja tveganja. Poleg tega mora organizacija utemeljiti vsako izključitev s področja uporabe.

3. **Organiziranje obvladovanja tveganja**, tj. vzpostavitev ustreznega delovanja zaposlenih v organizaciji na področju varnosti pri upravljanju informacijskih tveganj (vloge in odgovornosti). Takšno organiziranje mora odobriti vodstvo organizacije Bistveno je tudi, da določimo namen obvladovanja tveganja pri varovanju informacij, ker ta vpliva na celoten proces in zlasti na določitev konteksta.

Prepoznavanje tveganja

Namen prepoznavanje tveganja je, da določimo, kaj lahko povzroči potencialno izgubo ter kako, kje in zakaj lahko ta izguba nastane.

Sama aktivnost določa prepoznavanje sredstev, možnih groženj in šibkih točk, ki obstajajo (ali bi lahko obstajale) ter prepoznavanje že obstoječih kontrol, njihov vpliv na prepoznavanje tveganj in morebitne posledice. Prepoznavanje tveganja temelji na naslednjih opravilih:

1. **Prepoznavanje sredstev**. Prepoznavanje moramo izvesti tako podrobno, da zagotovimo dovolj informacij za oceno tveganja. Stopnja natančnosti vpliva na splošno količino informacij, zbranih med oceno tveganja. Stopnjo je mogoče v nadaljnjih ponovitvah ocene tveganja ponovno določiti kako drugače.

2. **Prepoznavanje groženj**. Opredeliti moramo splošne nevarnosti oz. grožnje in jih razvrstiti po tipu (npr. nedovoljene dejavnosti,

materialna škoda in tehnične napake). Upoštevati je potrebno tudi interne izkušnje iz preteklih incidentov ter pretekle ocene nevarnosti. Pri obravnavi groženj moramo upoštevati še vidike okolja in kulture.

3. **Prepoznavanje obstoječih kontrol**. Znova moramo identificirati in preveriti obstoječe kontrole z namenom zagotavljanja njihovega pravilnega delovanja. Kontrole, katerih vpeljava se načrtuje v skladu z načrti za vpeljavo obravnave tveganja, je treba upoštevati na enak način kot že vpeljane kontrole. Za identifikacijo obstoječih oz. načrtovanih kontrol morajo biti zbrane informacije preverjene še pri osebah, odgovornih za varovanje informacij, in pri uporabnikih, da ugotovimo, katere kontrole so resnično vpeljane za informacijske procese ali informacijske sisteme. Opravimo še izvedbo fizičnih kontrol na mestu samem in pregled rezultatov internih presoj.

4. **Prepoznavanje ranljivosti**. Prepoznati moramo ranljivosti, ki jih lahko izkoristijo grožnje, da škodujejo sredstvom oziroma organizaciji. Sama prisotnost ranljivosti še ne povzroči škode, ker je potrebna grožnja, ki bi jo uresničila.

5. **Prepoznavanje posledic**. Ta dejavnost določa škodo ali posledice za organizacijo, ki jih lahko povzroči negativni scenarij (incident). Negativni scenarij opisuje grožnje, ki jim je organizacija izpostavljena zaradi pomanjkljivosti oziroma niza pomanjkljivosti v informacijskem varnostnem sistemu. Učinek negativnega scenarija moramo determinirati ob upoštevanju meril učinka, opredeljenih v procesu vzpostavitev vsebin in njihovih soodvisnosti.

Okvirna ocena tveganja

Ocenjevanje tveganja je aktivnost dodeljevanja vrednosti verjetnostim in posledicam vsakega identificiranega tveganja. Sestavljajo jo naslednja

opravila:

1. **Izbira metodologije za okvirno oceno tveganja glede na specifičnost zahtev in specifičnost samega tveganja**: Tveganja lahko analiziramo različno natančno, odvisno od pomembnosti sredstva, obsega znanih ranljivosti in preteklih incidentov, ki so prizadeli organizacijo. Lahko je – odvisno od okoliščin – kvalitativna ali kvantitativna analiza ali kombinacija obeh. Kvalitativna okvirna ocena uporablja kvalifikacijske atribute za opis resnosti potencialnih posledic (npr. nizko, srednje, visoko) in verjetnost njihovega pojava. Prednost kvalitativne okvirne ocene je v preprostosti razumevanja, medtem ko je slaba lastnost odvisnost od subjektivne izbire ocene. Kvantitativna okvirna ocena uporablja ocenjevalno lestvico z numeričnimi vrednostmi (namesto opisnih ocenjevalnih lestvic) za posledice in verjetnost, pri čemer uporabljamo podatke iz različnih virov. Kvaliteta analize je odvisna od pravilnosti in popolnosti numeričnih vrednosti in veljavnosti uporabljenih modelov.

2. **Ocena posledic**: Oceniti moramo vpliv na poslovanje organizacije, ki ga lahko ima možen ali dejanski incident pri varovanju informacij. Pri tem moramo upoštevati kršitve varovanja informacij, kot so izguba zaupnosti, celovitosti ali razpoložljivosti sredstev. Vrednost vpliva na poslovanje se lahko izrazi v kvalitativni in kvantitativni obliki, vendar metoda določitve denarne vrednosti navadno zagotovi več informacij za odločanje in s tem olajša učinkovitejši proces odločanja.

3. **Ocena verjetnosti incidenta**: Oceniti moramo verjetnost uresničitve negativnih scenarijev (scenarijev incidenta). Po določitvi scenarijev incidenta je potrebno oceniti verjetnost pojava posameznega scenarija in vpliva, za kar ponovno uporabimo kvalitativne in kvantitativne ocenjevalne tehnike. Pri tem je potrebno upoštevati, kako

pogosto se grožnje uresničijo in kako lahko je izkoristiti ranljivost.

4. **Raven ocene tveganja**: Z okvirno oceno tveganja določimo vrednosti verjetnosti in posledic tveganja (kvantitativne ali kvalitativne vrednosti). Okvirna ocena tveganja temelji na ocenjenih posledicah verjetnosti. Poleg tega pri tem lahko upoštevamo stroškovne koristi, skrbi interesnih skupin in druge spremenljivke, primerne za vrednotenje tveganja.

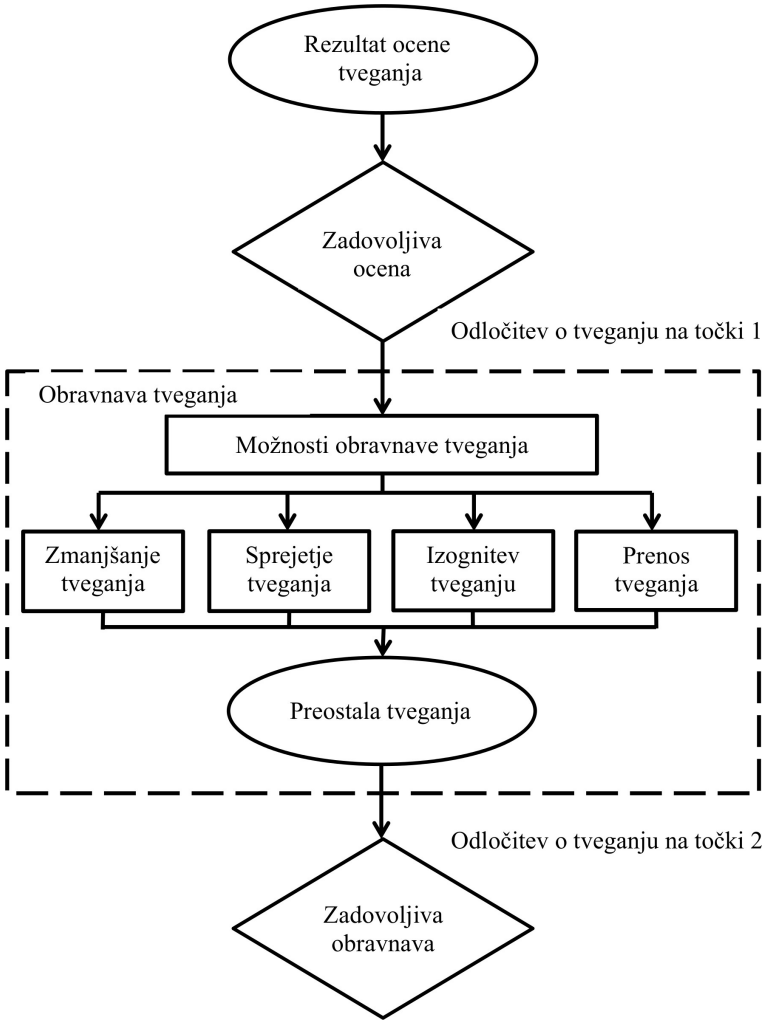
Vrednotenje tveganja

Pri aktivnosti vrednotenja tveganj primerjamo nivo tveganja z merili za oceno tveganja ter merili sprejemljivosti (opredeljenih v procesu vzpostavitve vsebin in njihovih soodvisnosti). Merila za vrednotenje tveganja, ki se uporabijo za sprejemanje odločitev, morajo biti skladna z opredeljenim eksternim in internim kontekstom obvladovanja tveganj pri varovanju informacij. Upoštevamo cilje organizacije, pomen poslovnega procesa oziroma z določenimi sredstvi podprte dejavnosti ali niz sredstev, stališča interesnih skupin itn. Odločitve, sprejete med vrednotenjem tveganja, večinoma temeljijo na sprejemljivi ravni tveganja. Vendar moramo upoštevati tudi posledice, verjetnost in stopnjo zaupanja v določitev tveganja in analizo. Združitev več nizkih ali srednjih tveganj lahko povzroči precej višja skupna tveganja, zato jih obravnavamo v skladu s tem spoznanjem.

Obravnava tveganja

Pri ravnanju s tveganji zagotovimo seznam prednostnih tveganj z negativnimi scenariji glede na merila tveganj. Slika 6.6 kaže zgoraj naštete štiri dejavnosti pri obravnavi tveganja.

Kot je razvidno iz slike, standard definira štiri načine soočenja s tveganji:



Slika 6.6: Obravnava tveganj [18]

1. **Zmanjšanje tveganja**: Raven tveganja je treba zmanjšati z izborom kontrol, tako da je preostala tveganja mogoče ponovno oceniti kot sprejemljiva. Izbrati je treba ustrezne in utemeljene kontrole, da se izpolnijo zahteve, ugotovljene med oceno tveganja in obravnavo tveganja. Na splošno lahko kontrole zagotovijo eno ali več naslednjih vrst zaščite: popravilo, odprava, preprečevanje, zmanjšanje vpliva, odvračanje, odkrivanje, obnova, spremljanje in ozaveščanje.

2. **Zavestno in objektivno sprejetje tveganja**: Odločitev brez nadaljnjih ukrepov mora biti odvisna od vrednotenja tveganja. Povsem mora ustrezati politikam organizacije in kriterijem za sprejem tveganj. Tveganja sprejmemo takšna, kot so.

3. **Tveganju se izognemo**: Dejavnosti ali pogoju, ki sproža določeno tveganje, se je treba izogniti.

4. **Prenos tveganja**: Tveganje je treba prenesti na drugo stranko, ki bo najučinkoviteje obvladala določeno tveganje glede na vrednotenje tveganja (na zavarovalnico na primer). Prenos tveganja lahko ustvari nova tveganja ali spremeni obstoječa, prepoznana tveganja.

Možnosti za obravnavo tveganja izberemo na podlagi rezultata ocene tveganja, pričakovanih stroškov za vpeljavo teh možnosti in pričakovanih koristi teh možnosti.

Sprejetje tveganj

Pri tej aktivnosti se odločimo, da tveganje sprejmemo, določimo odgovornost za to določitev in jo uradno zabeležimo. Načrti za obravnavo tveganj morajo opisati, kako obravnavamo ocenjena tveganja za izpolnitev meril za sprejetje tveganja. Pomembno je, da odgovorni pregledajo in odobrijo predlagane načrte za obravnavo tveganja in nastala preostala tveganja ter zabeležijo vse pogoje, ki so povezani s takšno odobritvijo.

Obveščanje o tveganju

Obveščanje o tveganju je dejavnost za sklenitev sporazuma o tem, kako obvladovati tveganja. Slednje storimo z izmenjavo in/ali delitvijo informacij o tveganju med osebami, ki sprejemajo odločitve, in drugimi interesnimi skupinami. Takšne informacije vključujejo obstoj, naravo, obliko, verjetnost, resnost, obravnavo, sprejemljivost tveganj in ostalo.

Oseba, ki sprejema odločitve, in zainteresirane javnosti, si morajo izmenjavati informacije o tveganju. Uspešna komunikacija med zainteresiranimi stranmi je pomembna, ker lahko odločilno vpliva na odločitve, ki jih je treba sprejeti. Sporočanje bo zagotovilo, da osebe, odgovorne za vpeljavo obvladovanja tveganja, in osebe, zainteresirane zanj, razumejo podlago, na kateri sprejememo odločitve in določene ukrepe. Komunikacija je dvosmerna.

Nadzor in ocenjevanje tveganja

Ocena tveganja določa vrednost informacijskih sredstev, prepoznava obstoječe grožnje in ranljivosti (ali ki bi lahko obstajale), prepoznava obstoječe kontrole in njihov vpliv na obstoječa tveganja, določa možne posledice in prednostni vrstni red ugotovljenih tveganj in jih razporedi v skladu z merili za vrednotenje tveganja, opredeljenimi pri določanju konteksta. Stalno spremljanje in pregledovanje sta nujna koraka, s katerima zagotovimo, da kontekst, rezultat ocene tveganja in obravnave tveganja ter načrti za obvladovanje ostanejo ustrezni glede na okoliščine. Organizacija se mora prepričati, da proces obvladovanja tveganj pri varovanju informacij in z njimi povezane dejavnosti ostanejo ustrezne glede na obstoječe okoliščine in se upoštevajo. Vsako dogovorjeno izboljšavo procesa ali ukrepov, ki so potrebni za izboljšanje skladnosti s procesom, moramo sporočiti vodstvu, da bi zagotovili, da nobenega tveganja ali elementa tveganja ne spregledamo ali podcenimo, da ustrezno ukrepamo, tveganje razumemo in smo se

sposobni nanj odzvati.

Poleg tega mora organizacija redno preverjati, da so ukrepi, ki se uporabljajo za merjenje tveganja in njegovih elementov, še vedno veljavni in v skladu s poslovnimi cilji, strategijami in politikami ter da se med obvladovanjem tveganja pri varovanju informacij ustrezno upoštevajo spremembe poslovnega okolja.

6.2.3 ISO 28000:2007

Ta standard se uporablja za izvajanje sistemov za upravljanje varnosti oskrbovalne verige v organizacijah. Osnovni namen standarda je, da še lahko neposredno in formalno pristopi k upravljanju varnosti organizacij tako, da se zagotovi poslovna uspešnost in verodostojnost organizacije" [6]. ISO 31000 je splošni standard za upravljanje tveganj, ISO 28000 pa specifična uporaba varnosti pri oskrbovalnih verigah. Pri tem upravljanje varnosti opredeljuje kot "uporabo sistematičnih in usklajenih dejavnosti in praks, prek katerih organizacija optimalno upravlja tveganj povezanimi z oskrbovalnimi verigami ter s tem povezanimi potencialnimi nevarnostmi in vplivi njih" [6].

ISO 28000:2007 določa zahteve za sistem upravljanja varnosti, vključno s tistimi vidiki, kritičnih za varnostne zanesljivosti dobavne verige.

ISO 28000: 2007 se uporablja za vse velikosti organizacij v kateri koli fazi proizvodnje ali oskrbovalne verige, ki želi:

1. vzpostaviti, izvajati, vzdrževati ali izboljšati sistem upravljanja varnosti;
2. zagotoviti skladnost z vzpostavljeno politiko upravljanja varnosti;
3. drugim dokazati takšno skladnost;
4. si prizadeva certificirati svoj sistem upravljanja varnosti tako, da je akreditiran s strani certifikacijskega organa; ali

5. da zase doseže skladnost s standardom ISO 28000.

Poleg tega lahko obstaja zakonodaja ali kakšne druge pogodbene obveznosti, ki vključujejo nekatere zahteve iz standarda.

Organizacije, ki se odločijo za certificiranja s strani tretje osebe (certifikacijskega organa na primer) dokazujejo, da pomembno prispevajo k varnosti dobavne verige.

Področja kot jih definira ISO 28000, kjer se tveganja lahko pojavljajo so:

1. Tveganja fizičnih odpovedi, kot so na primer funkcionalne odpovedi opreme, naključne odpovedi, zlonamerne poškodbe, teroristična ali kriminalna dejanja.

2. Operativna tveganja, ki vključujejo nadzor varnosti, človeškega faktorja in ostale aktivnosti, ki vplivajo na uspešnost, stanje in varnost organizacije.

3. Naravni okoljski dogodki (nevihte, poplave itd.), zaradi katerih lahko varnostni ukrepi in oprema postanejo manj učinkoviti.

4. Faktorji, ki niso pod nadzorom organizacije, kot na primer odpoved opreme ali storitev, ki jih izvajajo zunanji ponudniki.

5. Tveganja vseh zainteresiranih udeležencev organizacije, kot na primer nedoseganje regulativnih zahtev ali zmanjšan ugled blagovne znamke.

