FER, Upravljanje informacijskim sustavima,
Prof. dr. sc. Krešimir Fertalj

Usporedba koncepata i metoda koje se koriste u područjima upravljanja informacijskim sustavima i upravljanja informacijskom sigurnošću – seminarski rad

Mr. sc. Aleksandar Klaić, dipl.ing.

Sadržaj

Sažetak:

U radu se analizira područja upravljanja informacijskim sustavima i upravljanja informacijskom sigurnošću, razmatra se metode i modele koji se koriste u ovim područjima i uspoređuje sličnost pristupa u području sustavskog inženjerstva i sigurnosnog inženjerstva. Opisuje se važnost životnog ciklusa razvoja sustava, arhitekture informacijskih sustava, modela zrelosti sustava, upravljanja rizikom, odabira sigurnosnih kontrola i primjene metrika, kako za sustavsko, tako i za sigurnosno inženjerstvo.

Ključne riječi:

Informacijski sustav, informacijska sigurnost, upravljanje, životni ciklus razvoja sustava, sustavsko, sigurnosno i programsko inženjerstvo, arhitektura informacijskog sustava, model zrelosti sustava, upravljanje rizikom, operativni rizik, sigurnosne i IT kontrole, metrika.

1. Uvod

Područje upravljanja informacijskim sustavima u značajnoj mjeri je povezano i utječe na razvoj područja upravljanja informacijskom sigurnošću. Povezanost s jedne strane proizlazi iz sve veće rasprostranjenosti informacijske tehnologije i usluga te sve veće ovisnosti poslovnih procesa o informacijskoj tehnologiji i uslugama, čime se posljedično javlja i sve veći broj sigurnosnih prijetnji koje su direktno ili indirektno povezane s informacijskim sustavima. S druge strane, metode upravljanja informacijskim sustavima su, razvojno gledano, uvijek bile korak ispred sigurnosti tih sustava. Razlog je uglavnom u tome da su na sustavniji način pratile razvoj i širenje tehnologije, dok je sigurnost velikim dijelom dolazila naknadno, najčešće kao reakcija na probleme iz prakse.

Pored toga, metode upravljanja informacijskim sustavima, nadograđuju se na tradicionalno područje upravljanja projektima poznato od 1950-tih, dok je razvoj informacijske sigurnosti, u nešto većoj mjeri počeo koristiti iskustva tradicionalne (vojne i nacionalne) sigurnosti, tek u 1990-tim godinama. Upravljanje projektima, upravljanje informacijskim sustavima, kao i upravljanje informacijskom sigurnošću, predstavljaju danas multidisciplinarna područja, što ih čini dodatno povezanim, a povijesnim razvojem sva tri područja u velikoj mjeri proizlaze iz tehničke problematike. Stoga je danas neke metode u upravljanju informacijskim sustavima i upravljanju informacijskom sigurnošću, kao što je upravljanje rizikom, primjena metrika, organiziranje programa i projekata, razvoj arhitekture informacijskih sustava, korištenje kontrola i sl., moguće primjenjivati u oba područja, koristeći zajedničke norme kao što je primjerice COBIT.

U okviru ovoga seminara prikazuju se neki koncepti i metode koje se koriste u području upravljanja informacijskim sustavima i u području upravljanja informacijskom sigurnošću, te se razmatra njihova uloga u okviru životnog ciklusa razvoja sustava. Nadalje, procjenjuje se njihov međusobni utjecaj i primjenjivost u ovim područjima.

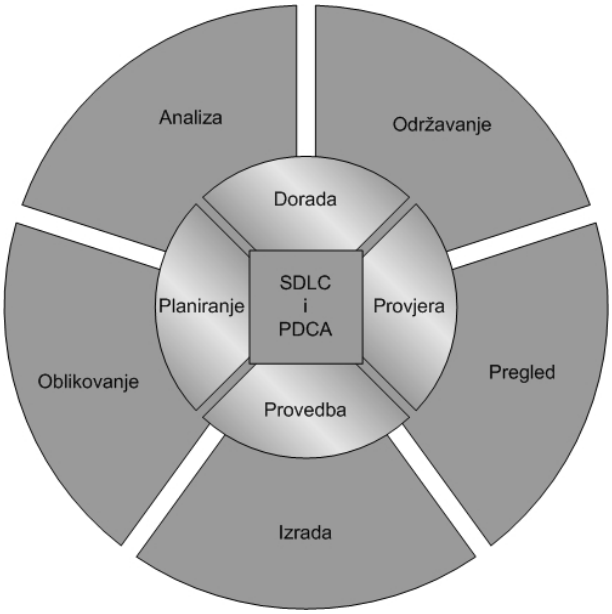
2. Životni ciklus razvoja sustava

Jedan od najvažnijih koncepata koji u velikoj mjeri povezuje metode koje se primjenjuju u različitim granama upravljanja, od projekata, preko informacijskih sustava, do informacijske sigurnosti, jeste životni ciklus razvoja sustava (engl. *System Development Life-cycle - SDLC*). Ovaj koncept razrađuje se sličnim modelima u različitim područjima kao što su sustavsko inženjerstvo i programsko inženjerstvo. U osnovi se radi o modelu kojim se opisuje određeni broj stanja sustava u okviru njegovog životnog ciklusa.

2.1. Modeli životnog ciklusa razvoja sustava

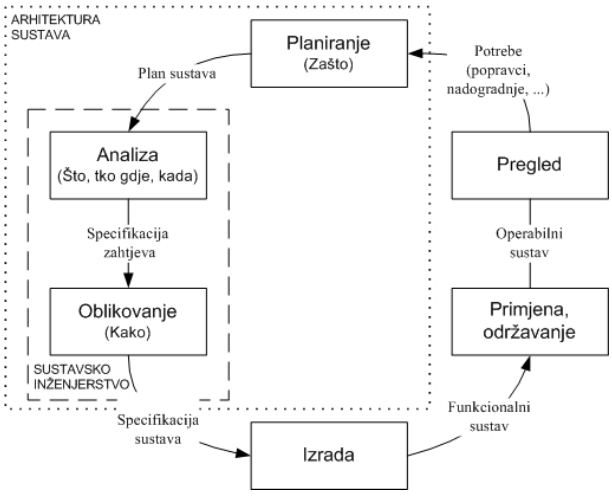
Tipičan životni ciklus razvoja sustava može se podijeliti u pet faza: analiza, oblikovanje, izrada, pregled i održavanje [1] [2] [3] (Sl.1.). Ciklus razvoja u svojoj osnovi predstavlja jednokratan proces, ali zbog niza postupaka kao što su popravci, dorade, prerade ili nadogradnje, on se ciklički ponavlja tijekom životnog ciklusa sustava. Ovakav proces sličan je PDCA procesu koji je uvela ISO/IEC organizacija u okviru niza normi u kojima se koriste sustavi upravljanja (npr. kvaliteta, okoliš, sigurnost) [4]. PDCA proces (engl. *Plan, Do, Check, Act*), koristi četiri faze:

planiranje, provedba, provjera i dorada (Sl.1.), koje se ciklički ponavljaju i u okviru kojih se razvija i dorađuje sustav upravljanja.



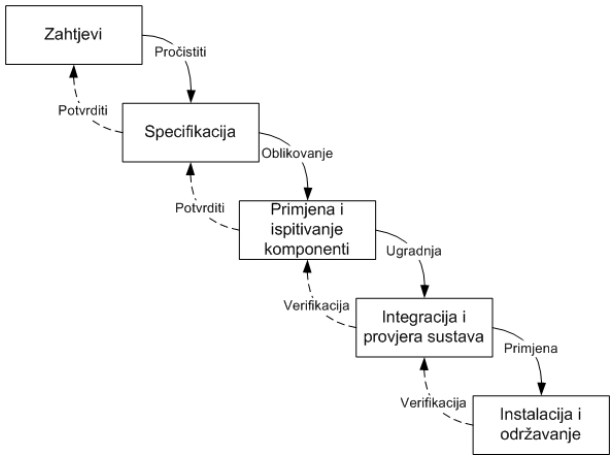
Slika 1. Životni ciklus razvoja sustava i PDCA proces.

Ovisno o vrsti sustava, faze životnog ciklusa mogu se nešto drugačije prikazivati. Tako je, primjerice u području upravljanja sigurnošću informacijskih sustava, uobičajeno koristiti sljedeće faze: planiranje / započinjanje, razvoj ili nabava / oblikovanje, provedba / izrada, uporaba / održavanje, odlaganje / povlačenje i uklanjanje iz uporabe [5] [12]. Životni ciklus za slučaj razvoja informacijskog sustava može se prikazati prema Sl.2. [1].

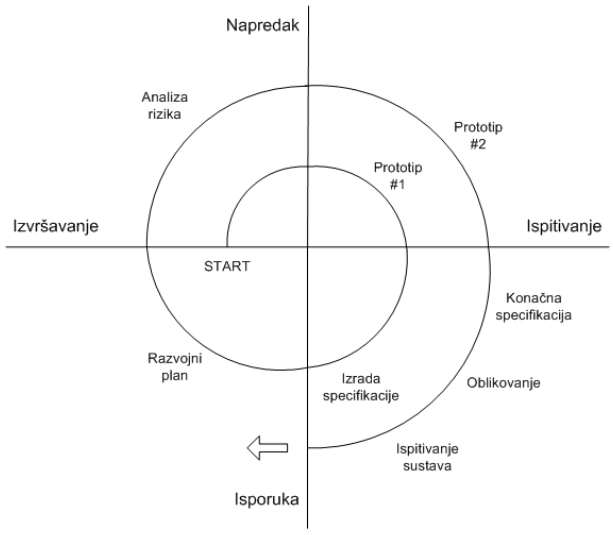


Slika 2. Životni ciklus i faze razvoja informacijskog sustava.

Uvođenje programskog, ali i sigurnosnog inženjerstva, ima za cilj uvođenje jasnih inženjerskih principa u svrhu postizanja ekonomičnih, pouzdanih i učinkovitih projektnih rješenja u ovim područjima, kao što je to i u slučaju sustavskog inženjerstva. U tu svrhu najčešće se primjenjuju tradicionalni, vodopadni model razvojnog procesa, od vrha prema dnu (Sl.3.), odnosno spiralni, iterativni model (Sl.4.) [1] [2] [7]. Osnovna razlika u primjeni je u tome da se spiralni model koristi u slučaju kada nije moguće na početku razvoja jasno utvrditi sve korisničke zahtjeve, odnosno tehničku specifikaciju koja iz njih proizlazi, te se u tom slučaju zahtjevi utvrđuju u iterativnom postupku kao na Sl.4.



