INFORMACIJSKI SISTEM U KONTEKSTU KORPORATIVNE SIGURNOSTI

INFORMATION SYSTEM IN THE CONTEXT OF CORPORATE SECURITY

Dr.sc. Zdenko Adelsberger

Rezime: *Već duže vremena prema informacijama se odnosi kao prema vrijednoj i važnoj imovini što je dovelo da su organizacije postale potpuno ovisne o informacijama i obradom informacija. Zbog toga se pitanju informacijskog sistema mora posvetiti posebna pažnja, jer razni događaji ili incidenti koji na neki način ugrožavaju informacijski sistem mogu izazvati ogromne štetne utjecaje na poslovne procese ili misije organizacije, u rasponu mjerila od nevažnih do katastrofalnih. Zato je nužnost sagledavanja informacijskog sistema u kontekstu korporativne sigurnosti od egzistencijalne važnosti za svaku korporaciju. U okviru rada daje se prikaz prelaza od zahtjeva korporativne sigurnosti na problem informacijske sigurnosti, međusobnu povezanost i utjecaj, te značaj međunarodnih standarda na tu problematiku u svjetlu praktičkih rješenja.*
Ključne reči: *informacijska sigurnost, korporativna sigurnost, ISMS, upravljanje rizicima*

Abstract: *For a long time the information is treated as a valuable and important asset, which led that organizations became totally dependent on information and information processing. Therefore, the issue of information systems requires special attention, because various events or incidents that somehow threaten the IT system can cause huge adverse effects on business processes or the mission of the organization, ranging in scale from insignificant to catastrophic. Therefore, the necessity of seeing the information system in the context of corporate security is of existential importance for any corporation. This paper gives an overview of the transition from the application of corporate security to the problem of information security, coherence and impact, and the importance of international standards on this issue in the light of practical solutions.*
Key words: *information security, corporate security, ISMS, risk management*

1. UVOD

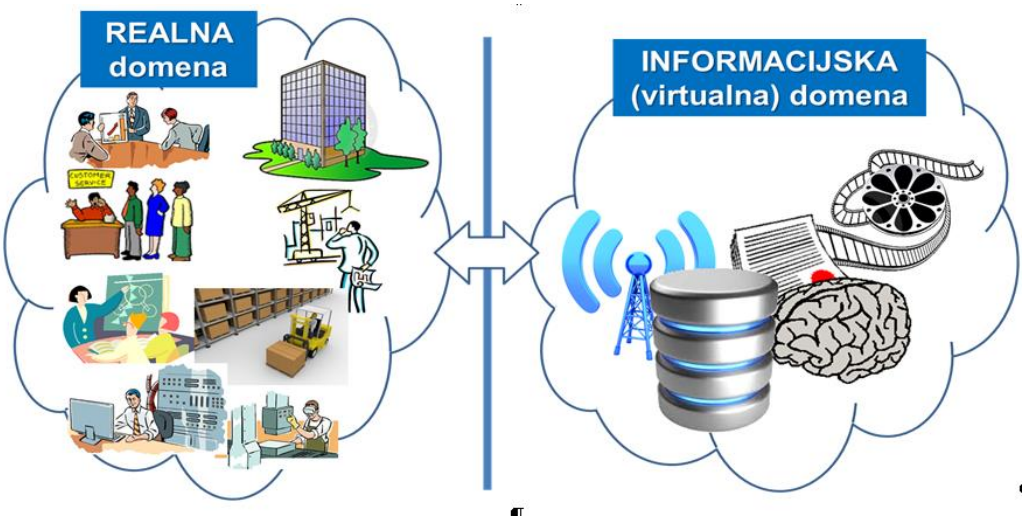
Govoriti o korporaciji se može na više načina i aspekata. Jedan os njih je svakako i sigurnost, kako u općem smislu, tako i u smislu pojedinih područja interesa. Sigurnost korporacije je u osnovi egzistencijalno pitanje. Naime, ako je nivo sigurnosti u korporaciji nizak, praktički po bilo kom osnovu, može se govoriti o velikoj ugroženosti ostvarenja misiji, vizije i ciljeva koji se želi postići. Kao posljedica pojavljuje se visoka vjerojatnost urušavanja korporacije ako se ne ostavruje misije, vizija, ali i niz planiranih ciljeva. Zato se na pitanje glavnog menadžera korporacije "Da li je sve u redu?" smatra u stvari pitanje "Da li se sve aktivnosti i događaji u korporaciji odvijaju po predviđenim planovima?". Ukoliko je odgovor potvrdan, tada se u slučaju provođenog nadzora smatra vrlo visoka vjerojatnost ostvarenja misije, vizije i ciljeva. Međutim, ako nije takva situacija i odgovor nije potvrdan, onda je vjerojatno već na djelu urušavanje ispunjenja misijie, vizije i ciljeva, što direktno ugrožava korporaciju, čak moguće i do nivoa egzistencije.