6. Načrtovanje in instalacija varnostne opreme, vključujoč menjavo, vzdrževanje itd.

7. Upravljanje informacij in podatkov ter komunikacije.

8. Grožnje za kontinuiteto delovanja.

6.3 Katalog tveganj v oskrbovalni verigi

Organizacije v današnjem času ne morejo delovati v izolirano varnem okolju brez tveganj, ki izhajajo iz oskrbovalnih verig. Še posebej lahko to trdimo zaradi trendov globalizacije in globalnega oskrbovanja, ki se pojavljajo v zadnjih letih in postajajo vedno bolj aktualni. Tveganja, ki izhajajo iz logistike in oskrbovalnih verig, postajajo glavna skrb v današnjih logističnih in oskrbovalnih procesih v vseh organizacijah. Posledično lahko trdimo, da je proces upravljanja tveganj ključnega pomena za neprekinjeno delovanje organizacij na vseh področjih delovanja. Najverjetneje je tveganja najlažje razumeti, če si jih predstavljamo v luči koncepta investicij. Te so baza vsake poslovne aktivnosti – omogočajo vzdrževanje, povečujejo obseg poslovanja ali omogočajo spremembe v poslovnih aktivnostih [4,16,17,20,21] – in hkrati vključujejo tveganja in njihovo upravljanje kot ključni faktor v operacijskih aktivnostih; praktično ni investicij brez tveganj.

Tveganja so integrirana v naša življenja, zdi se, kot da ljudje nikoli prej nismo posvečali toliko pozornosti izzivom, ki jih prinašajo tveganja, kot to počnemo danes. Veliko člankov, prispevkov in pogovorov se vrti okoli tematike tveganj, posledično obstaja veliko idej in predstav o tem, kaj tveganje sploh je in kaj predstavlja, kar kaže na kompleksnost problema, ki se pojavi, ko se nekdo loti obsežnega upravljanja tveganj.

Če se naslonimo na model upravljanja tveganj, kot nam ga nudi ISO 31000, vidimo, da so procesi, ki so vključeni v ocenjevanje tveganj, še posebej prepoznavanje in analiza tveganj, najbolj ključni v celotnem procesu upravljanja tveganj. Zavedati se je potrebno, da tveganja, ki niso zaznana v procesu prepoznavanja tveganj, tudi kasneje niso obravnavana in vključena v upravljanje tveganj, torej so spregledana in se nanje ne moremo pripraviti. Prav zaradi tega smo na Fakulteti za logistiko razvili model za učinkovito ocenjevanje tveganj v organizacijah. Pilotno testiranje modela je potekalo v sodelovanju s podjetjem, ki deluje pretežno na

področju skladiščenja, nadaljnja testirana pa še na dodatnih organizacijah in oskrbovalnih verigah iz prakse. Rezultat teh testiranj je obsežen katalog prepoznanih tveganj, kjer je vsako tveganje uvrščeno v kategorije po različnih dimenzijah, ki jih bomo podrobneje razložili v nadaljevanju. Ker je bilo testiranje v organizacijah zelo dobro sprejeto, lahko sklepamo, da smo na pravi poti za dosego našega cilja, ki je razviti široko uporaben model za upravljanje tveganj v oskrbovalnih verigah. Dodaten cilj predstavlja tudi dopolnjevanje spletnega kataloga tveganj, ki je objavljen pod Creative Commons licenco, kar dovoljuje vsem uporabnikom kataloga, da ga prosto uporabljajo pri svojem delu ter z idejami, predlogi in dopolnitvami sodelujejo pri njegovem nastajanju.

6.3.1 Model za ocenjevanje tveganj

Prvi korak pri procesu ocenjevanja tveganj je vedno prepoznavanje le-teh. Ta proces mora biti izpeljan zelo pazljivo ter biti čim bolj obsežen, da s tem zagotovimo prepoznanje čim več tveganj in se izognemo spregledu pomembnih tveganj. V modelu je proces prepoznavanja tveganj podprt s tremi metodami, ki jih priporoča tudi standard ISO 31010, to so odprt intervju, strukturiran intervju in vodeno viharjenje možganov (brainstorming). Usposobljeni strokovnjaki vodijo srečanja z zaposlenimi v določeni organizaciji, kjer je poudarek na prepoznavanju tveganj. Ta tveganja so kasneje umeščena v model preko kategorizacije po različnih dimenzijah ter opisana.

Ker verjamemo, da sta prepoznavanje in analiza tveganj ključna procesa pri upravljanju tveganj, smo v model uvrstili več dimenzij, ki pomagajo pri opisovanju in definiranju tveganj in posledično omogočajo informiran pristop k upravljanju tveganj. Ko je posamično tveganje prepoznano, ga z uvrstitvijo v posamezne dimenzije definiramo po temeljnih dimenzijah, ki so vključene v model. Kasneje v procesu je potrebno uvesti še dodatne dimenzije, ki so specifične za vsako organizacijo, torej jih v katalog

tveganj, ki ga izdelujemo, nismo uvrstili. Takšne kompleksnejše dimenzije opisa tveganj so na primer odnosi in medsebojni vplivi med tveganji, specifične posledice, ki jih lahko organizaciji prinese uresničitev posameznega tveganja in podobno.

Segmentiranje tveganj po ISO 28000

Model, ki smo ga ustvarili, in tudi katalog, ki iz njega izvira, sta strukturirana tako, da sta komplementarna standardu za zagotavljanje varnosti v oskrbovalnih verigah ISO 28000 in je opisan v tretjem poglavju. V tem standardu je definiranih več področij, kjer se lahko tveganja pojavljajo v organizaciji ali znotraj njene oskrbovalne verige. V prvem koraku procesa ocenjevanja tveganj, kot smo ga zastavili v našem modelu, se tveganja razvrstijo v skupine po ISO 28000, ki so:

1. Tveganja fizičnih odpovedi, kot npr. funkcionalne odpovedi opreme, naključne odpovedi, zlonamerne poškodbe, teroristična ali kriminalna dejanja.

2. Operativna tveganja, ki vključujejo nadzor varnosti, človeškega faktorja in ostale aktivnosti, ki vplivajo na uspešnost, stanje in varnost organizacije.

3. Naravni okoljski dogodki (nevihte, poplave itd.), zaradi katerih lahko varnostni ukrepi in prema postanejo manj učinkoviti.

4. Faktorji, ki niso pod nadzorom organizacije, kot npr. odpoved opreme ali storitev, ki jih izvajajo zunanji ponudniki.

5. Tveganja vseh zainteresiranih udeležencev organizacije, npr. nedoseganje regulatornih zahtev ali zmanjšan ugled blagovne znamke.

6. Načrtovanje in instalacija varnostne opreme, vključujoč menjavo, vzdrževanje itd.

7. Upravljanje informacij, podatkov in komunikacije.

8. Grožnje kontinuiteti delovanja.

Opis nekega tveganja po dimenziji skupin ISO 28000 predstavlja prvo skupino opisov, ki jih zajema spletni katalog tveganj. Ker so nekatera tveganja bolj kompleksna, jih ne moremo uvrstiti v samo eno skupino, zato so nekatera tveganja uvrščena v dve skupini – primarno in sekundarno.

Segmentiranje tveganj glede na vpliv na sredstva logistike

Pri analiziranju logističnih tveganj se moramo zavedati, da znotraj logističnih procesov in procesov v oskrbovalnih verigah obstaja več sredstev oziroma virov, ki so ključni za izvajanje logistike. Na podlagi raziskav ter posvetovanj s strokovnjaki s področja logistike smo za potrebe modela in kataloga sestavili seznam štirih primarnih virov, brez katerih logistični procesi ne morejo potekati. Ti so:

1. Tok blaga in/ali storitev mora biti upravljan od izvorne točke do porabne točke z namenom doseganja pričakovanj kupcev in potrošnikov.

2. Informacije so podatki (v vseh oblikah), ki predstavljajo vnos v informacijski sistem, ki jih obdela in tvori izhodne informacije, kot jih potrebuje organizacija [15].

3. Logistični infrastruktura in suprastruktura kot osnovne fizične in organizacijske strukture, ki so potrebne za logistične operacije.

4. Ljudje so osebje, ki je potrebno za načrtovanje, organiziranje, pridobivanje, uvajanje, dostavljanje, podporo, nadzorovanje in ocenjevanje logističnih sistemov in storitev. Lahko so notranji, zunanji ali pogodbeni, odvisno od potreb organizacije.

Vsaka posledica tveganj, ki se pojavljajo v oskrbovalnih verigah, lahko vpliva na enega ali več sredstev logistike. Če želimo učinkovito upravljati tveganja, se je potrebno zavedati, na katere vire ima posamezno tveganje vpliv. Ravno zato smo v model uvrstili kategorijo, ki te vplive definira. Prav tako kot s kategorijami po ISO 28000 tudi v tej kategoriji velja, da lahko posamezno tveganje vpliva na več kot eno sredstvo logistike, zato smo tudi pri tej kategoriji uvedli še kategorijo sekundarnega vpliva na sredstva logistike.

Segmentacija tveganj glede na nosilce tveganj – javnosti

Segmenti javnosti so skupine ljudi, ki jih lahko identificiramo na podlagi njihovega zanimanja za, odnosa do, ali trenutnega obnašanja glede na neko vprašanje. Kot takšne lahko ljudi (razdeljene na posamične javnosti) razumemo kot najpomembnejši del okolja, ki ga obravnavamo v procesu upravljanja tveganj. Pristop, kjer segmenti javnosti igrajo ključno vlogo pri upravljanju tveganj, je nov v znanstveni tehnično orientirani literaturi.

Ker je vsak človek edinstven in drugačen od ostalih, se lahko tudi posameznikov odnos do nekega tveganja, s katerim se srečuje, zelo razlikuje od odnosov ostalih do istega tveganja. Ravno zaradi tega imajo ljudje različne odnose in poglede na enako tveganje, kar je lahko rezultat različnih izpostavljenosti kot tudi različnih ocenjenih stopenj negotovosti. Ta problem najpogosteje gledamo ne na primeru posameznika, temveč na primeru posameznih skupkov ljudi, ki si delijo podobne značilnosti oziroma odnose do nekega tveganja, to so segmenti javnosti.

Naš pristop temelji na predpostavki, da je tveganje sestavljeno kot je opisano v prejšnjih poglavjih. S takšnim pristopom v modelu, in to v realnem primeru, opisujemo in ocenjujemo tveganja in njihove vplive drugače kot večina današnje literature. Temeljimo na že opisaneni predspostavki, da lahko samo živa bitja čutijo in razumevajo sama sebe, medtem ko neživa bitja tega niso sposobna. Ugotovimo lahko , da v končni fazi tveganja pri-

zadenejo samo ljudi, katerih značilnost je dojemljivost za razumevanje. V skladu s to teorijo v modelu vse ljudi, ki so deležniki v oskrbovalni verigi ali njenem okolju, segmentiramo na javnosti, to je na skupine ljudi s skupnimi interesi ali funkcijami, seveda z ozirom na določeno tveganje. Ko opisujemo tveganja v našem modelu, ena dimenzija predstavlja natančno to – opis, katere javnosti določeno tveganje prizadene. Ta teorija je v skladu z ISO 31000, kjer je kot eden izmed ključnih načel pri upravljanju tveganj opisano načelo: 'upravljanje tveganj upošteva človeške in kulturne faktorje. Prepoznava sposobnosti, razumevanje in namere zunanjih in notranjih ljudi, ki lahko pripomorejo ali zavirajo doseganje ciljev organizacije' [7]. Prav tako standard definira pomembnost komuniciranja in posvetovanja z deležniki organizacije, kar naš model dosega prav z segmentiranjem javnosti. ISO 31000 to pomembnost opisuje: 'Komunikacija in posvetovanja z deležniki je pomembna, saj le-ti ocenjujejo tveganja glede na svoje percepcije tveganja. Te percepcije se lahko razlikujejo zaradi različnih vrednot, potreb, domnev, konceptov in skrbi deležnikov. Ker lahko imajo njihovi pogledi ključen vpliv na sprejemanje odločitev, morajo biti deležnikove percepcije prepoznane, zapisane in upoštevane v procesu odločanja.' [7]

Segmentiranje tveganj glede na izvor

Oskrbovalna veriga je kompleksen sistem več organizacij, ki skupaj delujejo v določenem okolju, kjer se 'srečujejo z zunanjimi in notranjimi vplivi in faktorji, ki vplivajo na negotovost glede doseganja ciljev organizacije' [7]. Na podlagi obsega izvora posameznega tveganja lahko tveganja razdelimo po naslednji dimenziji, to je glede na izvor. V tej dimenziji tveganja delimo na skupine, ki izhajajo iz:

1. Opazovane organizacije, ki je vključena v oskrbovalno verigo;
2. Celotne opazovane oskrbovalne verige (ampak ne samo iz določene organizacije); ali

3. Iz zunanjega okolja, v kateri deluje oskrbovalna veriga.

Vsaka organizacija je odvisna od več tretjih oseb oziroma zunanjih organizacij. Kot del oskrbovalne verige je organizacija navadno tesno povezana in odvisna od drugih organizacij v določeni oskrbovalni verigi, manj pa z organizacijami zunaj nje. Zatorej mora vsaka organizacija razumeti, da imajo nanjo organizacije, ki so povezane v oskrbno verigo, določen vpliv, prav tako je opazovana organizacija vpliva na ostale organizacije v verigi. Zavedati se je potrebno, kot pravi tudi Andrew Steward, da odvisnosti same tudi pomenijo tveganje, saj po definiciji drži, da če smo odvisni od nekoga, lahko ta deluje tako, da bodo posledice tega delovanja imele negativni učinek na nas [26]. Isti avtor prepoznava tudi dejstvo, da odvisnosti pogosto niso prepoznane kot tveganja in jih ne upoštevamo v procesu ocenjevanja tveganj ali jih ignoriramo zaradi političnih razlogov; ta tveganja so hkrati bolj subtilna in se pojavljajo samo pri analizi poslovnih procesov, ne pa pri analizi tehnoloških komponent ali infrastrukture.

Segmentiranje tveganj glede na poslovno ali tehnološko dejavnost

Vse dejavnosti znotraj organizacije lahko opišemo kot pretežno tehnološke ali pretežno poslovne. V skladu s tem lahko tudi tveganja opišemo kot pretežno poslovna ali pretežno tehnološka, neizogibno pa se pojavijo tudi nekatera tveganja, ki imajo značilnosti obeh, torej jih opišemo kot univerzalna. Ta opis predstavlja še dodatno dimenzijo v našem modelu.

Seznam prepoznanih tveganj, njihove definicije po dimenzijah in dodatni opisi skupaj tvorijo bazo za katalog tveganj v oskrbovalnih verigah, ki je prosto dostopen in objavljen na internetu. Katalog je podrobneje opisan v nadaljevanju.

Nadaljnje definicije, ki so potrebne pri procesu ocenjevanja tveganj

Kot smo že omenili, so v procesu prepoznavanja, analize in ocenjevanja tveganj v specifični organizaciji potrebne še dodatne dimenzije, ki jih moramo uvesti, da dosežemo popolno razumevanje tveganj, njihovih povezav in vplivov. Te dimenzije so kratko opisane v nadaljevanju, v domeni vsake posamezne organizacije, ki se loteva ocenjevanja tveganj s pomočjo našega modela pa je, da jih implementira.

Zavedati se je potrebno, da so oskrbovalne verige prav tako raznolike kot današnji trg potrošnih dobrin. Na podlagi tipa dobrin ali storitev, ki jih dobavlja oskrbna veriga, lahko tveganja definiramo po dodatni dimenziji. Nekatera tveganja se pojavljajo univerzalno v vseh oskrbovalnih verigah, nekatere oskrbovalne verige pa imajo svoja specifična tveganja, na primer hladne verige, proizvodnja in prodaja nevarnih snovi in podobno.

Pri vrednotenju tveganj moramo med drugim definirati tudi njihov vpliv na specifične javnosti. Zavedati se je potrebno, da vsako tveganje na svoj način vpliva na neko javnosti ter da ta vpliv vsaka javnost drugače sprejema. Z analizo vplivov z ozirom na javnosti dosežemo boljši vpogled v posledice tveganja. Tu ne gre za isto dimenzijo ali isti postopek kot pri sami segmentaciji javnosti – ta dimenzija je poglobljena in išče tudi vplive in učinke tveganja na javnosti.

V realnih situacijah so tveganja in njihovi vplivi velikokrat odvisni od časa, v katerem se pojavijo. Zato mora model za ocenjevanje tveganj vključevati tudi dimenzijo časa, ki v proces prinaša nedeterminizem. V nekaterih časovnih okvirjih je lahko tveganje neznatno, medtem ko je isto tveganje v drugem časovnem okvirju ključno za uspešno poslovanje organizacije. V kolikor so takšni časovni okvirji prisotni, morajo biti v fazi ocenjevanja tveganj definirani, da pridobimo pregled nad spreminjanjem tveganja skozi čas.

Za vsako tveganje je potrebno določiti mejo sprejemljivosti. Pri tem

moramo upoštevati tudi časovno komponento, kjer je prisotna, da polno zajamemo vse nivoje potencialnega vpliva in znotraj njih pravilno določimo mejo sprejemljivosti.