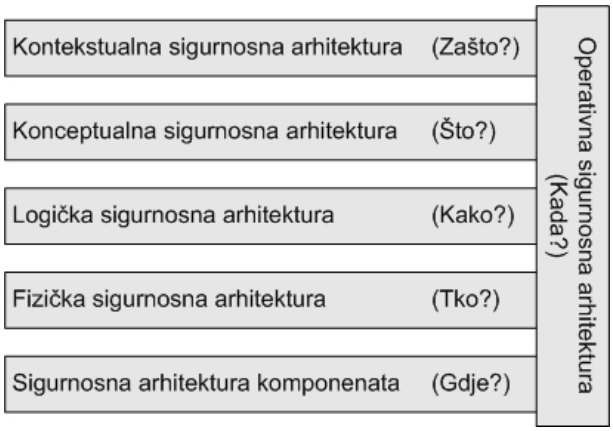
Slika 3. Vodopadni model razvojnog procesa.



Slika 4. Spiralni model razvojnog procesa.

2.2. Arhitektura informacijskog sustava

Kako je na Sl.2. naznačeno, razvoj arhitekture informacijskog sustava usko je povezan s fazama planiranja, analize i oblikovanja sustava. Tako se sigurnosna arhitektura sustava može prikazati prema [6] kroz šest slojeva arhitekture: kontekstualni, konceptualni, logički, fizički, komponentni i operativni sloj arhitekture (Sl.5.). Ovakav pristup sigurnosnoj arhitekturi vrlo je blizak fazama planiranja, analize i oblikovanja u okviru životnog ciklusa razvoja informacijskog sustava (Sl.2).

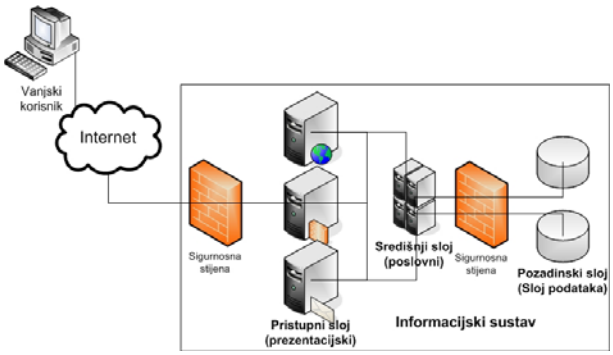


Slika 5. Slojevi sigurnosne arhitekture sustava.

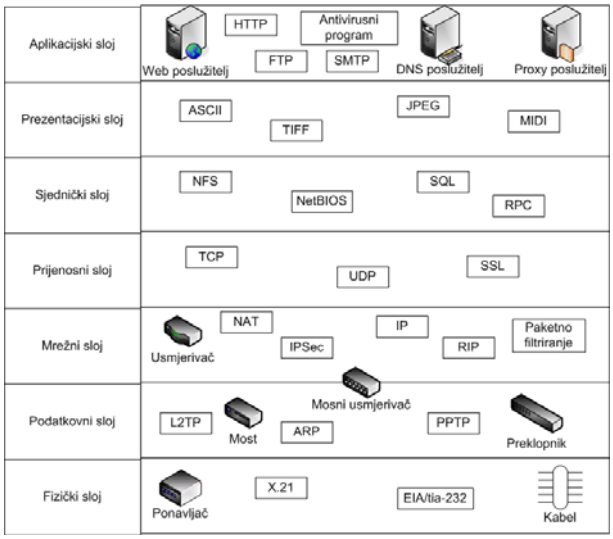
Arhitektura informacijskih sustava postala je važan razvojni faktor u izgradnji informacijskih sustava prvenstveno zbog njihove sve veće kompleksnosti. Isprva se to uočavalo kroz arhitekture operativnih sustava, a razvojem informacijske i komunikacijske tehnologije te širenjem Interneta, pristup izgradnji informacijskih sustava, kroz određene referentne modele arhitekture, postaje sve uobičajeniji. Neki od referentnih modela arhitekture informacijskih sustava usmjereni su na sigurnosnu problematiku pa se to obično naglašava u nazivu [6] [14], dok su drugi više usmjereni na aspekt funkcionalnosti samog informacijskog sustava [10] [13].

Jedan od važnih razloga za razvoj modela arhitekture informacijskih sustava, osobito u posljednjih dvadesetak godina, jeste sve veća potreba interoperabilnosti informacijskih sustava. U tom smislu, tipičan primjer takvih potreba predstavlja jedna međunarodna organizacija kao što je NATO, u okviru koje je potrebno na određeni način usuglasiti čitav niz NATO-vih, ali i nacionalnih, informacijskih sustava država članica, kako bi se osigurala učinkovita razmjena podataka [9]. Tako je NATO potkraj 1990-tih razvio koncept *NATO Command, Control, and Communication Technical Architecture – NC3TA*, kako bi poboljšao mogućnosti dijeljenja podataka (engl. *information sharing*), odnosno bolje interoperabilnosti između različitih NATO-vih i nacionalnih informacijskih sustava. Sredinom ovog desetljeća, NATO je otišao korak dalje razvojem *NATO Network Enabled Capability - NNEC* koncepta, čime je osim već prije definiranog cilja s NC3TA modelom arhitekture, otvorio novi koncept zahtjeva na proširenje mrežnih mogućnosti logističkih i vojnih sustava, gdje god i kad god je to moguće. Tako se utvrđuju zahtjevi mobilne interoperabilnosti različitih informacijskih sustava u operativnoj primjeni na područjima od interesa NATO-a. To znači potrebu razvoja modularnih informacijskih sustava, s povećanim zahtjevima interoperabilnosti na relaciji NATO - nacionalni sustavi, odnosno podrška za međusobno povezivanje takvih mobilnih i modularnih sustava u operativnoj primjeni i borbenim djelovanjima. Pored toga, zahtjevi koji su postavljeni pred NNEC koncept uključuju i povezivanje svih razina upravljanja i odlučivanja, tj. povezivanje operativnog, taktičkog i strateškog nivoa zapovijedanja, upravljanja i komuniciranja (engl. *Command, Control, and Communication - C3*), što obuhvaća sve sustave od senzorskih, preko oružanih, do potpore odlučivanju i suradnje u međunarodnom okruženju [10].

Kompleksnost informacijskih sustava i otvorenost prema Internetu, odnosno potreba za javnim informacijskim servisima, dovela je do primjene višeslojne arhitekture informacijskih sustava, tipično dvoslojne i troslojne [11]. Slojevita arhitektura omogućila je modularni pristup razvoju aplikativne programske podrške, ali i primjenu sigurnosnih elemenata prateći tradicionalni sigurnosni koncept obrane po dubini (engl. *defence-in-depth*) (Sl.6.). Troslojni pristup arhitekturi informacijskog sustava tako obuhvaća prezentacijski ili pristupni sloj (engl. *front-end tier*), središnji sloj (engl. *middle tier / middleware / business tier*) i pozadinski sloj (engl. *back-end tier*). Na sličan način, arhitektura za interkonekciju otvorenih sustava (ISO/OSI referentni model) predviđa slojeviti, modularni pristup komunikaciji između sustava. Na Sl.7. prikazani su neki tipični uređaji, protokoli i aplikacije po slojevima ISO/OSI modela.



Slika 6. Troslojna arhitektura informacijskog sustava s pristupnim, središnjim i pozadinskim slojem

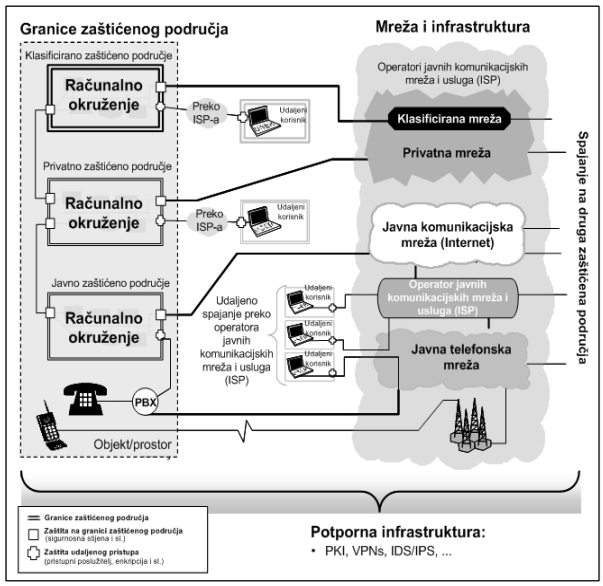


Slika 7. ISO/OSI referentni model i primjeri uređaja, protokola i aplikacija u pripadnim slojevima modela

Čitav niz modela funkcionalnih arhitektura informacijskih sustava, odnosno sigurnosnih arhitektura informacijskih sustava, razvijen je na ovim temeljnim konceptima.

Jedan od utjecajnijih modela sigurnosnih arhitektura informacijskih sustava je tehnički okvir za osiguravanje informacija - IATF (engl. *Information Assurance Technical Framework*), sponzoriran od američke Nacionalne sigurnosne agencije (engl. *National Security Agency – NSA*), koji je u stvari predstavljao zajedničke preporuke u području osiguravanja informacija za sektor državne uprave, gospodarski i akademski sektor. Zajedničkim razvojem, kroz suradnju predstavnika različitih institucija iz spomenuta tri sektora, postignuta je IATF V3.1 specifikacija čiji utjecaj se kasnije pokazao značajnim u stvaranju resornih i sektorskih arhitektura, kao što je primjerice arhitektura Ministarstva obrane SAD-a, Global Information Grid (GIG) [13]. GIG je korporativna, strateška poslovna mreža, koja istovremeno objedinjava i elemente taktičkog i operativnog sloja upravljanja, na sličan način kao prije spomenuti NATO NNEC koncept.

IATF definira proces razvoja informacijskog sustava s odgovarajućim osiguravanjem informacija i sigurnosnim zahtjevima za sklopovske i programske komponente koje se koriste u projektiranju informacijskog sustava. Od tri ključna elementa politike informacijske sigurnosti: osoba, procesa i tehnologije, IATF adresira tehnološki element te primjenjuje strategiju obrane po dubini. Četiri glavna tehnološka područja ove strategije obrane po dubini su: obrana mreže i infrastrukture, obrana granica zaštićenih područja, obrana računalnog okruženja i obrana potporne infrastrukture. Iako je razvoj IATF modela nastao na prijelazu stoljeća i danas više nije aktivan (V3.1 iz 2002.g. je završna inačica), temeljna strategija pristupa IATF sigurnosne arhitekture preuzeta je u nizu drugih pristupa arhitekturi informacijskih sustava (Sl.8.).