Govoriti o aspektima sigurnosti, kao što je već rečeno, može se na više načina. Npr. sigurnost resursa, sigurnost nabavke repro materijala, sigurnost okruženja (političkog, ekološkog, fizičkog, itd.), sigurnost tržišta zbog konkurencije ili nečeg drugog, itd. Jedan od najvažnijih resursa, ako ne i najvažniji, su informacije korporacije, ništa manje važne od ljudskih resursa, repro materijala, energije, itd. To znači, ugrožavanjem tako važnog resursa kao što su informacije u korporaciji direktno i to vrlo velikom brzinom prijeti kolaps korporacije. Kako su informacije unutar tzv., informacijskog sistema, onda se može lako pokazati da je informacijski sitem temeljni sigurnosni aspekt opstanka korporacije, bez obzira na njenu veličinu, djelatnost ili strukturu.

2. ODNOS REALNE I VIRTUALNE DOMENE KORPORACIJE

1) Dr.sc. Zdenko Adelsberger, Bluefield d.o.o., Zagreb, Hrvatska, e-mail: zdenko@bluefield.hr

Svaka korporacija ima dvije domene u kojima egzistira od svog osnutka, pa na dalje. Te dvije domene su realna i virtualna domena. Ilustracija te dvije domene je prikazana na slici 1.



Slika 1 - Odnos realne i virtualne egzistencijalne domene korporacije

U realnoj domeni se nalaze svi elementi korporacije u obliku fizičkih objekata: zdgrade, strojevi, ljudi, izvori energije, partneri, kompjuteri, itd. Međutim u virtualnoj domeni se nalazi „slika“, odnosno “kopija” korporacije iz realne domene, ali u obliku niza raznih informacija. Svaki objekt ili bilo kakva transakcija – promjena u realnoj domeni mora imati svog reprezenta u virtualnoj – informacijskoj domeni. Prema nacionalnim zakonima ili zahtjevima titulara – vlasnika korporacije, mora se uspostaviti direktna veza između realne domene i informacijske, odnosno da sve što se dogodi u realnoj domeni mora se na neki način dogoditi i u informacijskoj domeni. Na taj način se može govoriti o potpunoj “kopiji” korporacije u informacijskoj domeni, gdje je ta kopija dinamička, odnosno prati sve promjene u realnoj domeni. Uz to, za razliku od realne domene, jedino je u informacijskoj domeni i cijela povjest dinamike odvijanja promjena u realnoj domeni.

Nadzor i kontrola bilo koje korporacije se u biti provodi u dva nivoa. Prvi nivo je kontrola, odnosno provjera usklađenosti realne u informacijske domene. Tim postupkom se dobiva potvrda da je stanje u virtualnoj domeni jednako kao i u realnoj. U pravilu, taj nivo nadzora i kontrole provode interni i eksterni auditori i revizori. Drugi nivo je nadzor i kontrola informacijske domene u svrhu analize funkcioniranja korporacije. Taj nivo provode u pravilu uprava, vlasnici, državne institucije, banke, partneri, kao i druge zainteresirane strane, naravno svaka u obimu i po pitanjima relevantnim za njih.