Prepoznati moramo, da noben proces v organizaciji ne more potekati neodvisno od ostalih procesov. Enako velja za katero koli tveganje – nikoli ne obstaja tveganje, ki je izolirano in nima vpliva na procese znotraj organizacije in tudi znotraj oskrbovalne verige. Zato je potrebno definirati medsebojne odvisnosti med tveganji, kar predstavlja naslednjo dimenzijo organizacijsko specifičnega definiranja tveganj.

Splošna ideja upravljanja tveganj je, da mora imeti vsako prepoznano tveganje dodeljeno osebo ali skupino ljudi, ki so zadolženi za njegovo upravljanje in jih po navadi imenujemo lastniki tveganja. ISO 31000 definira lastnika tveganja kot "osebo ali entiteto z odgovornostjo in avtoriteto za upravljanje tveganja". Hkrati definira, da "mora organizacija zagotoviti, da obstajajo odgovornost, avtoriteta in primerne kompetence za upravljanje tveganj, ki omogočajo uvajanje in vzdrževanje kontrol za upravljanje tveganj in zagotavljajo primernost, učinkovitost in uspešnost teh kontrol." [7]. Z določitvijo specifične osebe, ki je odgovorna za določeno tveganje, dosežemo višjo stopnjo zavedanja pri tistih, ki morajo biti vključeni v proces upravljanja tveganj znotraj organizacije ali oskrbovalne verige.

6.3.2 Katalog tveganj v oskrbovalnih verigah

Končni produkt konvencionalnega prepoznavanja in ocenjevanja tveganj je katalog tveganj v oskrbovalnih verigah [19], ki vsebuje vsa prepoznana in opisana tveganja v določeni organizaciji. Težimo k temu, da vsa ta tveganja zberemo v katalog, ki je razširjen na raven celotne oskrbovalne verige oziroma na raven več oskrbovalnihih verig in je hkrati javno dosegljiv preko objavljenega spletnega kataloga tveganj v oskrbovalnih verigah, s čimer postane pomembno in uporabno orodje pri upravljanju tveganj. Proces upravljanja tveganj je velikokrat počasen in ne dovolj natančen, naša ideja

prosto dostopnega kataloga vseh do sedaj prepoznanih tveganj pa organizacijam nudi možnost, da pri procesu uporabijo tudi zunanja znanja, ko se lotevajo upravljanja tveganj. Katalog tveganj vsebuje logistična tveganja, ki so bila prepoznana v organizacijah z različnih področij delovanja, ravno zato je lahko odličen vir informacij za širok spekter organizacij, ki pristopajo k upravljanju tveganj, saj ga lahko uporabljajo kot smernice za prepoznavanje tveganj in kot kontrolni seznam ali odkljuknico, s katero ugotovijo, katera od že identificiranih tveganj lahko prepoznajo tudi znotraj svoje organizacije. Uporabo odkljuknice kot pripomočka pri ocenjevanju tveganj priporoča tudi standard ISO 31010, ki jo definira kot šeznam nevarnosti, tveganj ali napak pri kontrolah , ki je navadno sestavljen na podlagi izkušenj, najsi bo kot rezultat prejšnjih procesov upravljanja tveganj ali kot rezultat preteklih napak ali škodnih dogodkov" [8]. Na podlagi tega lahko ugotovimo, da je katalog, ki ga uvajamo, v skladu z načeli ISO 31010 in s celotno družino ISO 31000 standardov.

Potreba po takšnem katalogu logističnih tveganj je lahko vidna iz različnih perspektiv. Tudi ISO 31000 definira končni rezultat procesa prepoznavanja tveganj kot "obsežen seznam tveganj, ki vključuje dogodke, ki lahko povzročijo, povečajo, preprečijo, poslabšajo, pospešijo ali povzročijo zamudo pri doseganju ciljev organizacije" [7]. Organizacija lahko pristopi k procesu upravljanja tveganj samostojno, vendar velikokrat zaradi prevelikega obsega potrebnih aktivnosti k njemu ne pristopijo in se odločijo, da bodo obstoj tveganj in njihovo upravljanje spregledali. S pomočjo kataloga kot vira izkušenj in odkljuknice je velik korak v procesu ocenjevanja tveganj že narejen, kar omogoča organizaciji pristop k celovitemu upravljanju tveganj z manj preprekami in z več znanja. Vidimo lahko, da katalog, ki je trenutno edinstven v svetu, predstavlja ključen napredek pri upravljanju tveganj v logistiki na svetovnem nivoju.

Ker verjamemo, da mora biti vir s takšno pomembnostjo prosto dostopen vsem potencialnim uporabnikom, je objavljen pod licenco Creative

Commons, ki uporabnikom dovoljuje, da katalog prosto gledajo, nalagajo in delijo, ne smejo pa ga spreminjati brez odobritve in uporabljati za pridobitne namene, seveda pa morajo pri tem primerno navesti avtorja kataloga. Licenca, pod katero je objavljen, se imenuje 'Attribution – NonCommercial – NoDerivs. Ker je naša filozofija za katalogom takšna, da je to publikacija, ki iz dneva v dan raste in se spreminja, verjamemo, da je potrebno omogočiti vsem uporabnikom, da h katalogu prispevajo, ga komentirajo ali predlagajo dodatke. Zato vse uporabnike spodbujamo, da svoje predloge posredujejo uredniškemu odboru, ki predloge oceni in jih nato vnese v katalog, če so primerni. Pripombe se sprejemajo preko elektronskega naslova SC.RiskCatalog@gmail.com. Upamo, da bomo s tem dosegli širok interes za uporabo kataloga med strokovnjaki s področja oskrbovalnih verig, hkrati pa dodatno povečali njegovo kakovost in obseg. Vsak vodilni v oskrbovalnih verigah se mora zavedati pomembnosti sodelovanja med organizacijami. Ena sama organizacija nikoli ne more prepoznati toliko tveganj, kot jih lahko skupina organizacij, še posebej kadar govorimo o tveganjih v oskrbovalnih verigah. Naš cilj je zato povezati strokovnjake s celega sveta in vzpostaviti skupnost z enotnim ciljem – zagotavljati nova znanja na področju ocenjevanja logističnih tveganj in izpolnjevati katalog tveganj.

Katalog je dosegljiv na spletnem naslovu http://labinf.fl.uni-mb.si/riskcatalog [19]. Tu je podan obsežen seznam do sedaj prepoznanih tveganj, ki so opisana po zgoraj definiranih dimenzijah. Dodatno so podani opisi dimenzij in šifranti kategorizacije. Pri vsaki šifri kategorije znotraj dimenzije so podana tudi vsa tveganja, ki se uvrščajo v to kategorijo, da je katalog lažje pregleden tudi po posameznih kategorijah.

Spletna stran kataloga vsebuje štiri zavihke. Prvi je pozdravni (Welcome) z osnovnimi informacijami o katalogu. Drugi predstavlja podatke (Data), kjer so navedena vsa zaznana tveganja. Seznam teh tveganj se sproti dopolnjuje. Tveganja je mogoče sortirati po vseh kategorijah. Sledi

zavihek z opisom modela (Model). Zadnji vsebuje vse ključne informacije o samem katalogu – to je kolofon kataloga, o Creative Commons License in s povabilom za sodelovanje pri dopolnjevanju kataloga s podatki in razvijanjem modela.

Slika 6.7 prikazuje del zavihka s podatki o tveganjih, medtem ko slika 6.8 prikazuje del strani, kjer je opsian sam model, na katerem je katalog izdelan.

6.3.3 Zaključna diskusija o Katalogu

Na podlagi današnjih negotovih tržnih pogojev, zahtev globalizacije in vedno večjih zunanjih groženj lahko zaključimo, da lahko samo z učinkovitim upravljanjem tveganj v oskrbovalnih verigah zagotovimo kontinuiteto poslovanja organizacije. Upravljanje tveganj mora predstavljati prioriteto v vsaki organizaciji in mora biti vključeno v vse vidike poslovanja, če želimo zagotoviti njegovo uspešnost in učinkovitost. Vodilni se morajo zavedati groženj, ki pretijo organizaciji, prav tako pa morajo poznati in implementirati orodja, s katerimi jih lahko upravljamo in obvladujemo.

Naš model za ocenjevanje tveganj dovoljuje vodilnim, da k upravljanju tveganj pristopijo na poenostavljen način, kjer so vsi potrebni koraki opisani, hkrati pa že imajo tudi razdelan osnovni seznam potencialnih tveganj. Spletni katalog tveganj v oskrbovalnih verigah, ki je prosto dostopen vsem, uporabnikom nudi enostavno odkljuknico s tveganji, kot so jih prepoznali in definirali strokovnjaki s področja logistike. Med ocenjevanjem tveganj v specifični organizaciji je potrebno dodati še nekaj dimenzij, ki jih ni mogoče posplošiti in zatorej niso v obsegu kataloga. S tem dosežemo dodatno razumevanje tveganj in boljši izhodiščni vhod v procese upravljanja tveganj. Verjamemo, da razvit model in posledični katalog, še posebej z uvedbo težišča na ljudi in javnosti, predstavljata izjemen vir za upravljanje tveganj v vseh organizacijah in oskrbovalnih verigah.

Ker verjamemo, da lahko skupina strokovnjakov v večjem obsegu za-

login

Login

University of Maribor

Faculty of Logistics

article

Supply Chain Risk Catalog

Welcome | Data | Model | About

Below, you can find all data currently a part of the risk catalog. The included risks were identified and analysed in accordance with the model, which you can find here.

The table below is sortable by different columns, you can sort a column alphabetically by clicking on the column header.

Risk	Group according to ISO 28000	Secondary group according to ISO 28000	Primary logistics resource	Secondary logistics resource	Primary public	Secondary public	Origin of risk	Level of logistics planning	Source of risk	Area of impact	Risk cause	Po co
Limited or no access to the key locker	a.PHY		ISL		OPE		COM	OPL				
Fall of wall/ceiling	a.PHY		ISL		IMP	OPE	OSC	TPL				
Collapse of tent	a.PHY		ISL		IMP	OPE	OSC	TPL				
Planted bomb or explosive	a.PHY		ALS		ALL		OSC	OPL				
Damage to the forklift ramp	a.PHY		ISL	FLW	OPE		COM	OPL				
Damage of cranes, lifts	a.PHY		ISL	FLW	MNG	OPE	COM	OPL				
Collapse of the roof (snow)	a.PHY		ISL	FLW	IMP	OPE	OSC	TPL				

Slika 6.7: Izsek strani na zavihku s podatki v Katalogu tveganj oskrbovalnih verig [19]

Risk analysis is the second step in risk assessment, where the risk catalog also represents a valuable resource for organizations. ISO 31000 defines the purpose of risk analysis as developing an understanding of the risk. In our model, risks are described by different dimensions which define their attributes and provide information about general risk properties. We also propose some organization specific dimensions of definig risks during risk analysis, which every organization has to define in the frame of its specific external and internal context.

Risk evaluation as the final step of risk assessment as defined in ISO 31000 is the process of deciding about which risks need treatment and the priority for treatment implementation. This step can not be generalized and is therefore not in the scope of this risk catalog, but is entirely dependant on specific organizations.

Risk catalog

With our model we developed a tool for companies that are prepared to combine internal and external knowledge for identifying and defining risks.

The Risk catalog that represents the final product of this process, can be a permanent and valuable tool for a company's and supply chain's risk management processes. The catalog has to be examined and complemented on a regular basis to ensure actuality. It provides a base for risk management processes throughout the chain.

The current catalog with its identified risks is accessible here.

Dimensions of risk definition

List of groups by ISO 28000

This model is structured so that it complements an international standard on security in supply chains, ISO 28000. In this standard, several fields from where risks to a company or a supply chain can originate are defined. Each identified risk is placed in one of these groups.

Code	Description
PHY	Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action.
OPT	Operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety.
NAT	Natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective.

Slika 6.8: Izsek strani na zavihku z opisom modela v Katalogu tveganj oskrbovalnih verig [19]

gotovi potrebna znanja in izkušnje, na podlagi katerih lahko izpopolnimo model in katalog, je spletni katalog z opisom modela prosto dostopen preko spleta. Managerje in ostale strokovnjake s področja logistike in upravljanja tveganj spodbujamo, naj pri svojem delu uporabljajo katalog, v zameno pa nam sporočijo svoje pripombe, ideje in dopolnitve, da bomo skupaj dosegli vedno boljši in popolnejši spletni katalog tveganj v oskrbovalnih verigah.

Poglavje 7

IT investicije

Trend investicij, namenjenih razvoju informacijskih tehnologij (IT) v svetu in pri nas še vedno narašča [27]. IT investicije omogočajo [4]:

- vzdrževanje obstoječega poslovanja,
- njegovo povečanje ali
- spremembo poslovanja.

V večini primerov je skupni imenovalec poslovnih investicij ta, da velik ali celo pretežni del poslovne investicije predstavlja IT investicija, saj se v večini primerov IT izrazi kot poslovno kritična komponenta. Zato je pomen konkretnih poslovnih koristi podjetja ob IT investicijah tako velik [4]. Še več: pomembno je upravljanje IT investicije v njenem celotnem življenjskem ciklu v okviru upravljanja poslovnih investicij – tako IT investicijo naj ne bi obravnavali kot samostojno celoto, temveč le kot investicijo, vpeto v mrežo drugih poslovnih investicij. Vsaka IT investicija mora imeti jasno poslovno korist, mora prispevati k poslovnim ciljem podjetja in mora biti ocenjena skozi prizmo doprinosa k poslovnim ciljem. Imeti mora svojo upravičenost in pričakovano razmerje med vložkom in koristnostjo.

Predpogoj za določanje poslovne koristi IT investicije je, da pri odgovornih za poslovne investicije (to je poslovodstvo) dosežemo, da le ti razumejo, na kakšen način IT prispeva k doseganju zastavljenih poslovnih ciljev. Na vseh nivojih upravljanja podjetja in vsem nivojem upravljanja posamezne investicije mora biti jasno, na kakšen način in v kolikšni meri lahko investicije v IT omogočijo realizacijo posameznih poslovnih ciljev podjetja.

Do sedaj je manjkal strukturiran pristop, orodje ali ogrodje, namenjeno vodstvenemu kadru ali vodjem posameznih poslovnih investicij, ki bi bilo dovolj splošno, strukturirano in bi temeljilo na preizkušenih vzorcih upravljanja tako, da bi IT investicije upoštevalo kot sestavni del celotne poslovne investicije. Z Val IT smo dobili želeno ogrodje za upravljanje IT investicij.

Pogled na IT se skozi čas spreminja in še do nedavnega smo ocenjevali kakovost IT v luči dejavnikov, ki kažejo na uspešnost IT pri podpori izvajanju poslovnih procesov – nič več in nič manj. Ker danes skupaj z dopolnjeno optiko ocenjevanja uspešnosti poslovanja na IT gledamo tudi skozi prizmo uspešnosti investicij v IT, ne gre več samo za implementacijo IT rešitev. Vedno bolj se zavedamo, da gre za implementacijo nekaterih poslovnih sprememb, ki jih omogoča IT investicija. IT investicija postane del, ki je potreben za doseganje poslovnih rezultatov. V okviru ocenjevanja uspešnosti poslovne investicije začenjamo ocenjevati uspešnost investicije v IT. S tem se je osredotočenost zanimanja v svetu IT dodatno razširila na spremljanje uspešnosti IT investicij. Osrednji pojem v IT postane nova vrednost, ki jo pridobimo z IT investicijo. Sprašujemo se o koristih, ki jo IT investicija doprinese kot nova poslovna vrednost podjetja. Pri tem ne pozabimo, da gre pri IT investicijah tako za vzdrževanje kakor tudi za povečanje ali spremembo poslovanja.

Zaradi ocenjevanja IT investicij smo se začeli zavedati, da so IT tveganja bistveno kompleksnejša in pomembnejša, kot smo jih bili vajeni videti

in sprejemati v preteklosti. Po eni strani gre za evolucijo, prek katere spoznavamo in priznavamo nove elemente vpliva, ki jih ima IT na samo poslovanje, po drugi strani pa gre za dejstvo, da IT s časom enostavno predstavlja večji in pomembnejši delež poslovanja, s čimer se veča tudi utež vpliva same IT na poslovanje. Nadaljnja posledica se kaže tudi v zahtevi po spremembi upravljavskih praks – tudi upravljavskih praks v IT. Prakse, ki so bile še do včeraj aktualne, postajajo premalo kompleksne in nezadostne. Še včeraj namreč nismo investicijam v IT namenjali tolikšne pozornosti, kot jo zahteva današnji čas. Videti je, kot da postaja proučevanje uspešnosti investicij v IT osrednja tema, s katero se ukvarjajo ali se bodo ukvarjali vodje IT v podjetjih. Pri tem gre tako za javna kot za zasebna podjetja. Pri obeh je razlika samo v tem, da je ocenjevanje uspešnosti investicij v IT v javnem sektorju težje, saj gre pri javnih organizacijah za poudarjeno večplastnost ocenjevanja, kar prispeva k povečani kompleksnosti ocenjevanja.