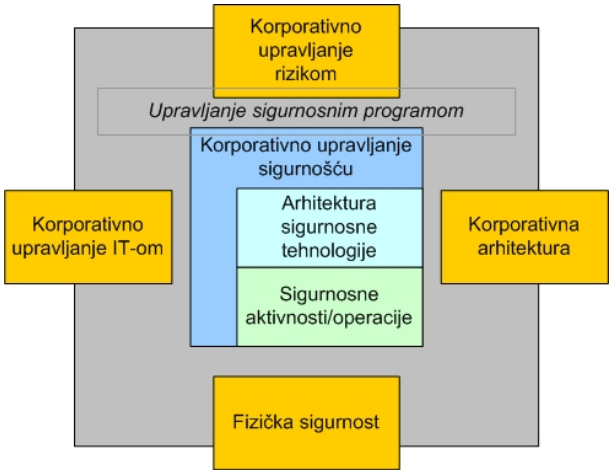
Slika 8. IATF model sigurnosne arhitekture i osnovni elementi strategije obrane po dubini

Prema [15] smjer kojim se treba kretati u daljnjem razvoju informacijske sigurnosti nužno vodi prema povezivanju korporativne razine upravljanja (vršna organizacijska razina kompleksnog organizacijskog sustava) sa sigurnosnom arhitekturom. Primarni razlog je u širokom utjecaju intenzivnog razvoja informacijske i komunikacijske tehnologije tijekom posljednjih

20-tak godina. Ovaj utjecaj značajno je izmijenio kako poslovni sektor, tako i državni sektor, ali istovremeno i sektor nacionalne sigurnosti u širem smislu (spektar od obrane, preko sigurnosno-obavještajnog segmenta, do javne sigurnosti). Stvaranje informacijskog prostora i pridruženih kibernetičkih prijetnji [16], rezultiralo je međusobno povezanim mrežama i drugom infrastrukturom koja, u određenoj mjeri, čini međusobno povezanim i ranjivim, spomenuta tri sektora. Zaštita ovakve, kritične nacionalne infrastrukture, od telekomunikacija, preko energije, vode, transporta i sl., čini nužnim povezivanje poslovne i sigurnosne politike, odnosno postavlja potrebu razrade poslovnom politikom upravljene sigurnosne arhitekture, što je i osnovni motiv razvoja metode iz [15]. Na sl. 9. slikovito je pokazana veza između koncentričnih krugova koji predstavljaju segmente modela korporativne sigurnosne arhitekture razrađene u [15]. Tako, primjerice, novi zahtjev privatnosti koji bi se postavio u određenom konkretnom slučaju, generirao bi nove principe upravljanja, politike i standarde, kao i primjenu nove tehnološke arhitekture. Implementacija novih standarda i arhitekture može povratno uzrokovati stvaranje novih sigurnosnih procesa ili drugih sposobnosti unutar segmenta aktivnosti/provedbe na Sl.9.

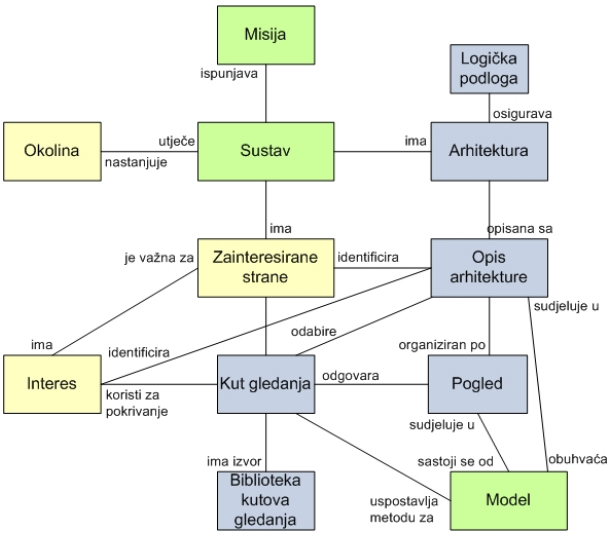
Slika 9. Model programa sigurnosti na korporativnoj razini

Na Sl.10. prikazane su na vanjskom rubu četiri korporativne komponente s kojima sigurnosna arhitektura mora biti na određeni način usklađena: korporativno upravljanje rizikom, korporativno upravljanje IT-om, korporativna arhitektura i fizička sigurnost. Zbog pomaka usmjerenosti modela na korporativnu razinu, upravljanje sigurnosnim programom odvija se u pozadini i postavlja se u širi kontekst korporativne razine poslovnog upravljanja. U tom smislu u sredini slike je postavljeno korporativno upravljanje sigurnošću sa elementima arhitekture sigurnosne tehnologije i sigurnosnih aktivnosti/operacija.



Slika 10. Komponente korporativne sigurnosne arhitekture

Norma IEEE Std 1471-2000, objavljena u rujnu 2000.g. [17] [18], preuzeta i od ISO organizacije u srpnju 2007.g. kao ISO/IEC 42010:2007, utvrđuje preporučenu praksu za opis arhitekture programski intenzivnih sustava. Ova norma predstavlja općeprihvaćene trendove u praksi opisa arhitekture i nudi referentni okvir za korištenje u ovom području, s ciljem postavljanja temelja za podizanje kvalitete sustava, ali i za postizanje ušteda pri realizaciji programski intenzivnih sustava. Programski intenzivni sustavi su kompleksni sustavi kod kojih programska podrška suštinski doprinosi projektiranju, konstrukciji, primjeni ili unaprjeđivanju sustava kao cjeline. Ogromna većina današnjih poslovno-tehnoloških sustava, odnosno kritična informacijska infrastruktura općenito [19], u velikoj mjeri zadovoljava ovu definiciju. Upravo zbog toga pristup arhitekturi sustava jednako je značajan bilo da ga promatramo iz kuta IT-a ili informacijske sigurnosti. Na Sl. 11. prikazan je koncepcijski model opisa arhitekture iz IEEE Std 1471-2000.



Slika 11. Koncepcijski model opisa arhitekture iz IEEE Std 1471-2000

Definicija arhitekture ovdje predstavlja najvišu razinu koncepcije sustava u njegovoj okolini (apstrakcija), dok je opis arhitekture model kojim se prikazuje određeno svojstvo arhitekture sustava. U tom smislu svaki sustav posjeduje određenu arhitekturu, a opis te arhitekture može biti normiran na predloženi način, kako bi se omogućila primjena standardnih rješenja u inženjerskoj praksi projektiranja. U tom smislu definira se i kut gledanja (engl. *viewpoint*), koji je dio modela arhitekture i obuhvaća interese koje zainteresirane strane žele postići prikazom, odnosno specifični pogled (engl. *view*) na prikaz arhitekture sustava (koncepcijski, logički, fizički i sl.) [6], što je u Tablici 1. prikazano za SABSA model arhitekture [6].

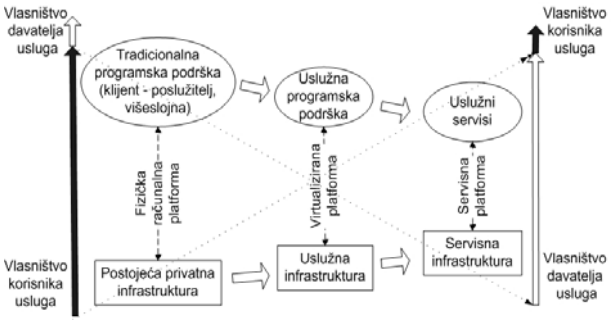
Tablica 1. SABSA matrica razrade šest pogleda na arhitekturu (apstrakcija) temeljem šest pitanja za razradu vertikalnih elemenata sadržaja pojedinih pogleda:

Razrada: / **Pogled:**	**Vrijednosti (Što?)**	**Motivacija (Zašto?)**	**Proces (Kako?)**	**Osobe (Tko?)**	**Lokacija (Gdje?)**	**Rokovi (Kada?)**
Kontekstualni	Poslovanje	Model poslovnog rizika	Model poslovnog procesa	Poslovna organizacija i svi povezani	Geografija poslovanja	Ovisno o poslovnim rokovima
Konceptualni	Profil poslovnih atributa (štićene vrijednosti)	Upravljački ciljevi	Sigurnosna strategija i arhitektonski slojevi	Model sigurnosnog entiteta i okvir povjerenja	Model sigurnosne domene	Sigurnosno povezani životni ciklus i rokovi
Logički	Model poslovnih informacija	Sigurnosne politike	Sigurnosni servisi	Shema entiteta i profila prava/privilegija	Definicija sigurnosne domene i poveznica	Ciklus sigurnosnog procesa
Fizički	Poslovni podatkovni model	Sigurnosna pravila, prakse i procedure	Sigurnosni mehanizmi	Korisnici, aplikacije i korisničko sučelje	Platforma i mrežna infrastruktura	Provedba upravljačke strukture
Komponentni	Detaljne podatkovne strukture	Sigurnosni standardi	Sigurnosni proizvodi i alati	Identiteti, funkcije, akcije i ACL-ovi	Procesi, čvorovi, adrese i protokoli	Rokovi sigurnosnih koraka i sekvenci
Operativni	Osiguravanje operacijskog kontinuiteta	Upravljanje operativnim rizicima	Upravljanje i podrška sigurnosnih servisa	Upravljanje i podrška aplikacijama i korisnicima	Sigurnost čvorova, mreža i platformi	Plan sigurnosnih operacija

Definicija arhitekture u najboljoj praksi je da predstavlja temelje organizacije sustava ugrađene u komponenete sustava, međuodnos komponenata kao i odnos prema okolini i načela kojima se vodi pri projektiranju i unaprjeđivanju sustava. Na Sl.11. vidljivo je kako opis arhitekture, osim obilježja sustava, uključuje opis sustava u kontekstu okoline, tj. utjecaje različite prirode kao što je razvojna, tehnološka, poslovna, operativna, organizacijska, politička, regulatorna, socijalna i sl. Nadalje, uvode se zainteresirane strane koje predstavljaju klijente sustava, korisnike, one koji održavaju ili razvijaju sustav, dobavljače, regulatore, vlasnike i sl. Pri tome je moguć čitav niz interesa kao što su: pristup podacima, integritet podataka, fleksibilnost, rasprostranjenost,

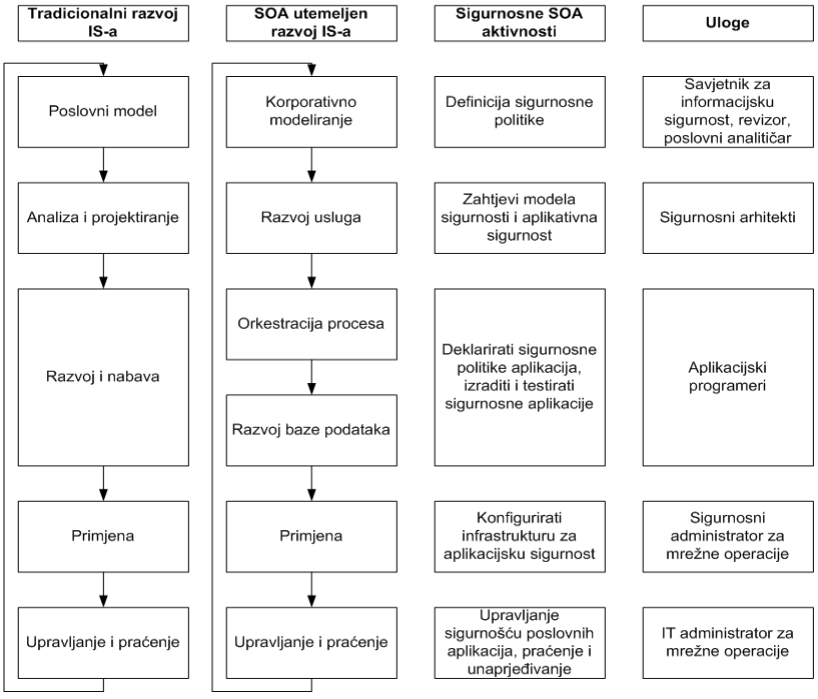
osiguravanje informacija, modularnost, otvorenost, performanse, kvaliteta usluga, iskoristivost i sl.