Može se reći da fizičko uništenje ključnih resursa, odnosno objekata u realnoj domeni se može relativno lako nadoknaditi s novim u koliko postoje odgovarajuća financijska sredstva. Međutim, uništenje ključnih informacija u informacijskoj domeni ne može se nadoknaditi jednostavno niti brzo, a u pravilu može dovesti do potpunog uništenja korporacije, bez obzira što su u realnoj domeni svi resursi na raspolaganju i funkcionalni.

Iz toga se može zaključiti: korporacija nedvojbeno postoji u realnoj i informacijskoj domeni. Egzistencija korporacije zavisi kako od njenog funkcionalnog postojanja u realnoj domeni, tako i od funkcionalnog postojanja u informacijskoj domeni. Pored toga, oštećenja ili uništenje u realnoj domeni ne dovodi do uništenja korporacije u virualnoj domeni, ali oštećenja ili uništenje u virualnoj domeni može izazvati i uništenje resursa i cijele korporacije u realnoj domeni.

U konačnici, u cilju očuvanja korporacije za ispunjenje njene misije, vizije i ciljeva nužno je provesti očuvanje iste, kako u realnoj, tako i u informacijskoj domeni.

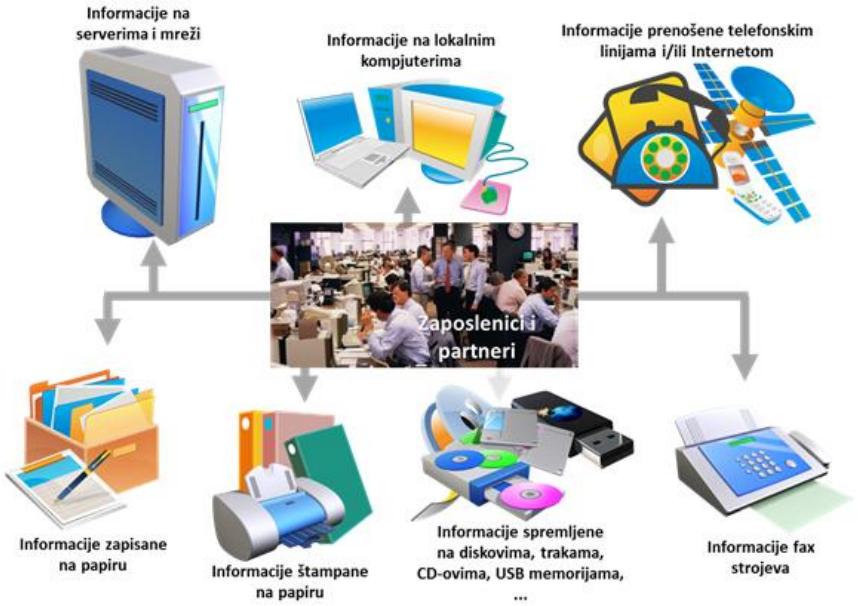
3. INFORMACIJA KAO OBJEKT INFORMACIJSKE DOMENE

Ključni objekt u informacijskoj domeni je informacija. Po definiciji u ovom kontekstu se pod informacijom smatra svaki podatak koji u nekom kontekstu ima vrijednost za korporaciju i predstavlja imovinu korporacije. U tom slučaju, informacija se mora kao i svaka druga imovina čuvati i sačuvati.
Prema vrstama, značajnim za korporaciju, informacije se mogu podijeliti na:

- **Vitalne informacije** - za ostvarenje poslovnih ciljeva
- **Osobni podaci** - definirani u smislu nacionalnih zakona o privatnosti
- **Strateške informacije** - potrebne za postizanje strateških ciljeva
- **Visoko vrijedne informacije** - čije prikupljanje, pohrana, obrada i prijenos zahtjeva dugo vremena i/ili uključene visoke troškove

Svaka od gore navedenih vrsta informacija imaju svoj vrijednosni razred za korporaciju i prema svakoj od njih se mora odnositi s odgovarajućom pažnjom, odnosno čuvati ih kao i drugu imovinu korporacije.