7.1 Upravljanje IT investicij s pomočjo Val IT

Tako praksa kakor empirične raziskave kažejo, da pri investicijah, ki jih upravljamo v okviru učinkovitega nadzornega ogrodja, dosežemo bistveno boljše rezultate, kakor če jih izvajamo brez nadzornih pristopov in ogrodij. Povedano drugače, podjetja dosegajo svojo želeno in pričakovano poslovno korist predvsem z:

- izbiro pravih investicij ter z
- učinkovitim upravljanjem izbranih investicij.

Upravljanje investicij se začne že v fazi koncipiranja investicije in traja vse do njene implementacije ter navsezadnje do posledičnih doseženih poslovnih koristi, ki so relativne glede na vrednosti, ki jih pričakujemo od investicije. Učinkovitega upravljanja ni mogoče izvajati brez učinkovitega

nadzora. Brez obojega, učinkovitega upravljanja in nadzora, namreč obstaja velika možnost, da investicije ne prinesejo koristi. Še več, slabo nadzorovane investicije vodijo v izgube.

Iz tega preprosto sklenemo: investicije v poslovne rešitve, ki so podprte z IT ali predvsem z IT, se lahko mnogokratno povrnejo, vendar samo ob zagotavljanju izvajanja ustreznih aktivnosti nadzora in upravljanja in ob popolni podpori in vključenosti vodstva podjetij na vseh ravneh vodenja. Vodstva v preteklosti niso imela dobrega pregleda nad vlaganji v IT. Praksa poročanja in vrednotenja IT vlaganj je bila pomanjkljiva. Takšna slaba praksa sicer še danes prevladuje, vendar se z vrednotenjem uspešnosti IT investicij praksa sama po sebi spreminja. Uspešnost investicij – mednje uvrščamo tudi IT investicije – namreč vodstva dobro razumejo in želijo razpolagati s poročili o njihovi uspešnosti.

Zaradi pomanjkanja predstave o tem, kaj so IT investicije, in zaradi problemov, ki nastanejo ob vrednotenju uspešnosti IT investicij, so pri IT Governance Institute raziskovali možnosti za izboljšanje obstoječega stanja. Dela so se lotili s pomočjo strokovnjakov iz poslovne in IT sfere. Nastala je tako imenovana Val IT iniciativa. Cilj je bil, da bi s to iniciativo vodstvom podjetij zagotovili različne smernice, ki so povezane z IT investicijami. Usmeritve so pripravili tako, da je mogoče zagotavljati večjo optimalnost IT investicij v okviru poslovnih rešitev ob znanih in sprejemljivih tveganjih. [7] Val IT je ogrodje z medsebojno komplementarnimi in dopolnjujočimi procesi ter drugimi navodili za upravljanje IT investicij, ki so prilagojena vodstvu upravljavske piramide. Procesi in navodila so pisani v jeziku vodstva na način, ki ga vodilni razumejo in uporabljajo. Ob tem so razpoznavne posamezne vloge članov vodstva ob IT investicijah.

Val IT je komplementaren COBIT-u. Slednjega poznamo že dlje časa. Obe ogrodji tvorita skupaj splošno, a vsestransko razvejano ogrodje, namenjeno nadzoru in upravljanju IT.

Val IT nam koristi, ko se osredotočamo na investicije in se sprašujemo:

1. Ali delamo prav? Ali so investicije pravilne? Pri tem gre za strateška vprašanja, med katerimi so pomembna še naslednja vprašanja povezana z IT investicijo:

   (a) Ali z odločitvijo o izbrani investiciji še podpiramo začrtano poslovno in IT vizijo?

   (b) Ali smo še konsistentni v principih naše poslovnosti?

   (c) Ali prispevamo k strateškim ciljem podjetja?

   (d) Ali zagotavljamo optimalno in/ali pričakovano povečanje poslovne koristi, upoštevajoč sprejemljiv vložek ob sprejemljivem nivoju tveganja?

2. Kolikšne in kakšne so dejanske koristi od investicije? Kolikšne in kakšne so glede na pričakovane? Gre za vprašanje poslovne koristi, v okviru katere se sprašujemo:

   (a) Ali je vsem, ki bi jim moralo biti, razumljivo, kaj pričakujemo od investicije? Je povsem jasno, kaj z investicijo želimo pridobiti?

   (b) Ali je vsem, ki bi jim moralo biti, razumljivo, kaj moramo storiti, kaj in koliko moramo vložiti v realizacijo IT investicije, da bi pridobili predvidene koristi?

   (c) Ali je metrika ocenjevanja uspešnosti IT investicije relevantna?

   (d) Ali je proces za dosego zastavljenih poslovnih koristi dovolj dobro zastavljen?

Po drugi strani se COBIT osredotoča na izvajanje IT procesov, ob katerih se sprašujemo:

1. Ali delamo pravilno? Gre za vprašanje arhitekture IT, v okviru katerega se v zvezi z IT investicijo sprašujemo:

   (a) Ali smo usklajeni z obstoječo arhitekturo?

   (b) Ali smo konsistentni z našimi arhitekturnimi principi?

   (c) Ali kaj prispevamo k izboljšanju naše arhitekture v celoti?

   (d) Ali smo usklajeni z ostalimi (lahko tudi zakonodajnimi) zahtevami?

2. Izvajamo IT procese dovolj dobro? Pri tem se sprašujemo o kakovosti servisov (ali storitev), ki jih nudimo z naslednjima vprašanjema:

   (a) Ali so naši delujoči procesi upravljanja in zagotavljanja servisov učinkoviti? Ali imamo učinkovit proces za izvajanje sprememb in dopolnitev v IT?

   (b) Ali imamo dovolj kakovostne, izobražene, vpeljane in razpoložljive tehnične in upravljavske človeške vire, s katerimi smo zmožni:

      i. Nuditi zahtevane servise v zahtevanih kakovostnih okvirih?

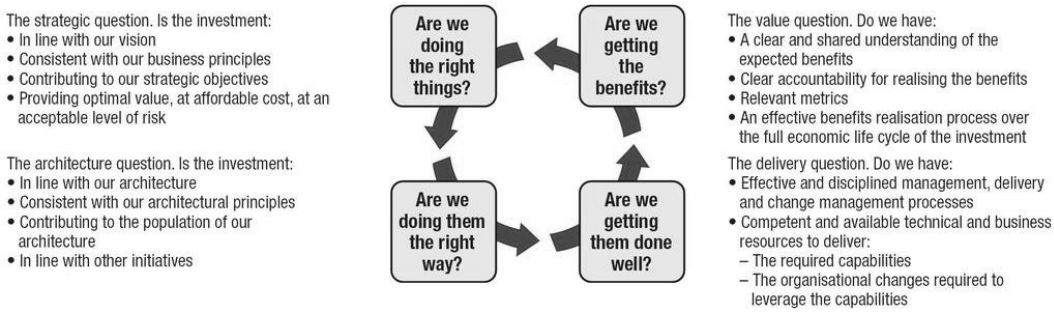
      ii. Izvajati organizacijske spremembe, ki so za izvedbo potrebnih sprememb in/ali dopolnitev?

Z zgornjimi vprašanji je prikazana osredotočenost obeh ogrodij: Val IT in COBIT. Razvidno je, da Val IT predstavlja nadgradnjo COBIT z vidika poslovne in finančne perspektive. Tako oba, Val IT in COBIT, združujeta najobsežnejši sistem spoznanj in dobrih praks, ki so nam trenutno na voljo v IT. Njihovo medsebojno odvisnost prikazuje slika 7.1.

7.2 Predstavitev Val IT

Pri uporabi Val IT se srečujemo z/s:

1. Osnovnimi pojmi, kot so poslovna korist, projekt, program, portfelj.



Slika 7.1: Štiri osnovna vprašanja s podvprašanji, ki si jih zastavljamo pri uspešnem upravljanju IT [4]

2. Principi, ki so značilni tako za investicije, ki vsebujejo IT, kakor za prakse doseganja (pričakovanih) poslovnih koristi.

3. Področji, v okviru katerih s posameznimi Val IT procesi upravljamo poslovne koristi, IT portfelj in IT investicije.

4. Procesi, ki jih definira Val IT

5. Navodili za upravljanje (kdo, kaj, kdaj, kje, kako, zakaj, ipd) za vsak Val IT proces posebej.

7.2.1 Osnovni pojmi

Val IT uporablja pojem "vrednost"ali poslovna korist kot osrednji pojem. Zato je smiselno še enkrat poudariti, da je koncept pojma "vrednost"kompleksen – je vsebinsko odvisen in seveda dinamično spreminjajoč skozi čas. Poslovna korist se spreminja tudi glede na različne perspektive opazovanja in glede na trenutno percepcijo opazovalca. Narava vrednosti ali poslovne koristi se spreminja glede na posamezno podjetje podobnega tipa in seveda še toliko bolj glede na različne tipe podjetij. Zagotovo so

poslovne koristi in vrednostni kriteriji v organizacijah javnega sektorja drugačni od profitno naravnanih podjetij. Zato moramo določiti metriko, s katero merimo posamezne poslovne koristi.

Takšno metriko je seveda potrebno tudi neprestano dopolnjevati in po potrebi spreminjati skladno s spremembami ciljev in vrednostmi posameznih podjetij. Val IT metrike ne podaja in jo je treba izdelati v vsakem posameznem okolju posebej. Takšen pristop je samoumeven ljudem, ki izhajajo iz poslovnega okolja, in manj ljudem, ki izhajajo iz IT okolja.

Projekt je mišljen kot skupek aktivnosti, ki je usmerjen k izvedbi nekega vnaprej opredeljenega izdelka ali storitve. Projekt je potreben, vendar ne zadosten člen v mreži ostalih projektov, s katerimi želimo doseči zastavljene poslovne cilje v okviru dogovorjene višine porabe sredstev in v okviru dogovorjenih časovnih okvirjev. (Zanimivo, vendar ta definicija ne omenja kakovosti izdelkov in storitev.)

Program predstavlja mrežo medsebojno odvisnih projektov, ki so potrebni in zadostni za uresničitev nekega poslovnega cilja. Takšni projekti lahko vsebujejo tudi spremembo poslovanja, kakšnega poslovnega procesa, načina dela posameznikov, spremembo organizacijske strukture in kompetenc posameznikov, lahko omogočajo uporabo novih tehnologij in podobno. Investicijski program je tista osnovna enota Val IT, ki obravnava IT investicijo.

Portfelj predstavlja skupino objektov škupnega interesa", ki jih upravljamo s ciljem optimiziranja poslovne koristi. Ti objekti so investicijski programi, IT projekti, IT servisi in siceršnje IT premoženje in IT viri. Pri tem je portfelj investicij ključen pojem, s katerim se ukvarja Val IT. IT projekti, servisi, premoženje in viri pa so ključni pojmi, s katerimi se ukvarja COBIT.

7.2.2 Principi

Principi [7], na katerih temelji Val IT, so naslednji:

1. IT investicije moramo upravljati kot portfelj investicij.
2. IT investicije morajo upoštevati celoten spekter aktivnosti, potrebnih za doseganje poslovne koristi. Ne gre samo za upoštevanje aktivnosti iz spektra, ki ga definirajo IT procesi, temveč gre za upoštevanje spektra vseh aktivnosti, ki jih izvajamo pri poslovnih procesih, v okviru katerih je potrebna IT podpora.
3. IT investicije je potrebno upravljati skozi njihov celoten življenjski cikel (v okviru siceršnje poslovne investicije).
4. Za doseganje želenih poslovnih koristi je potrebno sprejeti dejstvo, da obstaja veliko različnih vrst investicij, ki jih je potrebno različno upravljati, pregledovati in ocenjevati – vsako vrsto posebej na svoj način.
5. Za doseganje želenih poslovnih koristi moramo definirati in stalno pregledovati ter ocenjevati ključne metrike tako, da se lahko hitro odzovemo na morebitne nepravilnosti ali siceršnje spremembe v načrtu.
6. Za doseganje želenih poslovnih koristi moramo vključiti vse sodelujoče pri investiciji tako, da so določene njihove odgovornosti, da so zagotovljeni pogoji za uspešno dokončanje investicije in za doseganje poslovnih dobičkov.
7. Za doseganje želenih poslovnih koristi moramo ciklično izvajati pregledovanje, ocenjevanje, vrednotenje rezultatov ocenjevanja in izboljševanje posameznih segmentov investicije.

7.2.3 Področja

Val IT definira več procesov, ki naj bi jih izvajali vsi sodelujoči v procesih, s katerimi dosegamo poslovne koristi (to so tisti, ki izvajajo poslovne procese

v katere smo investirali). Ti procesi so združeni v tri področja:

1. Procesi upravljanja vrednosti (z označbo VG).
2. Procesi upravljanja portfelja (z označbo PM).
3. Procesi upravljanja investicij (z označbo IM).

Upravljanje vrednosti

Cilj upravljanja vrednosti ali poslovne koristi je zagotavljanje, da so upravljavske prakse sestavni del poslovanja podjetja. S tem je mogoče zagotoviti optimiziranje IT investicij skozi njihov celoten življenjski cikel v okviru siceršnjega življenjskega cikla poslovne investicije. Če vodstvo podjetja želi delovati v smislu nadzorovanja poslovne koristi, mora:

- vzpostaviti okvir za upravljanje nadzorovanja poslovne koristi, ki mora biti integriran v upravljanje podjetja;
- zagotoviti strateške usmeritve za odločitve povezane z investicijami;
- definirati lastnosti portfeljev, ki predvidevajo IT investicije; ter
- neprestano izboljševati nadzor doseganja poslovnih koristi, tako da se pri tem učimo na napakah pri obstoječem delu in izboljšujemo svoje ravnanje v bodoče.

Upravljanje portfelja

Cilji, ki jih želimo doseči s procesi tega področja, so usmerjeni v zagotavljanje stanja, v katerem je celoten portfelj programov, projektov, servisov in premoženja usklajen z investicijami v IT in z ostalimi poslovnimi investicijami, ter kot taki prispevajo k doseganju želenih poslovnih koristi z:

- vzpostavitvijo in upravljanjem posameznih IT virov;

- definiranjem praga rentabilnosti posameznih IT investicij;
- ocenjevanjem IT investicij, postavljanjem njihovih prioritet; izbiro, zavrnitvijo ali odložitvijo novih IT investicij;
- upravljanjem celotnega IT portfelja; ter
- nadzorovanjem in poročanjem o učinkovitosti IT portfelja.

IT investicijske programe je treba upravljati kot portfelj investicij. Programi morajo biti jasno definirani, ocenjeni, prioritete morajo biti postavljene, izbrane in upravljane skozi njihov celoten poslovni življenjski cikel zato, da je mogoče optimizirati poslovne koristi v okviru vsakega posameznega programa in v okviru celotnega portfelja programov. To vključuje tudi razporeditev posameznih virov, upravljanje rizikov, zgodnje odkrivanje in odpravljanje problemov ter zaznavanje zmot na nivoju celotnega portfelja.

Upravljanje portfelja zahteva tudi uravnoteženje celotnega portfelja, saj različne kategorije investicij povzročajo različno stopnjo kompleksnosti, stopnjo samostojnosti in porabe sredstev.

Upravljanje investicij

Upravljanje IT investicij zagotavlja, da posamezni IT investicijski programi podjetja dajejo optimalne rezultate v okviru sprejemljivih vložkov in z znanimi in sprejemljivimi riziki. Te zahteve dosegamo z:

- identifikacijo poslovnih zahtev;
- razvojem čistih, jasnih in razumljivih predlogov za investicijske programe;
- analizo alternativ pri implementaciji programov;

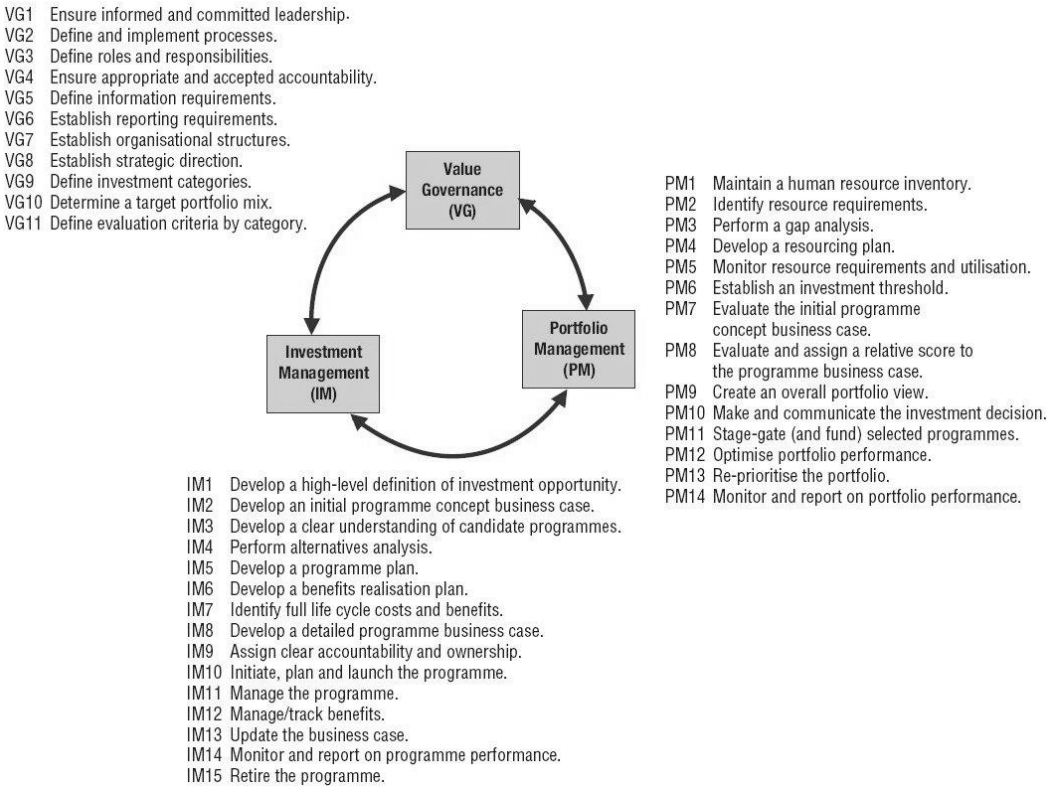
- definicijo in dokumentiranjem vseh programov ter podrobnim obravnavanjem posameznih poslovnih možnosti z detajlnim opisom vseh morebitnih dobičkov, ki jih je mogoče zaznati v življenjskem ciklu poslovne investicije;
- dodeljevanjem jasnih pooblastil in odgovornosti posameznikov;
- upravljanjem programov skozi njihov celoten poslovni življenjski cikel; ter
- nadzorovanjem in poročanjem o učinkovitosti programov.