Važnost aspekta arhitekture informacijskih sustava može se promatrati i kroz koncept uslužno orijentirane arhitekture (engl. *Service Oriented Architecture – SOA*), koji po mnogim analitičarima predstavlja arhitekturu budućnosti u području informacijskih sustava. Na Sl. 12. prikazana je uzajamna migracija programske podrške i računalne infrastrukture u smjeru servisno orijentirane arhitekture [20].



Slika 12. Evolucija programske podrške i računalne infrastrukture u smjeru servisno orijentirane arhitekture

Razlog zbog kojega evolucija prikazana na Sl.12. utječe na koncept arhitekture informacijskih sustava leži i u funkcionalnom i u sigurnosnom aspektu [22]. S funkcionalne strane težnje razvoja servisno orijentirane arhitekture slične su težnjama koje potiču normizaciju: mogućnost višestrukog korištenja računalnih resursa prema potrebi i s mogućnošću plaćanja na temelju efektivnog korištenja. Takav pristup vodi s jedne strane prema normizaciji kako bi različita rješenja bila međusobno iskoristiva i upariva, ali s druge strane vodi i prema specijalizaciji, s jedne strane korisničkog profila, a s druge strane uslužne podrške. U tom smislu SOA uvodi princip razdvajanja interesa, s jedne strane specijalizaciju na davanje usluga, a s druge strane specijalizaciju na korištenje usluga. U tom smislu se često puta i naglašava da je SOA više stil prikaza arhitekture nego nova arhitektura sama po sebi. Gledano s aspekta arhitekture informacijskog sustava u smislu apstrakcije rada sustava, može se reći da je višeslojni pristup klijentsko-poslužiteljskog modela osiguravao velike sličnosti u svemu osim u spomenutom modelu razdvajanja interesa. Upravo kao posljedica ovog modela razdvajanja interesa pojavljuju se prikladni protokoli komuniciranja (npr. Simple Object Access Protocol – SOAP) i opisni jezici (WSDL, XML, …), koji omogućavaju specijaliziranje na razvoj programske podrške za uspostavljanje interoperabilnih računalnih servisa koji se mogu koristiti na otvorenom tržištu servisno orijentiranih usluga.



Slika 13. Sigurnost u kontekstu životnog ciklusa razvoja informacijskog sustava temeljenog na SOA-i

Sigurnost SOA-e svodi se na elemente kao što su sigurnost i kontrola podataka, razvoj i korištenje SOA-e, koncept autentifikacije pri korištenju servisa, ili zahtjevi na tržišno dobavljive servisne komponente (engl. *Commercial of the shelf – COTS*). To znači da je moguće koristiti tradicionalni pristup najbolje prakse i norme kao što je ISO/IEC 27000 familija normi, zatim različite tehničke standarde za primjerice autentifikaciju, kriptografiju i drugo, u okviru web servisa, odnosno elemente sigurnosti ugrađene u okviru razvoja i implementacije web servisa. Usporedba razvoja životnog ciklusa pri tradicionalnom razvoju informacijskog sustava i razvoja informacijskog sustava temeljenog na SOA-i, sa fazama životnog ciklusa sigurnosnih aktivnosti pri razvoju SOA-e i ulogama koje imaju određene osobe za ove sigurnosne faze, prikazano je na Sl. 13. [21].

2.3. Model zrelosti sustava

Model zrelosti sustava (engl. *Capability Maturity Model – CMM*) uobičajeno se koristi u svrhu praćenja i procjenjivanja stanja razvojnog ciklusa velikih i kompleksnih projekata. Tipična primjena je i u procesima informatizacije kakvi su različiti e-Government projekti. Izvorno je model zrelosti nastao sredinom osamdesetih godina prošlog stoljeća, u svrhu poboljšanja procesa razvoja programske podrške. Cilj razvoja modela bio je povećavanje kvalitete razvoja, odnosno odgovarajući poticaj organizaciji za transformaciju vlastitih poslovnih procesa od neuređenih do zrelih procesa, koji se kontinuirano poboljšavaju. Od početka devedesetih godina prošlog stoljeća SEI (Software Engineering Institute), pri Carnegie Mellon sveučilištu u Pittsburghu, SAD, razvijao je CMM (Capability Maturity Model) modele, primjenjive za različite discipline, ali primarno usmjerene na programsko i sustavsko inženjerstvo [24].

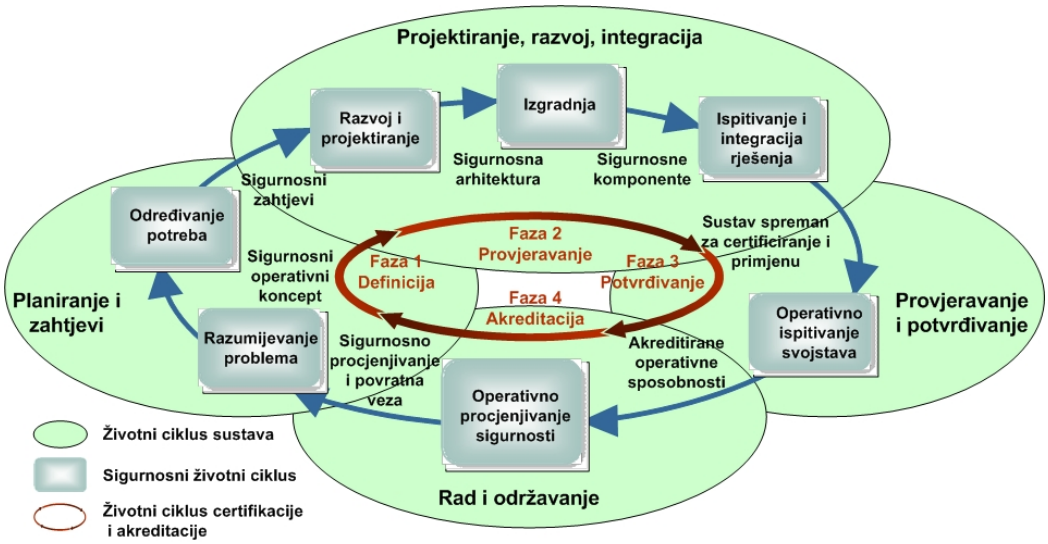
CMM model se uobičajeno sastoji od 5 stanja zrelosti procesa koji moraju imati jasno opisano osnovno načelo svakog stanja, detaljni opis kako prepoznati ostvareno stanje te osnovna obilježja svakog stanja. Kako se praćenje stanja zrelosti provodi za proces koji se sastoji od niza procesnih područja koja mogu biti različite razine zrelosti, razlikujemo fazni i kontinuirani model zrelosti. Fazni model podrazumijeva da sva procesna područja moraju biti na istoj razini zrelosti, kako bi proces mogao prijeći na sljedeću razinu, dok kod kontinuiranog modela pojedina procesna područja mogu imati različite razine zrelosti, odnosno može se postaviti prioritete na postizanje zrelosti određenih procesnih područja.

Model zrelosti za sustavsko sigurnosno inženjerstvo (engl. *System Security Engineering Capability Maturity Model - SSE CMM*) odigrao je važnu ulogu u povezivanju koncepata sigurnosnog inženjerstva [7], po uzoru na sustavsko inženjerstvo. Gledano iz kuta modela zrelosti, ono što povezuje modele zrelosti sustavskog inženjerstva i sustavskog sigurnosnog inženjerstva, jesu projektne i organizacijske prakse zrelosti procesa.

Razvoj modela zrelosti za sustavsko sigurnosno inženjerstvo započet je u ranim 90-tim godinama prošlog stoljeća, na inicijativu Nacionalne sigurnosne agencije iz SAD-a (engl. *National Security Agency - NSA*), u suradnji državnog i industrijskog sektora, a 2002.g., tako razvijeni model SSE CMM prihvatio je ISO/IEC kao novu normu 21827 [23] [25]. Osnovna ideja SSE CMM modela, odnosno norme ISO/IEC 21827, u stvari je integracija sigurnosnog životnog ciklusa u sustavski životni ciklus, čime se uvelike olakšavaju postupci certifikacije i akreditacije, odnosno osiguravanja informacija (engl. *information assurance - IA*), što je prikazano na Sl.14. Model SSE CMM omogućava postizanje nekoliko važnih ciljeva sigurnosnog inženjerstva:

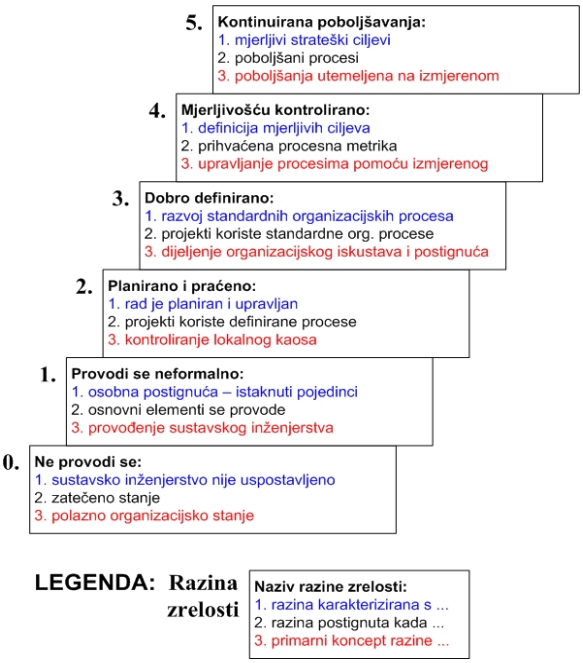
1. unaprjeđivanje procesa korištenjem ovog alata za evaluaciju sigurnosne prakse i usmjeravanje na poboljšanja;
2. osiguravanje organizacijskog povjerenja temeljenog na evaluaciji;
3. upravljanje rizicima temeljeno na mehanizmima mjerenja i praćenja organizacijskih sposobnosti;
4. procjenjivanje sposobnosti ponuditelja usluga sigurnosnog inženjerstva.