Sama informacija u osnovi je apstraktna i kao takva ne postoji u fizičkom obliku te je zbog toga u tom smislu teško uspoređivati s ostalom imovinom korporacije. Svaka informacija se mora nalaziti na nekom mediju da bi se mogla koristiti. Ti mediji na kojima se nalazi informacija su u funkciji nosioca informacije, a mogu biti raznih vrsta. Na slici 2 su prikazani neki od najčešćih oblika nosioca informacije unutar neke korporacije.



Slika 2 - Nosioci informacija u korporaciji

Kao što se može vidjeti na slici 2, postoji veliki broj nosioca informacija značajnih za korporaciju. Niz tih nosioca nisu pod kontrolom same korporacije što značajno može otežati osnovni zahtjev očuvanja informacije kao imovine. Svi objekti na kojima se u nekom obliku nalaze sve informacije korporacije naziva se informacijski sistem. Informacijski sistem (IS) se može definirati kao sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima. Ukoliko se promatra samo kompjuterska tehnologija (IT) kao tehnološka infrastruktura, onda se govori o IT sistemu, što je podskup od informacijskog sistema. Razlikovanje ta dva sistema i njihove granice razdvajanja je od posebne važnosti kod provođenja očuvanja informacija. Na slici 3 prikazana je ilustracija razlika informacijskog i IT sistema kako zorno izgleda u prirodi.

Slika 3 - Ilustracija informacijskog i IT sistema u okviru korporacije

Na slici 3 se može vidjeti da ilustracija A predstavlja situaciju u korporaciji u kojoj postoji informacijski sistem, ali i IT sistem, kao podskup od IS. Na ilustraciji B je situacija kada postoji informacijski sistema, ali ne postoji IT sistem. Istina, danas je teško zamisliti da ne postoji u korporaciji pored IS i IT sistem, kako zbog potrebe poslovanja, tako i kompatibilnosti i povezanosti s nizom zainteresiranih strana. Često se u korporacijama uz IT sistem uključuje i komunikacijska tehnologija, tako da se govori o ICT (Information and communications technology).

Resursi unutar kojih se nalaze informacije predstavljaju široki spektar raznih komponenti, a smatraju se resursima podrške u okviru informacijskog sistema. Mogu se podijeliti kako je prikazano u tablici 1.

Tablica 1. Vrste resursa podrške informacijskog sistema

Hardver kojeg čine svi fizički elementi podrške procesa, a uključuje	Aktivne uređaje za obradu podataka, prijenosne uređaje, fiksni uređaji, procesne periferije, pasivni mediji za podatke, elektronički mediji, ostali mediji
Softver koji se sastoji od svih vrsta programa s kojima se omogućava rad na obradi podataka	Operativni sistemi, softver za servise, održavanje ili administraciju, paketi softvera ili standardni softver, standardne poslovne aplikacije, specifične poslovne aplikacije
Mreže koje se sastoje od svih komunikacijskih sklopova korištenih za međuvezu nekoliko fizički udaljenih kompjutera ili elemenata informacijskog sistema	Mediji podrške, pasivne ili aktivne veze, komunikacijsko sučelje
Osoblje se sastoji od svih grupa ljudi uključenih u informacijski sistem	Donosioci odluka, korisnici, operativno osoblje i osoblje podrške, programeri
Mjesta su lokacije ili područja za smještaj fizičkih sredstava i njihove funkcije	Vanjsko okruženje, prostor, zone
Osnovne usluge Svi servisi potrebni za funkcioniranje organizacijskih uređaja	Komunikacije, komunalne usluge
Organizacijsko okruženje opisuje organizacijski okvir, a sastoji se od svih struktura osoblja dodijeljenih zadacima te procedura za kontrolu tih struktura	Uprava, struktura organizacije, projekt ili sistem organizacije podugovarači / dobavljači / proizvođači