7.2.4 Procesi Val IT

Vsa tri prej omenjena področja s posameznimi procesi prikazuje slika 7.2.

Procesi po posameznih področjih so naslednji:

1. VG Upravljanje vrednosti
   (a) VG1 – Vzpostavitev načina vodenja, ki zagotavlja informiranost in strinjanje z investicijo
   (b) VG2 – Definicija Val IT ogrodja za upravljanje in implementacijo Val IT procesov
   (c) VG3 – Definiranje lastnosti različnih portfeljev
   (d) VG4 – Integracija in prilagoditev upravljanja poslovnih koristi s finančnimi plani podjetja
   (e) VG5 – Vzpostavitev učinkovitega nadzora upravljanja
   (f) VG6 – Stalno izboljševanje praks upravljanja poslovnih koristi
2. PM Upravljanje portfelja
   (a) PM1 – Vzpostavitev poslovne strategije in ciljnih investicij



Slika 7.2: Zbirka dobrih praks, ki jih predvidevajo vsi trije procesi Val IT [4]

(b) PM2 – Iskanje možnosti za financiranje in določanje virov financiranja

(c) PM3 – Upravljanje iskanja človeških virov, potrebnih pri investiciji

(d) PM4 – Vrednotenje in izbira ustreznih programov

(e) PM5 – Nadzorovanje in poročanje o stanju portfelja investicij

(f) PM6 – Optimizacija portfelja investicij

3. IM Upravljane investicij

(a) IM1 – Razvoj in ocenjevanje koncepta začetnega poslovnega primera

(b) IM2 – Razumevanje drugega mogočega programa in različnih opcij implementacije

(c) IM3 – Razvoj plana za program

(d) IM4 – Razvoj načrta stroškov in koristi skozi celoten življenjski cikel

(e) IM5 – Razvoj podrobnega poslovnega primera drugega mogočega programa

(f) IM6 – Sprožitev in upravljanje programa

(g) IM7 – Posodobitev operativnega portfelja IT

(h) IM8 – Posodobitev poslovnega primera

(i) IM9 – Nadzorovanje in poročanje o stanju programa

(j) IM10 – Umik in ukinitev programa

7.2.5 Navodila za upravljanje

Navodila za vodstveni kader podjetja, ki jih prav tako podaja Val IT, so v pomoč pri upravljanju Val IT procesov. Navodila podajajo odgovore na tipična vprašanja vodilnih, kot so:

1. Kakšna je medsebojna odvisnost procesov in aktivnosti upravljanja poslovne koristi? Kaj so vhodi in izhodi procesov?
2. Katere so ključne aktivnosti, ki jih je potrebno v posameznem primeru upoštevati in ali jih je potrebno izboljšati? Kako in kaj meriti?
3. Katere vloge in odgovornosti morajo biti definirane za uspešno izvajanje upravljanja poslovne koristi?
4. Kako meriti in primerjati različno upravljanje poslovnih koristi?
5. Kateri in kakšni so indikatorji dobrega dela?

Za vsak proces Val IT vsebujejo navodila za upravljanje, vhode in izhode posameznih procesov, razlago posameznih aktivnosti s preglednico RACI (Responsible, Accountable, Consulted, Informed), cilje in metriko na različnih nivojih.

Poglavje 8

Dokumentni sistemi[1]

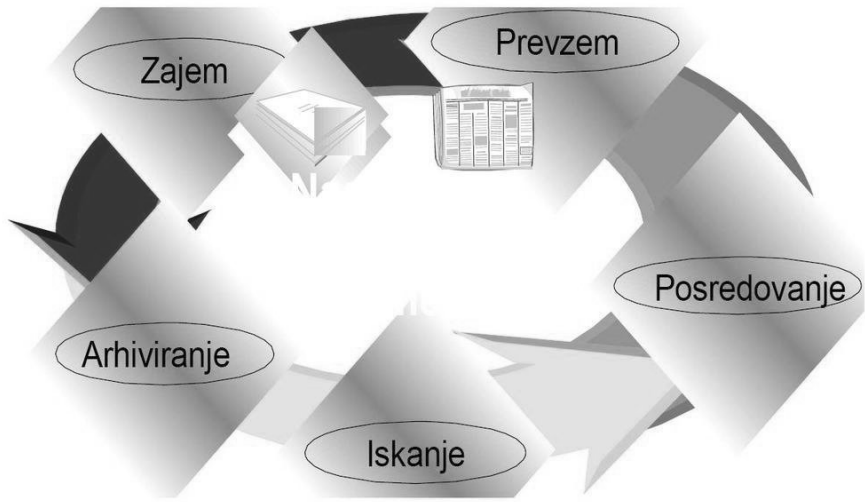
Elektronski dokumentni sistemi (EDMS – Electronic Document Management Systems) so računalniški sistemi za podporo poslovanja z elektronskimi in/ali papirnatimi dokumenti.

8.1 Življenjski cikel dokumentov

Osnovne funkcije dokumentnega sistema (glej sliko 8.1) so:

1. Vnos in zajem podatkov, ki vključuje tudi upodobitev dokumentov
2. Nadzor nad dostopom do dokumentov ali do njihovega dela. Pri tem ločujemo vsaj nadzor do zmožnosti branja in/ali popravljanja.
3. Življenjski cikel dokumenta (Workflow). Kdo kdaj kaj lahko v katerem delu ali fazi poslovnega procesa počne z dokumentom in kaj če ne napravi tistega, kar bi moral.
4. Obdelava dokumenta (OCR na primer)

[1] Avtorja: Mag. Mateja Izlakar in Dr. Borut Jereb



Slika 8.1: Življenjski cikel dokumentov (lasten vir)

5. Pregledovanje in posredovanje po, v življenjskem ciklu, predvidenih poteh.

6. Arhiviranje

8.2 Zakonodaja in notranja pravila

Cilj vsakega naprednega podjetja čim hitrejši prehod s papirnega v elektronsko poslovanje. Prehod želi narediti tako pri obvladovanju dokumentov v delovnih procesih kot tudi pri varni hrambi gradiva.

Tako dandanes večine vrst gradiv ni več potrebno hraniti v papirni obliki. To je mogoče v primeru, če zadostimo zakonodaji, kar pomeni, da sestavimo svoja notranja pravila, ki jih Arhiv RS potrdi. Notranja pravila so pravila igre in postopki, ki jih izvajamo pri izvajanju spremljevalnih storitev, to je pri zajemu in pretvorbi gradiva ter pri hrambi gradiva v

elektronski obliki. Te postopke moramo izvajati skladno z zakonodajo, ki je naslednja: Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA, Ur.l. RS, št. 30/2006), Uredba o varstvu dokumentarnega in arhivskega gradiva (Ur.l. RS, št. 86/2006) in Enotne tehnološke zahteve (ETZ), ki jih je izdal Arhiv RS in govorijo o načinih in organizaciji hrambe gradiva. Z izvajanjem postopkov, skladnih z zakonodajo, zagotavljamo gradivu dostopnost, uporabnost, avtentičnost in celovitost ter s tem vzpostavljamo pogoje za to, da gradivu v elektronski obliki zagotovimo pravno veljavo.

8.3 Dokumenti in gradivo

Kaj je dokument? Dokument je izviren ali reproduciran (pisan, risan, tiskan, fotografiran, fonografski, v elektronski obliki ali kako drugače zapisan) zapis, ki je bil prejet (vhodni dokument) ali je nastal pri delu družbe (lastni dokument, ki je lahko tudi izhodni dokument) in je pomemben za njeno poslovanje. Sestavi del dokumenta so tudi priloge, ki pojasnjujejo in dokazujejo vsebino dokumenta.

Dokumenti nastajajo, ko dejstva in dogajanja dokumentiramo. Pišemo zato, da imamo dokaze. Dokaze potrebujemo, ko iščemo resnico, utemeljujemo poslovne odločitve, dokazujemo dogovore in dejstva, dokazujemo, kako smo ravnali in da smo ravnali skladno s prepisanimi postopki.

Dokumenti in podatki sestavljajo gradivo. Dokumentarno gradivo je izvirno in reproducirano (pisano, risano, tiskano, fotografirano, filmano, fonografirano, magnetno, optično ali kako drugače zapisano) gradivo, ki je bilo prejeto ali je nastalo pri delu družbe. Arhivsko gradivo pa je dokumentarno gradivo, ki ima trajen pomen za znanost in kulturo ter pravno varnost oseb v skladu s strokovnimi navodili pristojnih arhivov.

8.4 Arhiviranje gradiva

Gradivo v papirni obliki, pa tudi gradivo, hranjeno na drugih analognih in digitalnih nosilci, hranimo v arhivskih prostorih. Ločimo dve vrsti arhivskih prostorov.

Priročni arhiv je arhivski prostor, v katerem se hrani gradivo, pomembno za tekoče poslovanje. Navadno se nahaja v bližini delovnega mesta. V njem se hranijo nerešene zadeve in zaključene zadeve, pri katerih je pogostost dostopov velika.

Glavni arhiv je osrednji arhivski prostor družbe, v katerem se hranijo zaključene zadeve. Dokumentarno gradivo se v glavnem arhivu hrani najmanj do izteka minimalnih rokov hrambe ali morebitne izročitve arhivskega gradiva državnemu arhivu. V glavnem arhivu se hrani le izvirno dokumentarno gradivo. Kopij v glavnem arhivu naj ne bi hranili.

Arhivski prostori glavnega arhiva morajo biti ustrezno zavarovani pred vlomom, tatvino, požarom, vdorom vode in drugimi škodljivimi vplivi, ki bi lahko povzročili uničenje ali poškodovali dokumentarno gradivo. V teh prostorih je potrebo zagotavljati tudi primerno temperaturo in vlago. Za glavni arhiv skrbi arhivar.

Prenos dokumentarnega gradiva iz priročnih arhivov v glavni arhiv se izvede enkrat letno, praviloma na začetku vsakega leta za preteklo poslovno leto.

Dokumentarno gradivo se po vsebinskih in drugih kriterijih združuje v vrste dokumentarnega gradiva. Vsaka vrsta gradiva ima v klasifikacijskem načrtu opredeljen rok hrambe. Klasifikacijski načrt je osnovni in najpomembnejši šifrant za razporejanje gradiva družbe. Primer klasifikacijskega načrta prikazuje preglednica 8.1:

Klasifikacijski znak je enolična oznaka vrste gradiva. Vsaka vrsta gradiva je v klasifikacijskem načrtu opisna še z imenom in rokom hrambe gradiva.

Klasifikacijski znak	Opis vsebine	Rok hrambe
1	KADRI	
10	Delovna razmerja	
100	Personalne mape	T
101	Štipendiranje	5 let
11	Izobraževanje	5 let
2	FINANCE IN RAČUNOVODSTVO	
20	Računi	10 let

Tabela 8.1: Klasifikacijski načrt

Rok hrambe gradiva je opredeljen z njegovo poslovno vrednostjo. V klasifikacijskem načrtu so navedeni minimalni roki hrambe gradiva. Minimalni rok hrambe je najmanjše število let obvezne hrambe gradiva. Podlaga za določitev rokov hrambe so zakoni, njihovi izvedbeni predpisi in interni predpisi družbe. Opredeljeni so s številom let (x let), z oznako trajno (T) ali arhivsko (A). Minimalni roki hrambe dokumentarnega gradiva se ne smejo skrajševati, lahko pa se podaljšujejo

Dokumentarno gradivo, ki so mu potekli minimalni roki hrambe in ga ni potrebno hraniti trajno ter ni bilo določeno kot arhivsko gradivo, se uniči. Dokumentarno gradivo, ki ima poseben pomen za poslovanje družbe, pa se hrani trajno.

Maksimalni roki hrambe dokumentarnega gradiva se določajo pri tistih vrstah dokumentarnega gradiva, ki vsebujejo osebne podatke. V primeru, ko gradivo vsebuje osebne podatke, je minimalni rok hrambe hkrati tudi maksimalni rok hrambe. Po preteku maksimalnega roka hrambe je treba gradivo izločiti iz arhiva in uničiti.

8.5 Spremljevalne storitve

Spremljevalne storitve imenujemo storitve, ki so povezane s hrambo gradiva v elektronski obliki, kot na primer zajem dokumentov, pretvorba dokumentov (iz papirne v digitalno obliko ali iz ene digitalne oblike v drugo digitalno obliko), zajem podatkov z dokumentov, uničevanje dokumentov. Sama hramba gradiva v digitalni obliki ne šteje med spremljevalne storitve.

Vendar je pa vsaj nekatere spremljevalne storitve potrebno izvajati za to, da zagotovimo elektronsko hrambo gradiva. Dokumente v papirni obliki zajamemo (skeniramo) in jih pretvorimo v elektronsko obliko. Ob tem se zastavljata dve vprašanji: katere vrste dokumentov je smiselno hraniti v elektronski obliki in v katerem trenutku njihovega življenjskega cikla jih je najbolj smiselno zajeti in pretvoriti v elektronsko obliko.

Če želimo zmanjšati obseg papirnega gradiva in arhivskih prostorov, v katerih hranimo papirno gradivo, je v elektronski obliki smiselno hraniti čim več dokumentov. Še posebno velik učinek dosežemo s tem, da v elektronski obliki hranimo dokumente, ki jih je treba hraniti dolgo časovno obdobje, 10 let in več, celo trajno.

Odgovor na drugo vprašanje pa se ponuja sam po sebi. Prej ko zajamemo in pretvorimo dokument v elektronsko obliko, manj imamo opravka s papirjem. Najučinkoviteje je, da dokumente zajamemo in pretvorimo ob njihovem nastanku ali prejemu, torej čim bolj na začetku njihovega življenjskega cikla. Cilj takega ravnanja je, da dokument na čim bolj učinkovit način prepotuje pot od svojega nastanka do elektronskega arhiva. Da bi bilo to res mogoče, je potrebno zagotoviti še avtomatizirano podporo procesom. Dokumenti namreč vstopajo v različne poslovne procese in če želimo doseči, da bo ravnanje z dokumenti učinkovito ter dostop do dokumentov hiter, enostaven in varen, je tudi procese, v katerih nastopajo ti dokumenti, treba informacijsko podpreti.

Kadar dokumente zajemamo na vhodu v podjetje, je pomembno, da

Signirni znak	Naziv delovnega mesta
1	UPRAVA DRUŽBE
100	Direktor družbe
101	Izvršni direktor
2	PROJEKTNA PISARNA
200	Vodja projektov
201	Svetovalec
3	PRODAJA
300	Vodja prodaje
301	Skrbnik ključnih kupcev
302	Skrbnik strank
4	TRŽENJE
400	Vodja trženja
401	Asistent v trženju
5	INFORMATIKA
500	Vodja informatike
501	Sistemski analitik

Tabela 8.2: Signirni načrt

jih po zajemu in pretvorbi usmerimo v pravi proces in k pravemu naslovniku. Pomembno je, da je dokument posredovan na pravo področje, k ustreznemu naslovniku. Kot pripomoček za to se v javni upravi, pa tudi v nekaterih podjetjih uporablja signirni načrt. Signirni načrt je seznam vseh delovnih mest v podjetju in signiranje pomeni dodeljevanje zadev v reševanje. Primer dela signirnega načrta prikazuje preglednica 8.2:

Vsako delovno mesto je označeno z enolično številčno oznako, ki se imenuje signirni znak in z nazivom delovnega mesta.

8.6 Varna elektronska hramba gradiva

Dokumente v elektronski obliki hranimo v informacijskem sistemu za hrambo gradiva. To je informacijski sistem za skladiščenje in iskanje dokumentarnega gradiva, ki nadzoruje posebne funkcije nastajanje, hrambe in dostopa do gradiva zato, da ohranja njegovo uporabnost, celovitost in dostopnost.