Certifikacija je pri tome postupak provjeravanja i potvrđivanja sukladnosti uređaja ili sustava sa specificiranim zahtjevima (primjerice norma ili utvrđena sigurnosna politika) i uobičajeno u području sigurnosti informacijskih sustava predstavlja korak prije akreditacije. Akreditacija je općenito postupak odobravanja rada organizacije ili informacijskog sustava u okvirima prihvatljive i utvrđene razine rizika [7].



Slika 14. Integracija sigurnosnog inženjerstva u životni ciklus sustavskog inženjerstva u svrhu omogućavanja uspješne primjene osiguravanja informacija

Na Sl.15. prikazan je tipičan primjer unaprjeđenja procesa temeljenog na modelu zrelosti, na kojem su označena glavna obilježja razina zrelosti, opis kada se razine dostižu, kao i primarna načela koja obilježavaju pojedine razine zrelosti. Općenito se razine zrelosti, neovisno o području primjene modela, najčešće nazivaju: inicijalna, ponovljiva, definirana, upravljana i optimizirana.



Slika 15. Primjer modela zrelosti za sustavsko sigurnosno inženjerstvo (SSE CMM)

U osnovi se metode sustavskog inženjerstva, metode programskog te sigurnosnog inženjerstva, kao i metode upravljanja kvalitetom i čitav niz najboljih praksi za upravljanje projektima ili sigurnošću, može promatrati u širem kontekstu programa poboljšavanja procesa (engl. *Process Improvement Program – PIP*).

Integracija modela zrelosti (engl. Capability Maturity Model Integration – CMMI) predstavlja nastavak razvoja CMM modela u smjeru zajedničkog okvira za različite modele (programsko, projektno, sustavsko i drugo inženjerstvo). To je nastavak projekta CMM u kojem sudjeluju predstavnici državnog i industrijskog sektora, uz nositelja the Carnegie Mellon Software Engineering Institute (SEI).

3. Upravljanje informacijskim sustavima i upravljanje informacijskom sigurnošću

Usporedbu koncepata i metoda u području upravljanja informacijskim sustavima i upravljanja informacijskom sigurnošću, razmotrit ćemo u okviru analize tri tipična područja u okviru upravljanja u kojima postoje sličnosti. Ova tri područja su područje upravljanja rizikom, područje sigurnosnih, odnosno IT kontrola, te područje metrike, odnosno općenito mjerenje u upravljanju procesima.

3.1. Upravljanje rizikom

U nastavku na poglavlje 2.3. Model zrelosti sustava, osvrnut ćemo se na primjenu modela zrelosti u području osiguravanja informacija, koja je usmjerena na poboljšavanje stanja upravljanja informacijskim rizicima u državnom sektoru Velike Britanije [26]. Ovaj model zrelosti osiguravanja informacija i okvira za procjenjivanje (engl. *Information Assurance Maturity Model and Assesment Framework*) sastoji se od modela zrelosti s pet razina i šest procesnih područja čija se stanja zrelosti opisuju u modelu. Pored toga, razrađen je okvir za procjenjivanje osiguravanja informacija, koji je predviđen za provedbu procesa revizije, ali i za interno praćenje stanja zrelosti u organizaciji. Sadržaj modela zrelosti i okvira za procjenjivanje uključuje obvezujuće zahtjeve sigurnosne politike [27] [28], a usklađen je sa zahtjevima za sustav upravljanja informacijskom sigurnošću (engl. *Information Security Management Framework – ISMS*) iz norme ISO/IEC 27001:2005. U okviru modela razrađeno je šest procesnih područja:

1. vođenje i korporativno upravljanje;
2. obuka, edukacija i svijest;
3. upravljanje informacijskim rizikom;
4. cjeloživotne mjere osiguravanja informacija;
5. osiguravanje dijeljenja informacija;
6. sukladnost.

Prva tri područja usmjerena su na poticanje razvoja i ugradnju kulture upravljanja informacijskim rizikom u državna tijela Velike Britanije. U četvrtom i petom području provodi se najbolja praksa mjera osiguravanja informacija, a u šestom se uvodi usklađeni program sukladnosti u području osiguravanja informacija.

Svako od ovih šest procesnih područja razrađeno je opisom pet razina zrelosti:

1. inicijalna (svijest o kritičnosti osiguravanja informacija za poslovanje);
2. uspostavljena (procesi osiguravanja informacija su institucionalizirani);
3. poslovno omogućena (procesi osiguravanja informacija su implementirani u kritičnim područjima poslovanja);
4. kvantitativno upravljana (broj izuzeća u implementaciji osiguravanja informacija na korporativnoj razini je poznat i opisan izvješćima);
5. optimizirana (odgovarajući procesi osiguravanja informacija su integralni dio normalnog poslovanja).

Svako od šest procesnih područja razrađeno je na ovih pet razina zrelosti čitavim nizom dodatnih obvezujućih elemenata opisa koji predstavljaju zahtjeve za ispunjavanje zrelosti svake pojedine razine zrelosti za pojedino procesno područje. Elemente opisa čine pitanja kojima se potvrđuje razina zrelosti i činjenice koje treba utvrditi da bi se utvrdila određena razina zrelosti. Primjerice za procesno područje 4. (cjeloživotne mjere osiguravanja informacija) razinu zrelosti 3. (poslovno omogućeni procesi osiguravanja informacija su implementirani u kritičnim područjima poslovanja), jedan od devet elemenata koji se provjerava jeste: 3.5 detekcija ranjivosti. Pitanja i činjenice koji su okvirom osiguravanja informacija utvrđeni za točku 3.5 su:

1. Je li proces otkrivanja ranjivosti poslovno kritičnih sustava institucionaliziran?
   a. Utvrditi detalje procesa i njegov doseg.
2. Jesu li postavljeni specifični ciljevi za smanjenje ranjivosti temeljeni na prijetnjama, lakoći iskorištavanja ranjivosti i potencijalnom utjecaju?
   a. Utvrditi detalje ciljeva i plan za smanjenje ranjivosti.
3. Poduzimaju li se penetracijska ispitivanja redovito i provodi li ih odobreno tijelo sukladno preporukama?
   a. Provjeriti izvješće penetracijskog ispitivanja i slijedne planove aktivnosti.

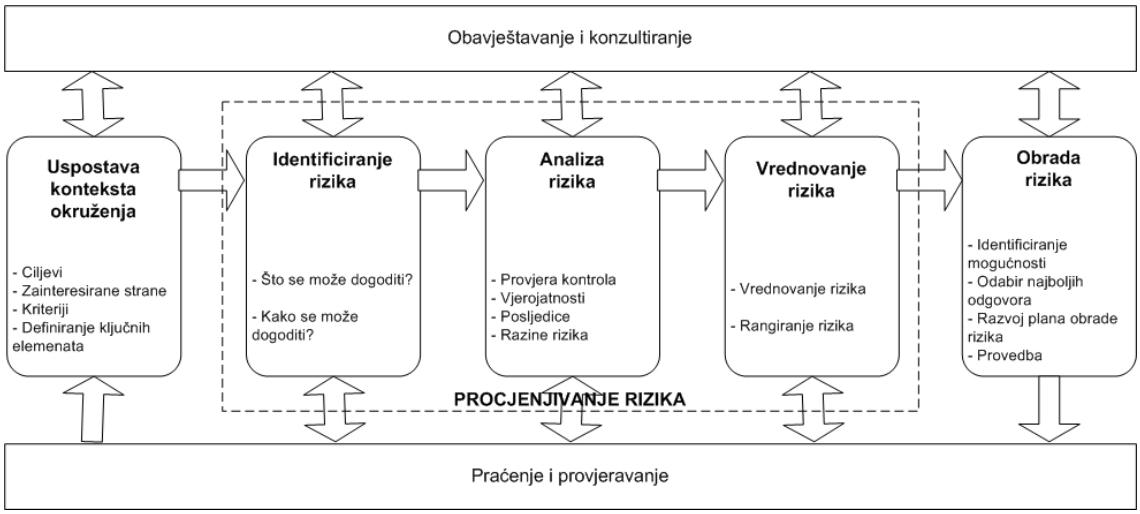
Prikazana metoda koja kombinira model zrelosti i okvir za mjere osiguravanja informacija, osigurava uvođenje upravljanja rizicima, podizanje razine mjera osiguravanja informacija, ali i stalno praćenje stanja mjera u različitim institucijama državnog sektora te usporedbu tih stanja.

Koncept metoda procjenjivanja i upravljanja rizicima sigurnosti informacijskih sustava u državnom sektoru, u osnovi se sastoji od tri faze, kao što je prikazano na Sl.16. [30] [31]:

1. procjenjivanje rizika (identificiranje, analiza i vrednovanje),

2. obrada rizika (izbjegavanje, smanjenje, prihvaćanje i prijenos),
3. uspostava cjeloživotnog procesa upravljanja rizikom.

Kako bi upravljanje rizikom sigurnosti informacijskog sustava bilo učinkovito implementirano u okviru određene organizacije, nužno ga je integrirati u životni ciklus razvoja informacijskog sustava [3] [31]. U Tablici 2. prikazana je podjela životnog ciklusa razvoja sustava (SDLC) sa osnovnim karakteristikama faza razvoja te je u desnoj koloni prikazana mogućnost integracije mjera upravljanja rizikom u svaku od faza životnog ciklusa.