Kada se pogledaju svojstva bilo koje imovine u korporaciji mogu se na temelju njih planirati postupci očuvanja iste. Tako i informacija ima svoja svojstva u upotrebnom smislu. Ta svojstva su:

- **Tajnost** – do informacije mogu doći samo ovlašteni korisnici
- **Cjelovitost** – informacija se ne može promijeniti bez znanja i odobrenja vlasnika, ali isto tako i postupci obrade informacije

- **Raspoloživost** – do informacije se može doći na mjestu gdje treba, u trenutku kada treba i u obliku kakav je potreban.

Obično se tajnost, cjelovitost i raspoloživost informacija označava sa C-I-A kao akronim od engleskih riječi **C**onfidentiality, **I**ntegrity, **A**vailability.

Pored ta tri svojstva informacije često se koriste i dodatna svojstva za informaciju kao:

- **Autentičnost** - svojstvo koje osigurava da je identitet subjekta zaista onaj za koji se tvrdi da jest.
- **Neporecivost** - svojstvo koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije (podatka).
- **Dokazivost** je svojstvo koje osigurava da aktivnosti subjekta mogu biti praćene jedinstveno do samog subjekta.
- **Pouzdanost** je svojstvo dosljednoga, očekivanog ponašanja i rezultata.

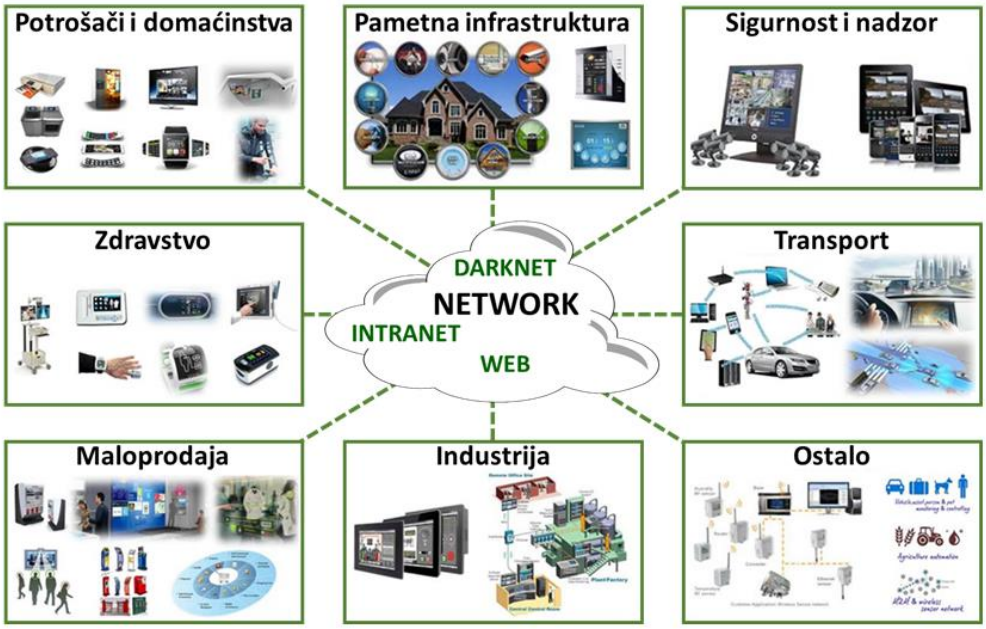
Ta dodatna svojsva su također izuzetno važna za informaciju, mada se može pokazati da proizilaze iz osnovna tri svojstva opisana s C-I-A.

Sigurnost informacije, a time i informacijske domene korporacije uvjetovana je očuvanjem svojstava informacije. Drugim rječima, narušavanje očuvanja svojstava informacije, narušava se i sigurnost informacijske domene, a time direktno i korporacije. Cjelokupni sistem očuvanja svojstava informacija unutar neke korporacije može se nazvati informacijski sigurnosni sistem ili sigurnosno rješenje za informacijski sistem. Na slici 4 je prikazana opća struktura sigurnosnog rješenja za informacijski sistem s pripadnim komponenetama.