Dokumente v elektronski obliki je mogoče hraniti na različnih nosilcih, vendar pa vsi nosilci niso primerni za dolgoročno hrambo gradiva. Dolgoročna hramba gradiva je hramba gradiva, daljša od petih letih. Primerni nosilci za dolgoročno hrambo dokumentov v elektronski obliki so na primer diskovna polja in magnetno-optični diski, neprimerni nosilci pa so CD-ji in DVD-ji. Tudi vse oblike zapisov niso primerne za dolgoročno hrambo. Primerne oblike so npr. tiff za grafične dokumente in pdf/a za tekstovne in mešane dokumente, za neprimerno obliko pa šteje jpg oblika zapisa. Primerni nosilci in oblike zapisa so opredeljeni v Enotnih tehnoloških zahtevah, ki predstavljajo del zakonodajnih podlag za varno elektronsko hrambo gradiva.

Pri arhiviranju dokumentov v elektronski obliki obstajajo različni poslovni modeli, v katerih sta različno zastopani vlogi tistega, ki je lastnik dokumentov (naročnik) in tistega, ki ima znanje in tehnologijo za e-arhiviranje dokumentov (izvajalec). Poslovni modeli so naslednji:

1. lastno izvajanje

2. delno zunanje izvajanje (delni outsourcing) arhivske funkcije

3. popolno zunanje izvajanje (popolni outsourcing) arhivske funkcije.

Slika 8.2: Poslovni model *Lastno izvajanje* storitev EDMS (lasten vir)

8.7 Poslovni modeli zajema, pretvorbe in elektronskega arhiviranja dokumentov

Poznamo tri modele storitve zajema, pretvorbe in elektronskega arhiviranja dokumentov:

1. lastno izvajanje,
2. delno zunanje izvajanje in
3. popolno zunanje izvajanje arhivske funkcije

Pri modelu lastnega izvajanja, lastnik dokumentov sam skrbi za zajem in pretvorbo ter elektronsko arhiviranje dokumentov, kot to prikazuje slika 8.2.

Pri modelu *Delno zunanje izvajanje* lastnik dokumentov sam skrbi za zajem in pretvorbo dokumentov, hrambo dokumentov v elektronski obliki pa zanj izvaja izvajalec.

Slika 8.3 prikazuje poslovni model delnega zunanjega izvajanja storitev EDMS. Pri tem modelu lastnik dokumentov sam skrbi za zajem in

Slika 8.3: Poslovni model *Delno zunanje izvajanje* storitev EDMS (lasten vir)

pretvorbo dokumentov, hrambo dokumentov v elektronski obliki pa zanj izvaja izvajalec.

Slika 8.4 prikazuje poslovni model popolnega zunanjega izvajanja EDMS. Pri tem modelu lastnik dokumentov izvajalcu preda dokumente v papirni obliki, izvajalec pa poskrbi za zajem in pretvorbo ter tudi hrambo dokumentov v elektronski obliki.

8.8 Različne vrste obdelav dokumentov

Dokumente je mogoče obdelati na različne načine. Izbiro načina obdelave narekuje predvsem vsebina dokumentov in zahteva po dostopu do arhiviranih dokumentov. Osnovne vrste obdelav so naslednje:

1. dosjejska obdelava (dosje sestavljajo dokumenti, ki pripadajo istemu poslovnemu dogodku, čeprav nastajajo v različnih obdobjih; cilj je sočasen dostop do vseh dokumentov v dosjeju))

2. paketna obdelava (dokumenti, ki sestavljajo paket, niso vsebinsko

Slika 8.4: Poslovni model *Popolno zunanje izvajanje* storitev EDMS (lasten vir)

povezani, druži pa jih neka skupna značilnost, npr. datum, po kateri jih kasneje v arhivu iščemo)

3. posamična obdelava (vsak dokument je opremljen s toliko podatki, da ga je pri poizvedbah mogoče natančno poiskati)

Če želimo, da bi bil dostop do iskanega dokumenta hiter in učinkovit in želimo, da je rezultat poizvedbe v arhivu točno tisti dokument, ki ga iščemo, se odločimo za posamično obdelavo. Tak način je na mestu v primerih, ko je pogostost iskanj dokumentov velika, zato je uporaben le natančen rezultat poizvedbe. Paketna obdelava pa je v nasprotju s tem primerna takrat, ko je vpogledov v določeno vrsto dokumentov malo, zato je za iskanje upravičeno porabiti malo več časa. Rezultat iskanja je namreč paket dokumentov, v katerem poiščemo želeni dokument. Paketna obdelava dokumentov je enostavnejša in zato cenejša.

8.9 Projekt izdelave notranjih pravil

Izdelava notranjih pravil ni enostavna naloga, ki bi jo naložili enemu zaposlenemu v podjetju ali dvema pričakovali, da bo opravljena v mesecu dni. Vsebina notranjih pravil namreč zadeva različna področja poslovanja v družbi, od organizacije, kadrov, razvoja informacijskih sistemov, njihove varnosti in administracije, pisarniškega poslovanja, revizije in seveda ravnanja z dokumentarnim in arhivskim gradivom. Notranja pravila vsebujejo opise postopkov izvajanja spremljevalnih storitev, torej zajema in pretvorbe gradiva v elektronsko obliko in hrambe gradiva v elektronski obliki. V teh postopkih s svojimi vlogami nastopajo različni udeleženci z različnih področij dela. Z namenom, da bi bilo mogoče postopke dela, ki zadevajo ravnanje z dokumentarnim gradivom in s tem notranja pravila dobro definirati in vanje zajeti vse potrebne korake ter vključiti vse potrebne udeležence, zahteva izdelava notranjih pravil sodelovanje strokovnjakov z različnih področij dela v družbi. To pomeni, da je izdelava notranjih pravil projekt, z jasno določenimi aktivnostmi, roki in sodelavci s konkretnimi zadolžitvami, ki lahko s svojim znanjem pripomorejo k uspešni izvedbi projekta.

Notranja pravila omogočajo ponovljivost postopkov. Namen definiranja pravil igre pri izvajanju spremljevalnih storitev in storitev hrambe gradiva je ravno v tem, da storitve izvajamo vedno na enak način in enako kakovostno. Zato moramo postopke zastaviti tako, da jih bo mogoče čim bolj učinkovito izvajati.

8.10 Pristop pri izdelavi notranjih pravil

Projekt izdelave notranjih pravil izvedemo v dveh fazah: v prvi opravimo pregled stanja in izdelamo načrt za pripravo notranjih pravil, v drugi pa pripravimo vsebino notranjih pravil samih.

Prvo fazo projekta izdelave notranjih pravil imenujemo priprava na zajem in hrambo gradiva. Za faza vključuje naslednje:

1. predhodno raziskavo, kjer spoznamo poslanstvo družbe, njeno organiziranost, ključne poslovne procese ter opredelimo poslovne in pravne zahteve za hrambo gradiva v elektronski obliki

2. analizo poslovnih aktivnosti, ki jo izvedemo tako, da popišemo dokumentarno gradivo v družbi in vrste gradiva, ki se hranijo v elektronski obliki ter s tem pridobimo vsebinski pogled v obstoječe dokumentarno gradivo družbe

3. študijo upravičenosti in študijo izvedljivosti elektronske hrambe

4. klasifikacijski načrt in pravilnik o arhiviranju

5. GAP analizo, ki da odgovore na vprašanja, katere sestavine notranjih pravil so v družbi že ustrezno opredeljene in dokumentirane in katere je potrebno še doreči in zapisati

6. oceno informacijskih sistemov v družbi, ki so kakor koli vezani na zajem, pretvorbo gradiva in hrambo gradiva v elektronski obliki

7. akcijski za izdelavo notranjih pravil.

Sledi naslednji korak, druga faza projekta, to je izdelava notranjih pravil.

Učinkovita izdelava notranjih pravil lahko temelji le na dobro izvedeni pripravi na zajem in hrambo gradiva v digitalni obliki. V 1. fazi projekta naredimo natančno inventuro stanja stvari na področju zajema, pretvorbe in hrambe gradiva v elektronski obliki in pridobimo vse informacije, potrebne za izdelavo notranjih pravil. V drugi fazi projekta izdelamo notranja pravila. To pomeni, da opredelimo postopke izvajanja spremljevalnih

storitev, opredelimo postopke izvajanja storitev elektronske hrambe, pripravimo manjkajoča navodila, pravilnike, politike in postopke.

Obseg notranjih pravil je odvisen od več dejavnikov. Ti so predvsem:

1. število različnih vrst gradiv, na katere se nanaša vsebina notranjih pravil (ni namreč potrebno, da notranja pravila govorijo o vsem gradivu, ki v družbi nastaja; govorijo lahko le o eni vrsti gradiva ali o nekaj vrstah gradiv, o tistih gradivih, ki se hranijo v elektronski obliki in za katere želimo papirne izvirnike uničiti, dokumentom pa zagotoviti pravno veljavo)

2. število načinov izvajanja zajema in pretvorbe gradiva in število sistemov za elektronsko hrambo gradiva (če se v družbi zajem in pretvorba gradiva v elektronsko obliko izvaja na enoten način in je vso gradivo v elektronski obliki hranjeno na enem sistemu za elektronsko hrambo, je obseg notranjih pravil manjši kot v primeru, ko se izvaja več različnih postopkov zajema in pretvorbe različnih vrst gradiv ali pa je gradivo v elektronski obliki hranjeno na različnih sistemih)

3. poslovni model: ali ima družba pogodbenega partnerja, registriranega ponudnika spremljevalnih storitev in storitev hrambe s potrjenimi notranjimi pravili, ki za družbo izvaja zajem, pretvorbo, hrambo gradiva ali družba vse te postopke izvaja sama in sama hrani gradivo v elektronski obliki (več dela družba sama, večji je obseg njenih notranjih pravil).

8.11 Primer elektronskega arhiviranja dokumentacije ob vpisu študenta

Za primer poslovanja z dokumenti nam bo služil postopek vpisa študenta v dokumentni sistem, ki ga izvajamo na Fakulteti. Za razumevanje postopka

je potrebno poznati osnovne pojme pisarniškega poslovanja, ki jih definira Zakon o splošnem upravnem postopku (ZUP).

Pri poslovanju Fakulteta ni, razen v redkih primerih, zavezana voditi upravnega postopka po zakonu, vendar velja, da se pravila upravnega postopka smiselno uporabljajo v vseh javnopravnih zadevah, četudi ne gre za upravno zadevo, kadar organizacije oziroma javnopravni subjekti državljanom odrejajo določeno ravnanje ali urejajo njihove pravice in koristi (javna podjetja, zavodi, združenja, zbornice, policija, ustanove, agencije, univerze, posebne varnostne službe), če s svojimi predpisi nimajo urejenega posebnega postopka. Gre za zagotavljanje procesnega varstva in procesnega reda. [35]

V Sloveniji mnogo javnih ustanov (predvsem pa vse upravne enote) uporabljajo za podporo svojim upravnim postopkom aplikacijo SPIS. Aplikacija deluje tako, da omogoča poslovanje skladno z ZUP in hkrati omogoča elektronsko hrambo dokumentov v skladu z ostalo zakonodajo, ki predpisuje način dela z elektronskimi dokumenti. Namenjena je učinkovitejši računalniški podpori pisarniškega poslovanja, zadeve in dokumenti se evidentirajo elektronsko, evidence se nahajajo na enem mestu in s tem so zadeve in dokumenti shranjeni organizirano, evidentiranje je enostavno, evidence so urejene in pregledne, dokumenti so dostopni v skladu s pristojnostmi uporabnikov. S tem je omogočena standardizacija in delna avtomatizacija delovnih postopkov.

Najprej si poglejmo definicije tistih najosnovnejših terminov, ki se uporabljajo pri pisarniškem poslovanju, pa še niso bili definirani v zgornjem tekstu:

Zadeva je celota vseh dokumentov in prilog, ki se nanašajo na isto vsebinsko vprašanje ali nalogo (srajčka, ovoj v katerem se nahajajo vsi dokumenti in priloge v zvezi z reševanjem vsebinskega vprašanja).

Vhodni dokumenti so vsi tisti dokumenti, ki jih organ javne uprave prejme (recimo prispela pošta ali dokumenti oddano osebno ali ...).

Tekoča zbirka dokumentarnega gradiva je zbirka, v kateri se hranijo zadeve najmanj dve leti po dokončni rešitvi.

Stalna zbirka dokumentarnega gradiva je zbirka dokončno rešenih zadev in zaključenih evidenc ali delov evidenc, ki jih organ mora hraniti skladno s predpisi več kot dve leti.

Zakonodaja zahteva, da morata biti tekoča in stalna zbirka realizirani tako, da gre za ločeni zbirki. S tem zagotavljamo, da so tudi dostopi do teh zbirk ločeni.

Oddaja prošnje

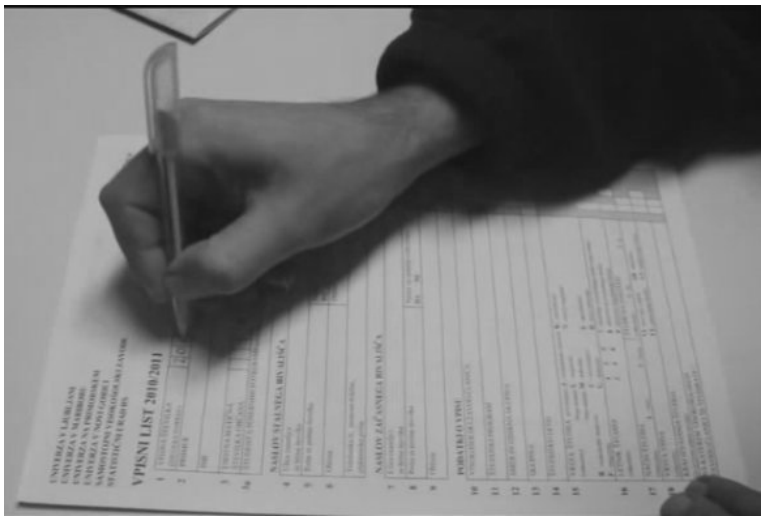
Celoten postopek se začne s študentovo oddajo vpisnega formularja in ostalih listin, ki so potrebne ob vpisu, kar prikazuje slika 8.5 in večpredstavna vsebina pod sliko.

Po študentovi oddaji vseh potrebnih listin, uradna oseba za vsakega posameznega študenta najprej kreira zadevo, kar prikazuje slika 8.6.

V računalniški obrazec, prek katerega kreiramo zadevo vpišemo v posamezna polja naslednje vrednosti:

1. V polje *Opis zadeve* vpišemo `Vpis 2010/2011`.

2. V polje *Klasifikacijski znak* vpišemo šifro klasifikacijskega znaka `6032 Vpis`. Vpis opravimo s pomočjo vnaprej pripravljenega seznama vseh možnih klasifikacijskih znakov našega klasifikacijskega načrta. Glej sliko 8.7. Ob vpisu klasifikacijskega znaka se samodejno napolni polje *Rok hrambe* z vrednostjo `T`, ki določa, da je gradivo trajno. Klasifikacijski načrt vsebuje tudi informacijo o trajanju hrambe, kar je bilo opisano že zgoraj.



Večpredstavna vsebina

Slika 8.5: Oddja vpisnega formularja (lasten vir)

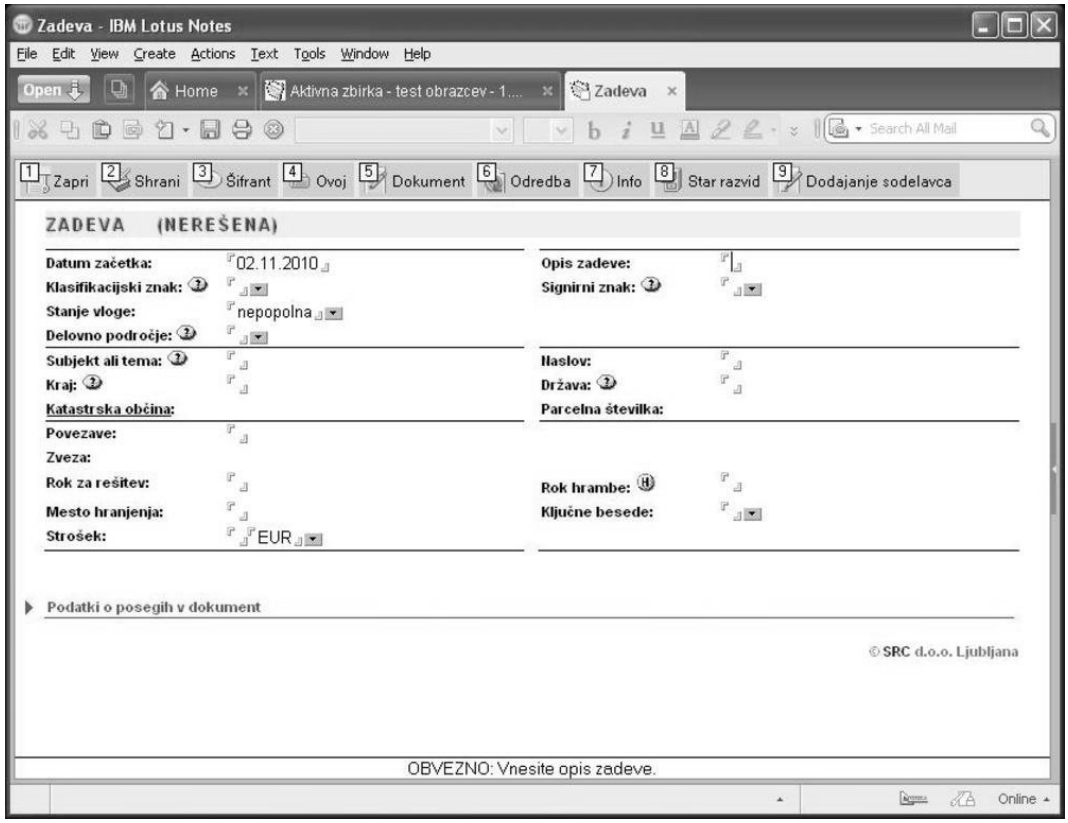
3. Za polje *Signirni znak* izberemo, iz vnaprej pripravljenega seznama vseh možnih signirnih znakov našega signirnega načrta, šifro *114 - (Referat za študentske zadeve)*. Glej sliko 8.8.