Slika 16. Faze procesa upravljanja rizikom

Tablica 2. Integracija upravljanja rizikom u životni ciklus razvoja sustava:

Faze životnog ciklusa razvoja sustava (SDLC)	Karakteristika faze	Potpora aktivnosti upravljanja rizikom
1. Početni zahtjevi	Izražava se potreba te dokumentira namjena i opseg IT sustava	Identificirani rizici se koriste u razvoju zahtjeva sustava, uključujući sigurnosne zahtjeve, kao i sigurnosni operativni koncept (strategija)
2. Razvoj ili nabava	IT sustav je projektiran, nabavljen, programiran, razvijen ili na drugi način konstruiran	Rizici koji su identificirani tijekom ove faze mogu biti korišteni za podršku sigurnosne analize IT sustava koja može voditi u potrebu izmjena arhitekture ili projekta tijekom razvoja sustava
3. Izvedba	Sigurnosna obilježja sustava trebaju biti konfigurirana, omogućena, ispitana i potvrđena	Proces upravljanja rizicima podržava procjenjivanje izvedbe sustava sukladno početnim zahtjevima i u okviru modeliranog operativnog okruženja. Odluke koje se tiču identificiranih rizika moraju biti donesene prije puštanja sustava u rad i odgovarajuće sigurnosne kontrole trebaju biti implementirane.
4. Primjena i održavanje	Sustav izvodi predviđene funkcionalnosti. Tipično, sustav se prilagođava na stalnoj osnovi kroz dodavanje sklopovske ili programske podrške, kao i	Aktivnosti upravljanja rizikom provode se kroz periodičnu reakreditaciju sustava ili kada se događaju velike promjene u IT sustavu u njegovoj operativnoj - produkcijskoj okolini (npr. nova sučelja na

	promjenama organizacijskih procesa, politika i procedura.	sustavu – ispitivanje kontrola i zaštitnih mjera).
5. Odlaganje	Ova faza može uključivati odlaganje sklopovske i programske podrške te dokumentacije sustava. Aktivnosti mogu uključivati prenošenje, arhiviranje, uništavanje podataka, kao i odgovarajuće zbrinjavanje sklopovske i programske podrške.	Aktivnosti upravljanja rizikom provode se za komponente sustava koje će se odlagati ili zamijeniti, kako bi se osiguralo odgovarajuće zbrinjavanje sklopovske i programske podrške te preostalih podataka u komponentama sustava, odnosno provođenje migracije sustava na siguran i sustavan način.

Upravljanje rizikom u području informacijske sigurnosti u novije vrijeme povezuje se s pojmom operativnog rizika. Iako ne postoji jednoznačna definicija operativnog rizika, najčešće se primjenjuje definicija nastala u okviru Basel II norme, koja opisuje operativni rizik kao rizik gubitka nastao zbog neodgovarajućih unutarnjih poslovnih procesa ili procesa u kojima postoje slabosti ili pogreške, odnosno zbog ljudskog faktora i tehničkih sustava ili zbog vanjskog događaja [16].

Basel norma je vršni dokument sektorske regulative bankarstva, koji u stvari predstavlja međunarodnu bankovnu normu koju je kreirao Bazelski odbor za bankovni nadzor (Basel Committee on Banking Supervision – BCBS). BCBS se sastoji od predstavnika središnjih banaka i bankovnih regulatora iz nekoliko EU država, Japana i SAD-a, koji potiču međunarodnu kooperaciju banaka i izdaju smjernice za nadzor banaka. Iako aktualna inačica Basel II norme nije zakon, njegovi zahtjevi preuzimaju se u zakonodavstvima velikog broja država u svijetu (npr. EU direktive 2006/48/EC, 2006/49/EC, koje su obvezujuće za sve države članice EU) i propisuju se kroz različite nacionalne propise koji mogu biti zakoni, uredbe ili pravilnici, odnosno odluke središnjih banaka, kao nadležnih tijela. U RH je preuzimanje Basel II norme utvrđeno donošenjem novog Zakona o kreditnim institucijama (NN 117/08) te čitavim nizom predviđenih podzakonskih akata [32].

Definicija operativnog rizika kao rizika od gubitka izdvaja ga od tipičnih financijskih rizika koji su spekulativne prirode, odnosno rizika koji se poduzimaju u smislu ostvarivanja dobiti (npr. kreditni rizik ili valutni rizik). Nadalje, povezanost operativnog rizika s unutarnjim poslovnim procesima, osobama, sustavima i vanjskim događajima može se staviti u određeni odnos s temeljnim konceptima pristupa politici informacijske sigurnosti, odnosno upravljanja informacijskom sigurnošću.

Tradicionalni pristup upravljanju informacijskom sigurnošću temelji se na propisivanju minimalnih sigurnosnih mjera, koje su utvrđene prema stupnjevima tajnosti podataka. To znači da se mjere zaštite primjenjuju na klasificirani podatak u bilo kojem obliku, odnosno na objekte (tehnologija i procesi) i subjekte (osobe) koji koriste ili pristupaju tim klasificiranim podacima. Ovakav pristup se primarno primjenjuje u okviru organizacija koje koriste klasificirane podatke (državni sektor i pravne osobe koje s njim surađuju) te podrazumijeva da je klasificirani podatak isključivi objekt zaštite, a sama metoda se primjenjuje na ljude, organizaciju (procese) i na tehnologiju, kada i ako su u doticaju s klasificiranim podacima [28]. Dakle, može se reći da definicija operativnog rizika u dobroj mjeri odgovara i riziku klasificiranih podataka u državnom sektoru, odnosno tradicionalnom pristupu u kojem se prijetnje promatra kroz skupine nezgoda, otkaza i napada.

Metode upravljanja rizicima u okviru suvremenog pristupa upravljanju informacijskom sigurnošću, temelje se na identificiranoj imovini unutar opsega sustava upravljanja informacijskom sigurnošću (ISMS), zatim na identificiranim prijetnjama za tu imovinu, identificiranim ranjivostima koje bi ove prijetnje mogle iskoristiti te na procjeni utjecaja koje gubitak povjerljivosti, cjelovitosti ili raspoloživosti može imati na imovinu. Sigurnosne kontrole (zaštitne mjere) štite identificiranu imovinu, tj. vrijednosti koje je organizacija identificirala u okviru opsega ISMS-a. I ovdje se može reći da definicija operativnog rizika odgovara metodi razvoja ISMS-a.

U osnovi, ovako definirani operativni rizici predstavljaju sveobuhvatno viđenje prijetnji, bilo

da prijetnje nastaju u okviru unutarnjih slabosti organizacije, zbog prirodnih nepogoda, ili zbog drugih, vanjskih prijetnji, te uslijed namjernog ili nenamjernog napada. Upravljanje operativnim rizikom znači balansiranje između rizika koji je povezan s nekom aktivnošću te rizika koji je povezan s neprovođenjem te aktivnosti. Nadalje, pojedinačni rizici imaju međusobnu interakciju na složen način te ublažavanje jednog rizika gotovo sigurno uvećava neki drugi. Stoga je nužna široka slika cjelokupnog poslovanja u kojem se upravlja operativnim rizikom [6].

Kao primjeri operativnog rizika mogu se navesti sljedeći karakteristični rizici:

1. Rizik informacijske sigurnosti, povezan s neovlaštenim otkrivanjem, modificiranjem ili gubitkom raspoloživosti podataka koji imaju svojstvo povjerljivosti;
2. Rizik održavanja i operativnog okruženja poslovnog objekta, povezan s upravljanjem kontinuitetom poslovanja i održavanjem IT-a;
3. Rizik sukladnosti s legislativom i regulativom, povezan s propisanim obvezama iz područja informacijske sigurnosti;
4. Rizik klimatoloških uvjeta i vremenskih nepogoda, povezan s upravljanjem kontinuitetom poslovanja.

Potrebno je napomenuti da, ovisno o primijenjenoj metodi ili internoj prosudbi pojedine organizacije, skup operativnih rizika može biti vrlo šarolik, ali se u osnovi uvijek radi o istoj skupini neprofitnih rizika, odnosno rizika koji su prijetnja za gubitke organizacije. Tako postoje detaljnije ili manje detaljne podjele operativnih rizika po vrsti, pri čemu se mogu posebno naglašavati i tretirati područja kao što su: rizik okvira upravljanja (neadekvatna infrastruktura upravljanja rizicima), reputacijski rizik institucije (javno mnijenje, mišljenje korisnika, reputacija na tržištu, …), rizik kriminalnih i nedozvoljenih radnji (sve vrste kibernetičkog kriminala, …), rizik lanca snabdijevanja (prekidi, loša usluga ili upravljanje), kulturološki rizik (neadekvatan tretman kulturoloških sadržaja koji utječu na zaposlenike kao jezik, religija, način oblačenja, …), geopolitički rizik (problemi u nekim državama zbog političke nestabilnosti, loše infrastrukture ili kulturoloških razlika), rizik ljudskog potencijala (pronalaženje, razvoj i zadržavanje zaposlenika, zaštita od seksualne i rasne netrpeljivosti). U osnovi se većina ovih prilično detaljno razrađenih rizika može podvesti pod jedan od prije istaknuta četiri rizika pa način pristupa operativnom riziku uglavnom ovisi o vrsti organizacije koja provodi upravljanje rizikom (veličina, područje djelovanja, tržište, …).

Gledano iz kuta upravljanja informacijskim sustavom, operativni rizici u svojoj bazičnoj podjeli na nezgode, otkaze i napade, odnosno općenitoj definiciji rizika od gubitka u tijeku redovnih poslovnih aktivnosti, predstavljaju temelj za različite metode koje uvode detaljniju razradu rizika, ali u okvirima definicije operativnih rizika. Slična je situacija i u upravljanju projektima koje prepoznavanje rizika usmjerava prema tipičnim elementima projektnog okruženja kao što su: rokovi, planovi, razvojno okruženje, korisnički zahtjevi i dr. U osnovi radi se o operativnim rizicima zbog kojih može doći do gubitaka kao što je gubitak uslijed kašnjenja projekta, gubitak uslijed nezadovoljavanja korisničkih zahtjeva ili propast projekta.

Kao što je već prikazano i pojašnjeno prema Sl.16., u svim ovim slučajevima, metode upravljanja rizicima koje se koriste su slične. Procjenjivanjem rizika prisutni se rizici identificiraju, analiziraju i vrednuju (prioriteti), nakon toga obradom se odabire jedan od načina obrade: izbjegavanje, smanjenje, prihvaćenje ili prijenos rizika, a uspostavom okvira za trajno upravljanje rizicima periodički se ponavlja cijeli proces.