Slika 4 - Struktura sigurnosnog rješenja za informacijski sistem

Na slici 4 se može vidjeti da sigurnosno rješenje ima dvije komponente: tehničku i organizacijsku. U međusobnom odnosu, praktična iskustva pokazuju da se u domeni tehnologije nalazi oko 20-tak %, a u domeni organizacijskog rješenja sigurnosti oko 80-tak %. To drugim rječima pokazuje da se sigurnosno rješenje za informacijski sistem ne može kupiti na tržištu. Jedan dio, tehnička rješenja (alarmi, zaštitni zidovi, kamere, softver, hardver, itd.) se može nabaviti na tržištu, ali organizacijska rješenja se moraju razviti i provesti u samoj korporaciji i u pravilu nisu prenosiva iz jedne korporacije u drugu, mada su principi svuda isti.

Problemi vezani s informacijama i informacijskim domenama korporacije se povećavaju iz dana u dan i teško je točno predvidjeti gdje će to završiti. Danas oko 76 posto izvršnih direktora u svijetu istražuje IoT (Internet of Things) i njegove mogućnosti, dok će 95 posto poslovanja do 2018 postati dio interneta stvari. Naime, kompanije se danas sve više odmiču od tradicionalnih modela poslovanja te se trude doći što bliže krajnjem korisniku. Ilustracija IoT-a prikazana je na slici 5.



Slika 5 - Ilustracija IoT-a (Internet of Things)

U tom kontekstu se može vidjeti da se u većem ili manjem obimu dio informacijskog sistema korporacije seli van nje u svijet mreža distribuiranih po čitavom svijetu, uključujući sve nivoe i oblike, kao npr. intranet, web, darknet, odnosno deep web. To upućuje da se za korporacije pojavljuje ozbiljan problem kontrole i nadzora vlastitih informacija kao imovine koja se nalazi na resursima koji pripadaju nekim drugim vlasnicima i nosiocima s potencijalno raznim interesima.

4. ODNOS PROCESA I INFORMACIJE

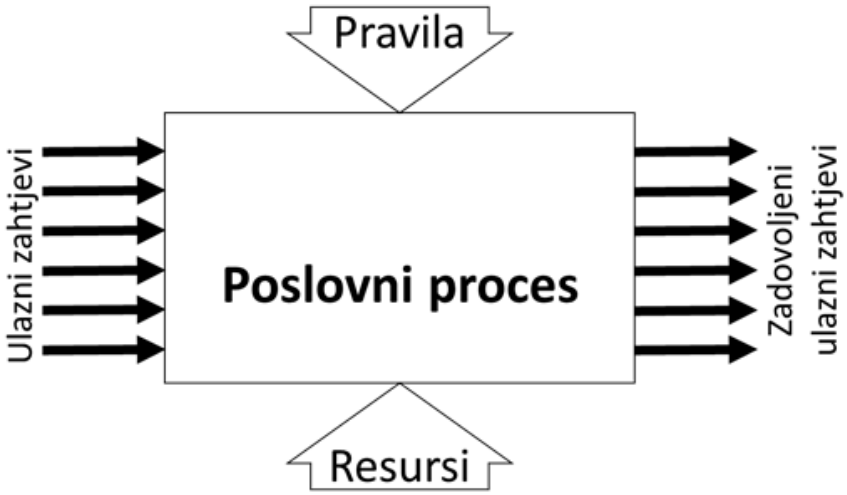
Prema ISO 9001 od revizije iz 2000 godine u svakoj korporaciji koja želi implementirati sistem upravljanja kvalitetom, ali i drugih sistema upravljanja na temelju ISO standarda, mora se provesti procesni pristup. To u praksi znači da se sve aktivnosti koje se provode u organizaciji trebaju promatrati kao dio nekog poslovnog procesa. U skladu s navodima ISO 9001 proces se može predstaviti kao što je prikazano na slici 6.