4. Izpolnimo ostala potrebna polja.

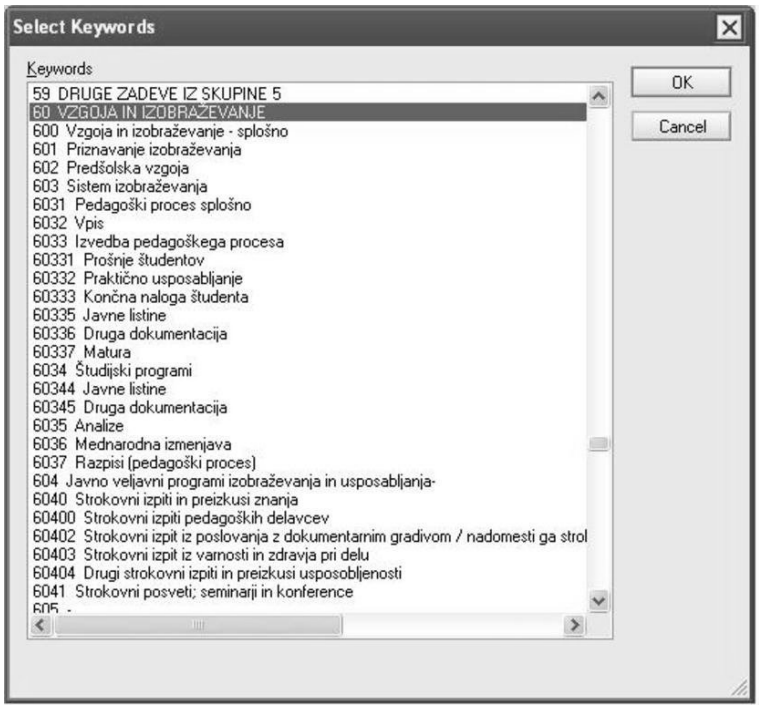
Slika 8.9) prikazuje stanje računalniškega obrazca po vpisu vseh polj, ki so v danem primeru potrebna.

Ko smo zadevo shranili smo v bistvu napravili srajčko ali ovoj, v katero vlagamo dokumente, ki so vezani na vpis posameznega študenta v posameznem šolskem letu. Ob shranitvi zadeva dobi tudi svojo zaporedno številko.

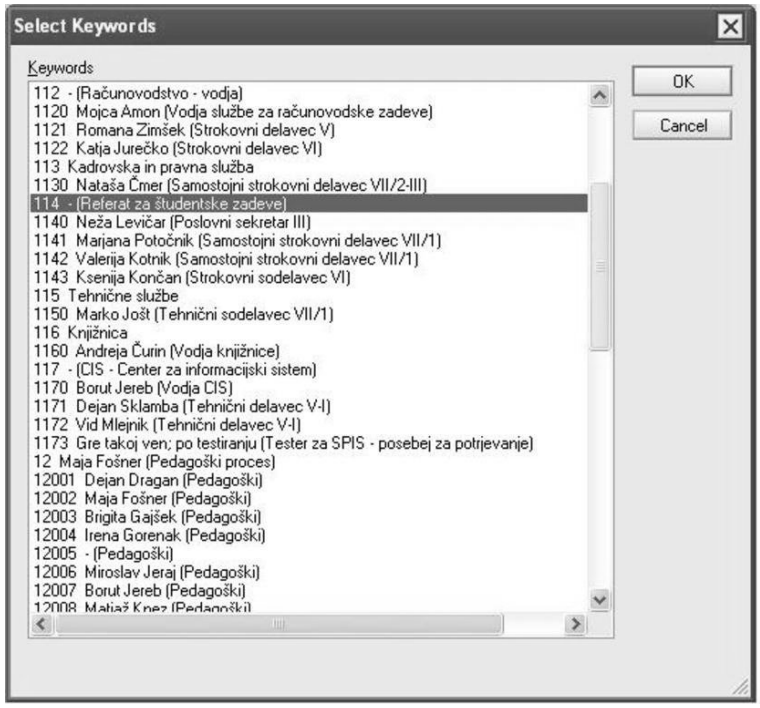
Sledi korak v katerem dodamo (ali "vložimo") v zadevo en vhodni dokument (gre za e-dokument). Več papirnih dokumentov lahko smiselno združimo v en e-dokument. Večina študentov bo imela v tej zadevi samo



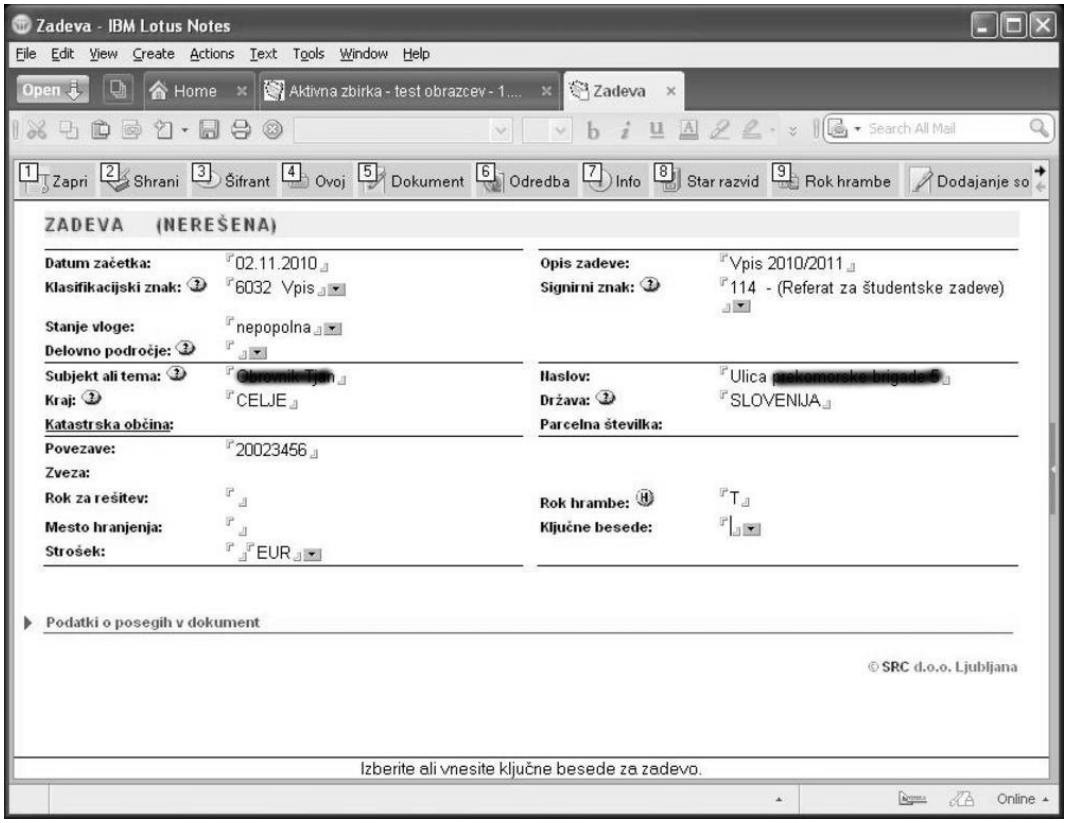
Slika 8.6: Kreiranje zadeve (lasten vir)



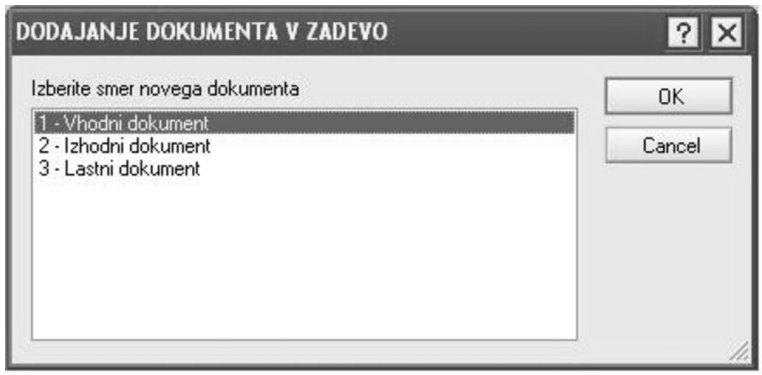
Slika 8.7: Izbira klasifikacijskega znaka (lasten vir)



Slika 8.8: Izbira signirnega znaka (lasten vir)



Slika 8.9: Izpolnjen obrazec *Zadeva* (lasten vir)



Slika 8.10: Prvi korak kreiranja vhodnega dokumenta v obstoječi zadevi (lasten vir)

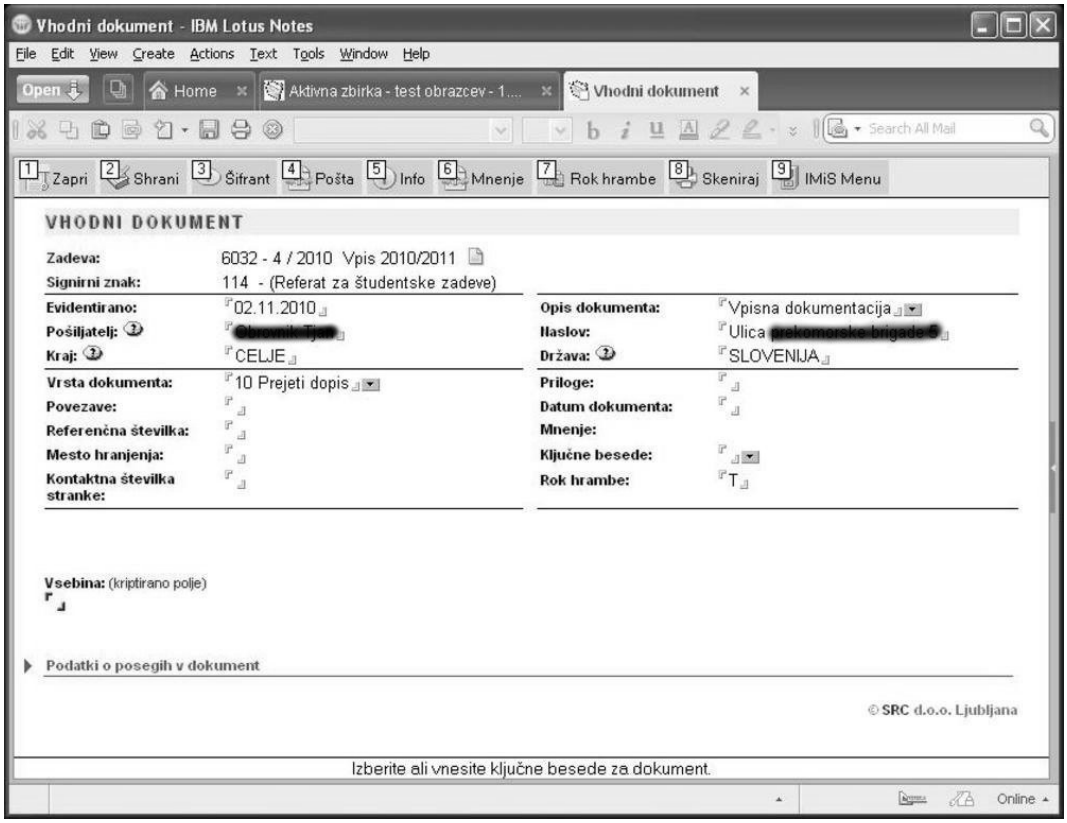
en e-dokument. Nekateri pa se bodo oglasili v Referatu večkrat in oddali več dokumentov, ki smiselno sodijo v zadevo `6032 Vpis` tekočega leta in tako bo kreiranih več e-dokumentov.

Ob fazi kreiranja vhodnega dokumenta se vse informacije, ki jih je bilo mogoče prenesti iz zadeve, samodejno prenesejo tudi na dokument. Postopek prikazujeta sliki 8.10 in 8.11. Prav tako se tak dokument tudi oštevilči skladno z predpisanim algoritmom, ki zahteva, da se v številki dokumenta skriva tudi številka zadeve, iz katere dokument izhaja.

V računalniški obrazec, prek katerega kreiramo vhodni dokument vpišemo v polje *Vrsta dokumenta* izberemo šifro vrste dokumenta, ki je v našem primeru `10 Prejeti dopis`. Šifre izberemo iz šifranta, ki ga prikazuje slika 8.12.

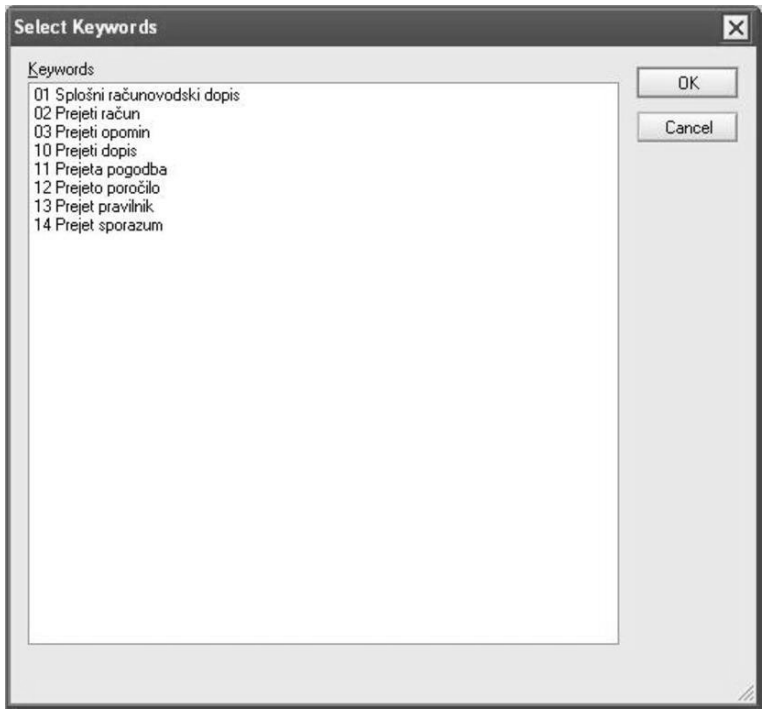
Sledi postopek upodabljanja prejetih papirnih dokumentov. Slike upodobitve so vezane na vhodni dokument. Postopek uporabljanja prikazuje slika 8.13 in večpredstavna vsebina, ki je dostopna prek spletnega naslova pod sliko.

Kasnej, ko bo potrebno poiskati vpisno dokumentacijo za nekega štu-

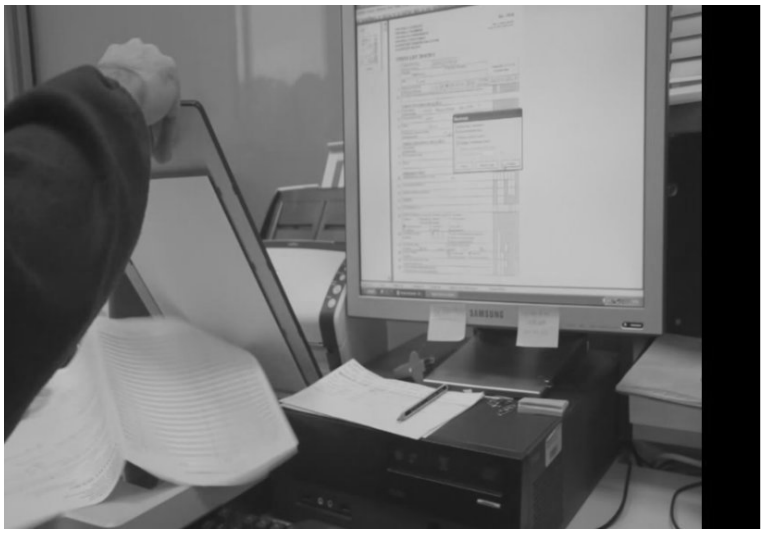


Večpredstavna vsebina

Slika 8.11: Drugi korak kreiranja vhodnega dokumenta v obstoječi zadevi (lasten vir)



Slika 8.12: Izbira vrste dokumenta (lasten vir)



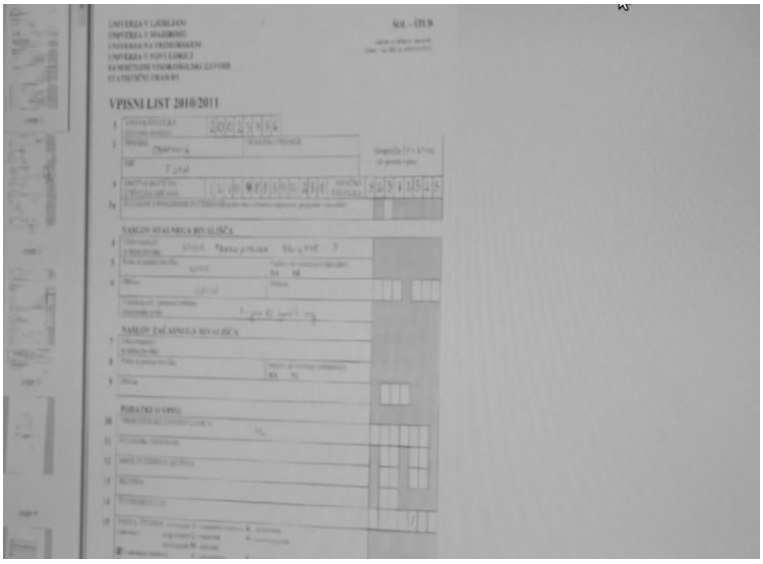
Večpredstavna vsebina

Slika 8.13: Upodabljanje papirnih dokumentov (lasten vir)

denta v nekem šolskem letu, jo bomo poiskali prek elektronskega sistema in ne več v predalih in omarah. Tovrstni način iskanja je neprimerno hitrejši in enostavnejši. Poleg tega praktično izničimo možnost, da se je nek del dokumentacije založil, uničil, odtujil ali izgubil. Sistem omogoča beleženja vseh spreminjanj in vpogledov v dokumentacijo.