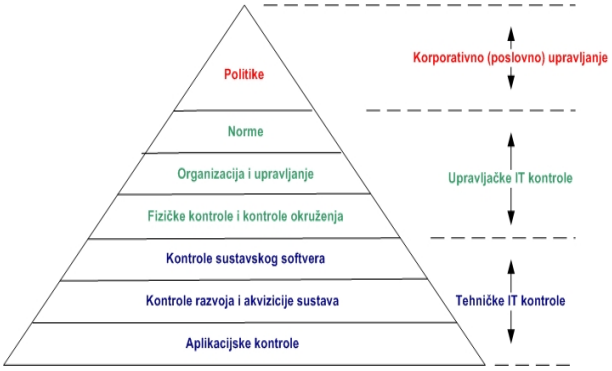
3.2. Kontrole

Kao što je već rečeno, područje upravljanja informacijskim sustavima i područje sigurnosti informacijskih sustava usko su povezana i koriste sličan pristup upravljanju rizikom, kakav se primjenjuje u nizu suvremenih, međunarodnih i nacionalnih normi informacijske sigurnosti [33] [34] [35] [36] [37] [38]. Razlog za to je veliki broj sigurnosnih prijetnji i ranjivosti povezanih sa suvremenom informacijskom i komunikacijskom tehnologijom. Upravljanje rizikom ima za cilj svesti vjerojatnost rizika primjene informacijske tehnologije u okvire prihvatljive za upravu određene organizacije. To znači, kako će vjerojatnost da neka prijetnja iskoristi ranjivost informacijskog sustava biti na odgovarajući način umanjena tako da bude u suglasju s ciljevima i načelima pristupa organizacije riziku.

Primjena sigurnosnih kontrola u području sigurnosti informacijskih sustava stoga na određeni

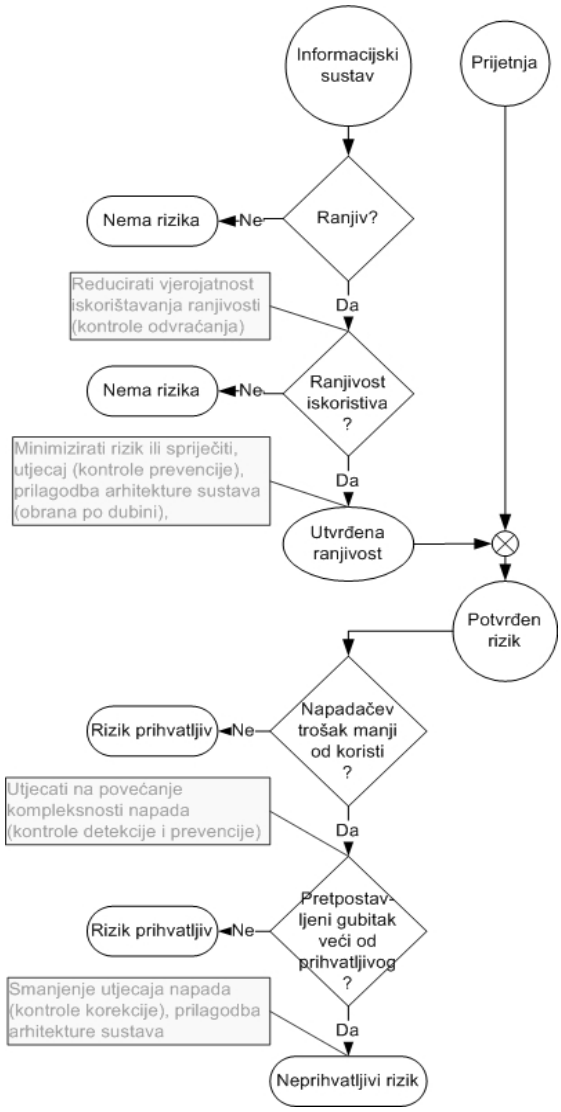
način prati dva ključna smjera upravljanja informacijskom tehnologijom. Prvi smjer pokriva životni ciklus informacijskih sustava i u okviru ovog procesa moraju se prepoznati i na odgovarajući način sigurnosno usmjeravati sve specifičnosti informacijske tehnologije koje dolaze do izražaja u različitim fazama životnog ciklusa informacijskog sustava (Tablica 2.). Drugi smjer predstavlja specifičnosti IT kontrola i općenito se može prikazati kao na Sl. 17. [39].

Prema Sl.17. može se vidjeti da ovaj model IT kontrola u stvari obuhvaća segment korporativnih upravljačkih politika (vršni dio kojemu pripadaju zakonodavne obaveze, kao i politika informacijske sigurnosti), segment upravljačkih IT kontrola (srednji dio, koji obuhvaća regulativne obaveze i općenito upravljanje tehnologijom u okruženju), i na kraju skup tehničkih kontrola koje pokrivaju problematiku uvođenja informacijskog sustava kroz razvoj ili nabavu, kao i problematiku sustavske i aplikacijske programske podrške.



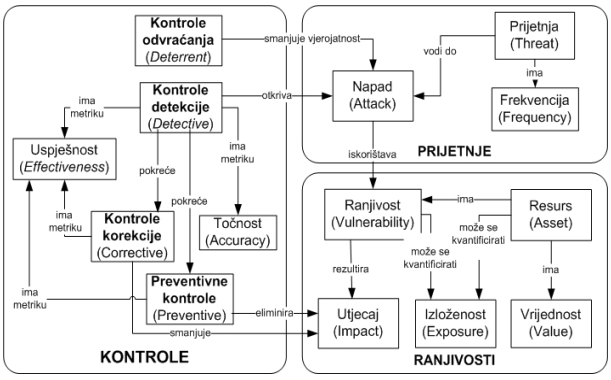
Slika 17. Slojevi u okviru kojih se realiziraju IT kontrole

Na Sl.18. prikazan je proces obrade rizika sigurnosti informacijskih sustava, na temelju kojeg se odabiru odgovarajuće sigurnosne kontrole informacijskog sustava. Sigurnosne kontrole općenito mogu biti kontrole odvraćanja (engl. *deterent*), kontrole detekcije (engl. *detection*), preventivne kontrole (engl. *prevention*) i korektivne kontrole (engl. *corrective*).



Slika 18. Obrada rizika, ključne točke u postupanju

Kao što se sa dijagrama toka na Sl.18. može vidjeti, odabir kontrola u uskoj je vezi, ne samo sa obilježjima informacijskog sustava (ranjivosti), već i sa okolinom, tj. prijetnjama. U tom smislu na Sl. 19. prikazan je logički model sigurnosnih kontrola na kojem se mogu vidjeti načini djelovanja pojedinih vrsta kontrola kao i njihova osnovna obilježja. Model je utemeljen na analizi međudjelovanja kontrola, prijetnji i ranjivosti. Na logičkom modelu naznačene su i mogućnosti uvođenja metrika za pojedine veličine koje obilježavaju prijetnje, ranjivosti i kontrole [28].

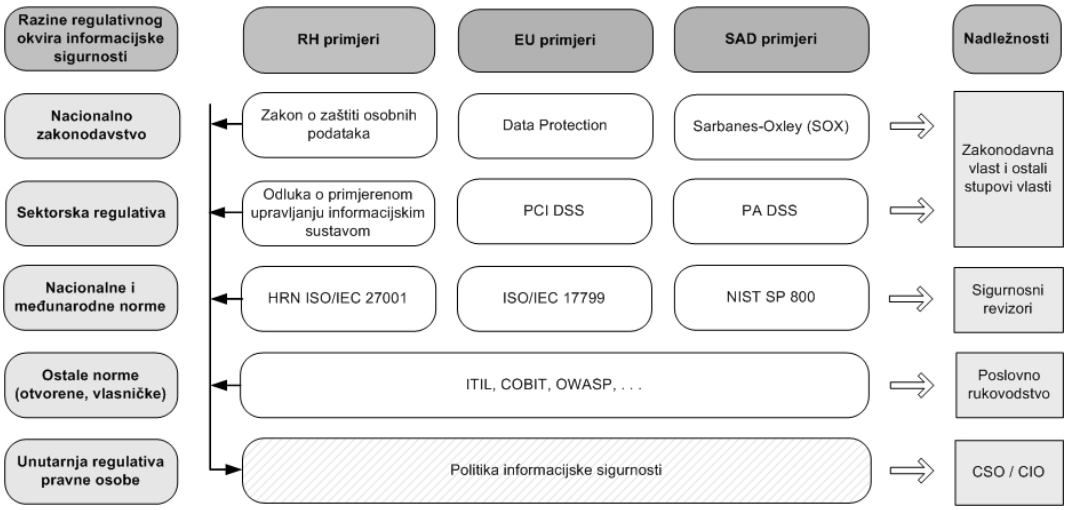


Slika 19. Logički model sigurnosnih kontrola

Opisane četiri vrste kontrola primjenjuju se za različite kategorija kontrola, a najčešće se koristi podjela na sljedeće kategorije sigurnosnih kontrola [31]:

1. tehničke kontrole (engl. *technical*);
2. upravljačke kontrole (engl. *management*);
3. operativne kontrole (engl. *operational*).

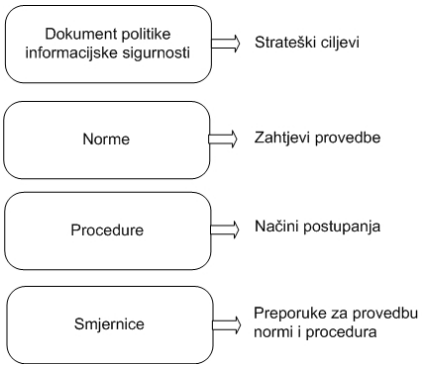
Kategorizacija sigurnosnih kontrola slična je kategorizaciji IT kontrola prikazanoj na Sl.17. Upravljačke kontrole povezane su sa donošenjem i provedbom odgovarajućih dokumenata politike informacijske sigurnosti [16]. Kako na sadržaj politike informacijske sigurnosti u nekoj organizaciji utječe čitav niz zakonskih i regulativnih obaveza (Sl. 20.), tako je i politika informacijske sigurnosti organizacije opisana kroz čitav niz dokumenata kojima se na modularan način opisuju ciljevi, zahtjevi provedbe, obvezujuće procedure, kao i smjernice za provedbu normi i procedura (Sl. 21.)



Slika 20. Utjecaj različitih razina zakonskog i regulativnog okvira informacijske sigurnosti na razvoj unutarnje politike informacijske sigurnosti pravne osobe[1]

U operativnu grupu kontrola spadaju kontrole koje se bave slabostima u operativnom radu informacijskog sustava, odnosno organizacije. Tipične su kontrole za pristup ili odlaganje medija s elektroničkim zapisima, fizička zaštita pristupa određenim prostorima u kojima se nalazi IT oprema, izrada i pohrana sigurnosnih kopija, zaštita prijenosnih računala, neprekidno napajanje, zaštita od požara, kontrola vlage i temperature, alarmi i sl. U tradicionalnoj politici informacijske sigurnosti kakva se primjenjuje u državnom sektoru [28], uobičajeno je operativne kontrole obuhvatiti dokumentom koji se naziva sigurnosne operativne procedure (engl. *Security Operating Procedures* - *SecOPs*).