Kao što se može vidjeti na slici proces je predstavljen kao niz uređenih aktivnosti koje se obavljaju u skladu s nekim pravilima uz pomoć resursa. Osnovna funkcija svakog poslovnog procesa je pretvaranje ulaza u izlaz, odnosno zadovoljenjue ulaznih zahtjeva.

Prema ISO standardima se predlaže primjena PDCA kruga za upravljanje procesima. Svi elementi relevantni za upravljanje procesom prema PDCA krugu (planiranje, provedba, provjera i djelovanje) predstavljaju isključivo informacije. Može se lako pokazati da su ulazni zahtjevi, stupanj zadovoljenja ulaznih zahtjeva na izlazu, pravila i resursi u stvari informacije. To dovodi do zaključka: ako je proveden procesni pristup upravljanja korporacijom ili bilo kojom organizacijom, a upravljanje procesom se temelji na informacijama, onda se i upravljanje organizacijom zasniva isključivo na informacijama. Ništa novo. To bi trebalo biti već davno svakom jasno. Ali, u praksi se ne doživljava takav način razmišljanja kao sastavni dio pristupa sistema upravljanja, odnosno, većina mendžera nije toga ni svjesna. Zato, za takve slučajeve gdje se zanemaruje informacija kao ključna imovina (resurs) poklanja se glavna pažnja svim ostalim vrstama resursa, a informacije se i ne spominju u tom kontekstu. Zašto je tako? Zbog nepostojanja svijesti o važnosti i vrijednosti informacija, a o znanju da se ni ne govori.

U revizijama standarda koje predstavljaju specifikacije zahtjeva, nakon 2012 godine prema Aneksu SL, više se ne spominje dokumentacija, već dokumentirane informacije. Dijelom i zbog probijanja u svijest činjenice da je informacija kao resurs temelj upravljanja bilo kakvom organizacijom. Na taj način, su u pojam dokumentirane informacije uključeni svi oblici ranijih dokumenta, ali i zapisi i ostali oblici informacija relevantni kako za upravljanje tako i

za funkcioniranje procesa, odnosno bilo kakve organizacije.



Slika 6 - Blok shema procesa prema ISO 9001

5. OKVIR ZA SIGURNOSNO RJEŠENJE INFORMACIJSKOG SISTEMA

Da bi se očuvala svojstva informacije neke korporacije najpoznatiji okvir u svijetu, a time i najšire primijenjen, je temeljen na primjeni međunarodnog standarda ISO/IEC 27001, koji predstavlja specifikaciju zahtjeva za uspostavu, održavanje i poboljšanje sistema za upravljanjue informacijskom sigurnošću (ISMS - Information Security Management System). Trenutno važeća revizija je iz 2013 godine. Pored specifikacije zahtjeva u ISO/IEC 27001 za uspostavu ISMS-a u korporaciju, objavljen je i niz smjernica kojima se pomaže u rješavanju pojedinih zahtjeva u smislu primjene najbolje prakse. Takve smjenice su npr. ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC 27008, itd.)

ISO/IEC 27001 pruža model za uspostavljanje, implementaciju, upravljanje, nadzor, pregled, održavanje i usavršavanje ISMS-a u cilju zaštite informacija, odnosno cjelokupne informacijske imovine. Informacijska imovina obuhvaća informacije u bilo kojem obliku, pohranjene u bilo kojem obliku, a koristi se za bilo koju svrhu, od strane organizacije, ali i vanjskih korisnika.

Da bi se postigla sukladnost s ISO/IEC 27001, organizacija treba implementirati ISMS koji se temelji na procesu procjene rizika kako bi identificirala rizike za informacijsku imovinu. Kao dio ovog posla, organizacija treba odabrati, implementirati, nadzirati i pregledati razne mjere za upravljanje tim rizicima. Ove mjere su poznate kao kontrole. Organizacija mora odrediti prihvatljive razine rizika, uzimajući u obzir poslovne zahtjeve i definirane zahtjeve. Primjeri definiranih zahtjeva su zakonski i regulatorni zahtjevi ili ugovorne obveze. ISO/IEC 27001 može koristiti organizacija bilo koje vrste i veličine.