8.12 Zaključna misel o dokumentnih sistemih

Vzpostavitev zakonsko skladnega zajema, pretvorbe in hrambe dokumentov je obsežen projekt, ki se ga je potrebno lotiti z vso resnostjo. Bistven sestavni del tega so notranja pravila, to so pravila, ki jih kot svoj interni akt sprejme podjetje glede hrambe svojega gradiva. Pred pričetkom izdelave notranjih pravil je potrebno sprejeti odločitev o vrstah gradiv, ki so predmet notranjih pravil in o poslovnem modelu pri izvajanju zajema, pre-



Večpredstavna vsebina

Slika 8.14: Iskanje in pregled dokumentacije (lasten vir)

tvorbe in elektronske hrambe gradiva. Pri odločanju o poslovnem modelu je smiselno vsekakor pretehtati vse možnosti, pa ne zaradi obsega notranjih pravil, temveč predvsem zaradi ravni kakovosti izvajanja storitev zajema, pretvorbe in elektronske hrambe gradiva.

Poglavje 9

Vodenje projektov

Poglavje v prvem delu podajajo osnovne definicije, na katere naletimo pri upravljanju projektov in področje umestijo v širši kontekst. Drugi del opisuje devet osnovnih področij znanj, ki jih pri upravljanju potrebujemo pri vodenju projekta. Na koncu so opisani še štirje „zakoni“ vodenja, ki naj bi jih upošteval vsaj uspešen vodja.

9.1 Osnove in splošen pregled področja

Kaj je projekt?

Projekt je začasna dejavnost, s katero ustvarjamo enkratne izdelke ali storitve. Za razliko od rednega, ponavljajočega dela, ima projektno delo značaj začasnosti in enkratnosti.

Kaj je vodenje projekta?

Vodenje ali upravljanja projekta je uporaba znanj, veščin, orodij in tehnik pri izvajanju projektnih aktivnosti z namenom, da dosežemo cilje projekta.

Slika 9.1: Potrebna področja znanj za vodenje projektov (lasten vir)

Relacije z ostalimi disciplinami

Devet različnih znanj potrebnih za vodje projektov vsebujejo tudi:

1. splošno sprejeta znanja in prakse s področja vodenja in
2. potrebna (največkrat tehnična) znanja in prakse iz področij, ki so predmet projekta.

Slika 9.1 prikazuje prepletenost potrebnih znanj uspešnega upravljavca ali vodje projektov.

Projekt kot del celote

Na izvajanje projekta vplivajo:

1. Strateški plani

2. Programi
3. Ostali projekti in
4. Podprojekti

Ključni vplivi na vodenje projektov

1. Faze projekta in življenjski cikel projekta
2. Udeleženci projekta (vodja projekta, naročnik, član projektnega tima, sponzor, izvajalec; zunanji, notranji; lastnik, investitor; prodajalec, pogodbenik; posameznik, podjetje, vlada; začasen ali stalen lobist; etc). Zaznati je potrebno vse udeležence in vse možne konflikte med njimi, ki so plod različnih ciljev in pričakovanj.
3. Vplivi organizacije in njene kulture (funkcionalna/linijska, matrična, projektna organizacija, etc)
4. Ključne vodstvene/upravljavske veščine (finančne, strateško planiranje, organizacijske, nadzor, delegiranje, delo pod pritiskom, timsko delo, voditeljske, etc)
5. Vplivi socialnega in ekonomskega okolja

9.2 Devet področij potrebnih znanj za vodje projektov

Upravljanje integracije

V času izvajanja projekta je potrebno pravilno koordinirati vsa potreba opravila tako, da dosežemo zastavljene cilje projekta in tako, da vse različne elemente projekta pravilno koordiniramo.

Sem spada tudi:

1. Razvoj projektnega plana 2. Izvajanje projektnega plana 3. Kontrolirano in integrirano izvajanje sprememb (glede na plan).

Upravljanje obsega

Opravljena morajo biti vsa potrebna opravila, ki jih je potrebno izvesti za uspešno dokončanje projekta in s tem dosego ciljev projekta tako, da pri tem ne izvajamo opravil, ki za dosego ciljev projekta niso potrebna.

Sem spada tudi:

1. Projektna pobuda - inicializacija
2. Planiranje obsega
3. Definiranje obsega (dobro definiraj mejo, ki določa kaj je in kaj ni predmet projekta)
4. Verifikacija obsega
5. Kontrola sprememb obsega

Upravljanje časa

Zagotavlja, da bomo končali projekt v predvidenem času.

Sem spada tudi:

1. Definicija vseh aktivnosti (WBS - Work Breakdown Structure)
2. Definicija časovne odvisnosti med aktivnosti in določanje časovne zaporednosti za vsako aktivnost posebej
3. Ocenjevanje časa trajanja za vse aktivnosti
4. Izdelava porazdelitve
5. Kontrola sprememb porazdelitve

Upravljanje stroškov

Projekt mora biti končan s predvidenim finančnim obsegom.

Sem spada tudi:

1. Planiranje potrebnih nefinančnih virov za izvedbo projekta
2. Predvidevanje in ocenjevanje stroškov za vse potrebne nefinančne vire
3. Zagotavljanje finančnih virov
4. Finančna kontrola

Upravljanje kvalitete

V okviru projekta je potrebno zagotoviti postavljene zahteve.

Sem spada tudi:

1. Planiranje kvalitete
2. Zagotavljanje kvalitete
3. Kontrola kvalitete

Upravljanje ljudi

Sodelavci na projektu morajo biti izbrani in razporejeni na takšna dela in naloge in biti morajo vodeni tako, da lahko največ prispevajo k uspešnemu zaključku projekta.

Sem spada tudi:

1. Planiranje organizacije
2. Pridobivanje sodelavcev
3. Razvoj tima

Vodenje komuniciranja

V času projekta je potrebno zagotavljati:

- pravočasno in
- ustrezno:
  - ustvarjanje,
  - zbiranje,
  - razširjanje,
  - arhiviranje in
  - urejanje

informacij (dokumentacije)

Sem spada tudi:

1. Planiranje komuniciranja (med udeleženci projekta)
2. Distribucija informacij (med udeležence projekta)
3. Poročanje o stanju (udeležencem projekta)
4. Kreiranje administrativnih zabeležk

Upravljanje s tveganji

Zahteva identificiranje, analizo in izvajanje ustreznih reakcij na tveganje.

Sem spada tudi:

1. Planiranje upravljanja s tveganji
2. Identifikacija tveganj
3. Kvalitativna analiza tveganj

4. Kvantitativna analiza tveganj
5. Planiranje odzivov na tveganja
6. Opazovanje in kontrola tveganj

Upravljanje nabav

Ob izvajanju projektov je potrebno izvajati proces nabave izdelkov in/ali storitev zunaj ali v podjetju.

Sem spada tudi:

1. Planiranje nabav
2. Planiranje iskanja potrebnih dobrin ali planiranje izdelave razpisov
3. Izvedba iskanja ali razpisovanja
4. Izbira dobaviteljev
5. Administracija s pogodbami
6. Zaključevanje nabav

9.3 Splošno o vodenju

9.3.1 Štirje temeljni zakoni vodenja

1. Zahtevajmo od sebe več kot kdorkoli drug! Sodelavci hočejo biti ponosni na svojega šefa. Sem jim lahko za vzgled?
2. Zahtevajmo od sodelavcev več kot kdorkoli drug! Sodelavci so potencialni svetovni prvaki! Jih žalimo s tem, ko od njih premalo zahtevamo?
3. Spoznajmo svoje sodelavce bolje kot kdorkoli drug! Sodelavci pričakujejo, da pokažemo interes zanje. Sem pripravljen to storiti?

4. Obvarujmo sodelavce pred občutki strahu! Sodelavci potrebujejo varnost, da dosežejo najboljše rezultate! Jim nudim varnost?

Literatura

[1] BusinessDictionary.com. Risk. `http://www.businessdictionary.com/definition/risk.html`, nov 2014. [Online; accessed 21. november 2014].

[2] Adam Greene. A process approach to project risk management. *Department of Civil and Building Engineering, Loughborough University*, 2009. [Online; accessed 21. november 2014].

[3] InvestorWords.com. Risk. `http://www.investorwords.com/4292/risk.html`, nov 2014. [Online; accessed 21. november 2014].

[4] *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0.* IT Governance Institute, 2008.

[5] ISO. *ISO/IEC TR 18044:2004; Information technology – Security techniques – Information security incident management.* ISO, 2004.

[6] ISO. *ISO 28000:2007; Specification for security management systems for the supply chain.* ISO, 2007.

[7] ISO. *ISO 31000:2009; Risk management – Principles and guidelines.* ISO, 2009.

[8] ISO. *ISO 31010:2009; Risk management – Risk assessment techniques.* ISO, 2009.

[9] ISO. *ISO Guide 73:2009; Risk management – Vocabulary.* ISO, 2009.

[10] ISO. *ISO/IEC 27005:2011; Information technology – Security techniques – Information security risk management.* ISO, 2011.

[11] ISO. *ISO 22301:2012; Societal security – Business continuity management systems – Requirements.* ISO, 2012.

[12] ISO. *ISO/IEC 27001:2013; Information technology – Security techniques – Information security management systems – Requirements.* ISO, 2013.

[13] ISO. *ISO/IEC 25000:2014; Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE.* ISO, 2014.

[14] ISO. *ISO/IEC/IEEE 12207:2017; Systems and software engineering – Software life cycle processes.* ISO, 2017.

[15] Borut Jereb. Zadolževanje informacijskih virov. pages 237–24. Ljubljana: Slovenski inštitut za revizijo, 2002. 10. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov.

[16] Borut Jereb. Upravljanje it investicij. pages 7–22. Ljubljana: Slovenski inštitut za revizijo, 2008. 16. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov.

[17] Borut Jereb. Upravljanje it investicij s pomočjo val it. Ljubljana: Slovensko društvo Informatika, 2008. Dnevi slovenske informatike 2008 - DSI, Portorož, Slovenija, 09.-11. april.

[18] Borut Jereb. *Upravljanje tveganj.* Univerza v Mariboru, Fakulteta za logistiko, 2014.

[19] Borut Jereb and Tina Cvahte. Risk catalog. `http://labinf.fl.uni-mb.si/risk-catalog`, 2012. [Online; accessed 25. november 2014].

[20] Borut Jereb, Tina Cvahte, and Bojan Rosi. Val it v logistiki = val it in logistics. *Economics & economy*, 1(2):91–109, 2013.

[21] Borut Jereb, Teodora Ivanuša, and Bojan Rosi. Systemic thinking and requisite holism in mastering logistics risks : the model for identifying risks in organisations and supply chain. *Amfiteatru economic*, 15(33):56–73, 2013.

[22] Borut Jereb and Mateja Škornik. Upravljanje informacijskih tveganj po iso/iec 27005:2008. pages 9–28. Ljubljana: Slovenski inštitut za revizijo, 2009. 17. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov.

[23] Johnathan Mun. *Modeling Risk: Applying Monte Carlo Simulation, Real Options Analysis, Forecasting, and Optimization Techniques*. Wiley - Finance, 2006.

[24] Roy O'Connor. Introduction to ISO/IEC software engineering standards. `https://slideplayer.com/slide/4687065/`. [Online; accessed 27. januar 2019].

[25] Steven J. Ross. Four little words. *ISACA Journal*, 1, 2009.

[26] Andrew Steward. On risk: Perception and direction. *Computers & Security*, 23:362–370, 2004.

[27] John Thorp. The val it story. *ISACA Journal*, 2006.

[28] Computer science. `http://en.wikipedia.org/wiki/Computer_Science`, okt 2010. [Online; accessed 15. oktober 2010].

[29] Information systems (discipline). http://en.wikipedia.org/wiki/Information_systems_(discipline), okt 2010. [Online; accessed 15. oktober 2010].

[30] Information technology. http://en.wikipedia.org/wiki/Information_technology, okt 2010. [Online; accessed 15. oktober 2010].

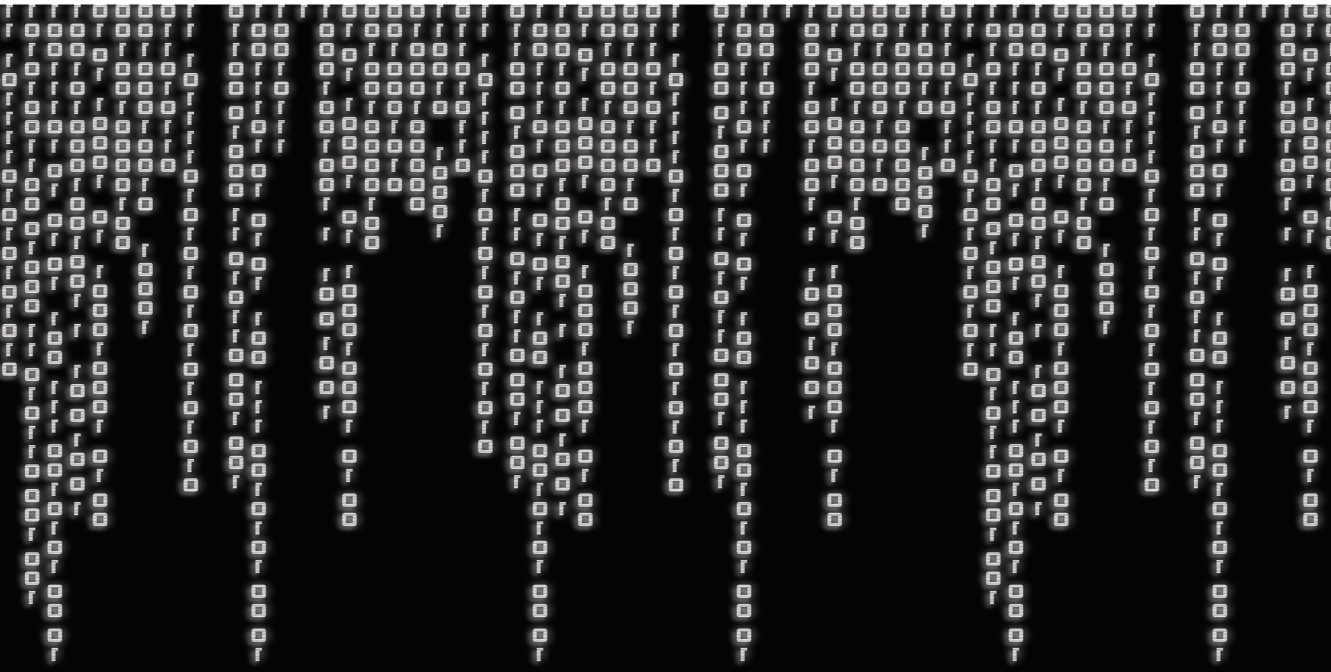
[31] EMŠO, davčna številka... http://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/emso-davcna-stevilka/#c199. [Online; accessed 15. oktober 2010].

[32] ISO and IEC release information security standard to help detect it intrusions. http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1267, July 11, 2006. [Online; accessed 15. oktober 2010].

[33] Logistika. http://sl.wikipedia.org/wiki/Logistika, okt 2010. [Online; accessed 15. oktober 2010].

[34] Risk. https://en.wikipedia.org/wiki/Risk, nov 2014. [Online; accessed 21. november 2014].

[35] Marijan Štriker. *Splošni upravni postopek, Priročnik za udeležence seminarja*. Ministrstvo za javno upravo RS. 2. izd., 3. natis., 2005.



Univerza v Mariboru

Fakulteta za logistiko