Sigurnosna područja koje se identificiraju u okviru ISMS-a prema aneksu A iz ISO/IEC 27001 su: politike informacijske sigurnosti, organizacija informacijske sigurnosti, sigurnost ljudskih resursa, upravljanje imovinom, kontrola pristupa, kriptografija, fizička sigurnost i sigurnost okoliša, operativna sigurnost, sigurnost komunikacija, nabavka sistema te razvoj i održavanje, odnosi s dobavljačima, upravljanje incidentima informacijske sigurnosti, aspekti informacijske sigurnosti kontinuiteta poslovanja, i usuglašenost. Tih 14 sigurnosnih područja osigurava sveobuhvatnost očuvanja informacija kao imovine, ali u konačnici u većini slučajeva gotovo cjelokupnu sigurnost korporacije ako se proširi i na ostale sisteme, a ne primjeni samo na informacijski sistem.

Relno promatrajući značaj informacije kao resursa u korporaciji za sve sisteme upravljanja može se postaviti pitanje: kako se može imati povjerenje u bilo koji sistem upravljanja, funkcioniranje korporacije ako nije uspostavljeno sigurnosno upravljanje informacijama temeljeno na ISMS-u.

Smatram da je svaka korporacija koja je implementirala bilo koji sistem upravljanja na temelju ISO standarda, a nije uspostavila ISMS

u biti na staklenim nogama i zlonamjerni zaposlenik, ili vanjski napadači na informacijski sistem može relativno lako ugroziti misiju korporacije, kao i ostvarenje njenih planiranih poslovnih ciljeva.

6. ZAKLJUČAK

Iz iznesenog nije teško uočiti značaj očuvanja informacija kao oblika imovine. Taj značaj često predstavlja strateško pitanje egzistencije korporacije, jer se može pokazati da informacije u pojedinim slučajevima mogu imati višestruko veću vrijednost od sve ostale imovine koju korporacija posjeduje.

U praksi se najčešće još uvijek sreće nedovoljna svijest o značenju i vrijednosti informacija na svim nivoima kako korporacija, tako općenito i društva. Pravu vrijednost informacija najbolje osjete pojedinci npr. kod krađe identiteta, korporacije kod manipulacije s poslovnim podacima i upravljačkim informacijama sistema, itd. Tada se obično bolnim putem otkriva značaj i važnost očuvanja informacija i njihov utjecaj na korporaciju. To može dovesti ne samo do financijskih gubitaka nego i do ljudskih žrtava.

Zato se postavlja pitanje: zar je nužno doživjeti tragediju i onda shvatiti da je učenje na greškama najskuplja škola, a problem počinje na nedovoljnoj svijesti i obrazovanosti ljudi ili automata koji donose odluke na temelju informacija, a da nisu u stanju utvrditi ispravnost upravo tih informacija.

LITERATURA

[1] ISO 31000:2009 - Risk management - Principles and guidelines, ISO
[2] Craig Schiller; Seth Fogie; Colby DeRodeff; Michael Gregg, Threat Analysis, Syngress, 2007, ISBN 978-1-59749-224-9
[3] Evgueni D. Solojentsev, Scenario Logic And Probabilistic Management Of Risk In Business And Engineering, Springer, 2008, ISBN 9780387779454
[4] Donald W. Marquardt: The ISO 9000 Family Of International Standards, McGraw-Hill Companies, Inc., 1998, ISBN 9780070340039
[5] Ray Tricker: ISO 9001:2008 For Small Businesses, Fourth Edition, Butterworth-Heinemann, 2009, ISBN 9781856178617
[6] ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
[7] ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements
[8] Dale Neef, Managing Corporate Reputation And Risk: A Strategic Approach Using Knowledge Management, Butterworth-Heinemann, 2003, ISBN 9780750677158