[1] PCI DSS – Payment Card Industry Data Security Standard
PA DSS – Payment Application Data Security Standard
NIST – U.S. National Institute of Standards and Technology
ITIL – Information Technology Infrastructure Library
COBIT – Control Objectives for Information Technology
OWASP – Open Web Application Security Project
CSO/CIO – Chief Security/Information Officer



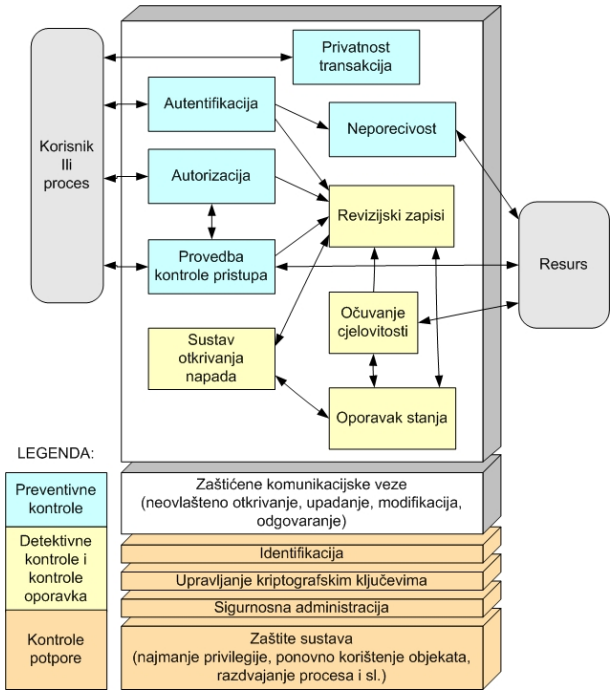
Slika 21. Hijerarhijske razine u skupu dokumenata politike informacijske sigurnosti

Za potrebe ovog rada najzanimljivije su tehničke kontrole pa ćemo malo detaljnije proanalizirati vrste tehničkih kontrola. Prema [31] tehničke kontrole mogu se podijeliti na kontrole za potporu, koje su općih obilježja i uobičajeno prisutne u potpori IT sigurnosti (npr. upravljanje kriptografskim ključevima) te su nužne za implementaciju drugih kontrola, zatim preventivne kontrole (npr. autentifikacija i autorizacija) te detektivne kontrole i kontrole oporavka (npr. detekcija i uništavanje virusa). Na Sl. 22. detaljnije je prikazan koncept tehničkih kontrola iz kojeg je vidljivo da se tu sadržajno radi o uobičajenim funkcionalnostima suvremenih informacijskih sustava. Tako prema Sl.22. razlikujemo preventivne, detektivne i korektivne tipove kontrola te kontrole potpore [39].

Gledajući iz kuta revizije koja obuhvaća i IT reviziju, odnosno fokusirana je na ispravnost i zakonitost provođenja određenih poslovnih procesa pa tako i IT podrške, vidljiva je sličnost u konceptu, bilo u odnosu na podjelu prikazanu na Sl.17., ili na drugu, često korištenu podjelu, na opće i aplikacijske kontrole.

Prema COSO definiciji [40] interna revizija (engl. *audit*) je proces koji poduzimaju uprava, rukovoditelji i drugo osoblje, kako bi u razumnoj mjeri dali jamstvo postizanja organizacijskih ciljeva kao što je učinkovitost i uspješnost operacija, pouzdanost financijskog izvještavanja i sukladnost s primjenjivim zakonodavnim i regulativnim propisima. IT kontrole okružuju sve potrebne procese koji osiguravaju informacije i informacijske usluge i pomažu smanjiti rizike povezane s korištenjem tehnologije u okviru organizacije. Stoga ove kontrole obuhvaćaju široko područje od ciljeva politike pa do primjene politike, od zaštite fizičkog pristupa do omogućavanja praćenja aktivnosti i transakcija odgovornih pojedinaca, od automatske obrade pojedinih vrsta podataka pa do mogućnosti analize velikih količina podataka.

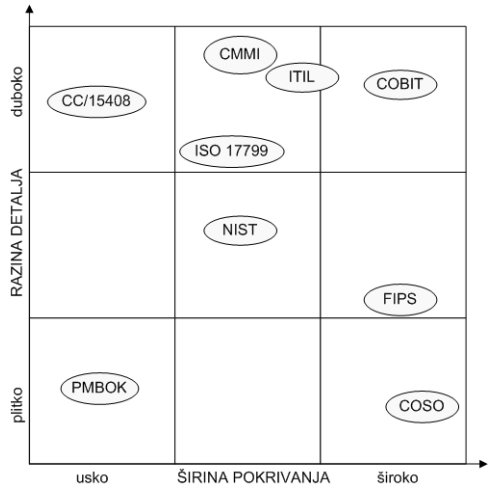
Gledajući iz kuta IT sigurnosti (Sl.22.), prema [31] cilj tehničkih sigurnosnih kontrola je osiguravanje kritičnih i osjetljivih podataka, informacija i procesnih funkcija implementiranih u okviru IT sustava. S obzirom na izniman razvoj informacijske i komunikacijske tehnologije u posljednja dva desetljeća, aktualnu transformaciju tradicionalnog - tržišnog društva, temeljenog na privatnom vlasništvu, u suvremeno - informacijsko društvo, temeljeno na znanju – informacijama, s obzirom na otvorenost i međupovezanost informacijskih sustava danas, ovisnost poslovnih procesa i društva o informacijskoj tehnologiji i znanju organiziranom u okviru suvremenih informacijskih usluga, te na prijetnje i ranjivosti suvremenog informacijskog prostora, može se reći da je u projektiranju informacijskih sustava sve manje razlika između funkcionalno usmjerenog i sigurnosno usmjerenog pristupa, odnosno da funkcioniranje informacijskih sustava nije prihvatljivo bez sigurnosnih elemenata, kao što sigurnost nema smisla bez funkcionalnih elemenata.



Slika 22. Tehničke sigurnosne kontrole

Danas je moguće korištenje različitih normi kako bi se postiglo odgovarajuće upravljanje informacijskim sustavima. U tom smislu neke

norme su više usmjerene na područje upravljanja informacijskom tehnologijom (npr. COBIT), druge na područje upravljanja informacijskim uslugama (npr. ITIL), a treće na područje upravljanja sigurnošću informacijskih sustava (npr. NIST SP 800, ISO/IEC 27001/02). Jedan način usporedbe ovih normi moguće je prikazati prema Sl.23., gdje je na apscisi prikazana širina pokrivanja, odnosno sveobuhvatnost norme, dok je na ordinati prikazana razina detalja dokumentacije prikazanih normi, u tehničkom i operativnom smislu. Prikaz je napravljen relativno u odnosu na normu za poslovno upravljanje informacijskom tehnologijom COBIT (engl. *Control OBjectives for Information and related Technology – COBIT*) [41].



Slika 23. Usporedba u radu spominjanih normi u području informacijskih sustava u odnosu na COBIT

3.3. Metrika

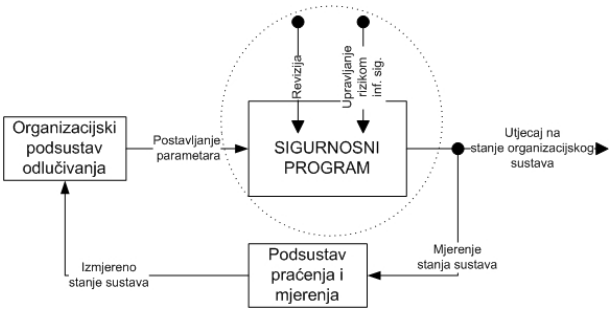
Tradicionalni pristup upravljanju informacijskom sigurnošću primjenom minimalnih sigurnosnih procedura (engl. *baseline procedures*), nastao je i uspješno se mogao primjenjivati u zatvorenim informacijskim okruženjima s jasno profiliranim i simetričnim prijetnjama. Suvremene norme poput ISO/IEC 27001 daju široke okvire za razvoj programa informacijske sigurnosti u različitim institucijama i sektorima. Norma ISO/IEC 27001, za razliku od minimalnih sigurnosnih procedura koje predstavljaju statički pristup mjerama zaštite (fiksno utvrđen i „neovisan“ o okolini), koristi procjenu rizika i dinamički pristup sigurnosnoj okolini u kojoj se ISMS ostvaruje, u skladu s provedenom procjenom rizika u konkretnom sigurnosnom okruženju. Zahtjevi korporativnog upravljanja i usklađivanja poslovnih ciljeva sa sigurnosnim programima traže daljnji iskorak u metodama, prvenstveno u smjeru sustavnog mjerenja parametara na taktičkoj i osobito strateškoj razini, a koji su bitni za upravljanje informacijskom sigurnošću, ali gledano s aspekta upravljanja poslovnim sustavom [28].

Metrika je općenito sustav ili postupak mjerenja, pri čemu su očekivana svojstva takvog mjerenja konzistentnost, lakoća prikupljanja podataka, kvantitativno izražavanje i korištenje jedinica mjere [42]. Sigurnosna metrika, podrazumijeva analizu i interpretaciju podataka dobivenih mjerenjima, iz koje je moguće zaključiti koje je akcije potrebno poduzeti u cilju uklanjanja sigurnosnog rizika i poboljšanja cjelokupnog stanja sigurnosti [43].

Zahtjevi za mjerenjem danas dolaze iz različitih izvora, najčešće iz zakonodavno-regulatornih, kao što je to već spomenuto vezano za poslove revizije u poglavlju 3.2 Kontrole. Sve veća potreba za upravljanjem različitim procesima, također postavlja zahtjeve na odgovarajuće mjerenje veličina na temelju kojih se upravlja procesima. U području informacijske sigurnosti, tradicionalni pristup upravljanju informacijskom sigurnošću, jednako kao i suvremeni, ne obraćaju dovoljnu pažnju na mjerenje. U većini organizacija jedini načini prikupljanja podataka o stanju sigurnosti jesu kroz proces upravljanja rizikom ili kroz neku vrstu revizije. Pri tome usmjerenost upravljanja rizikom nije na performansama ili strateškom povezivanju sigurnosti s poslovnim ciljevima, već na identificiranju rizika informacijske imovine i na razvoju sigurnosnih kontrola. Ovdje se najčešće radi o operativnoj razini podataka, ponekad taktičkoj, a vrlo rijetko strateškoj razini u smislu poslovnog upravljanja. Dodatni problem predstavlja subjektivnost procjene u metodama upravljanja rizikom. S druge strane, revizija osigurava najvećim dijelom „povijesne“ podatke o usklađenosti sa zahtijevanom normom pa teško može služiti za strateško upravljanje, odnosno za procjenu trendova značajnih za upravljanje određenim procesom [49].

Gledano iz kuta procesa kojim se upravlja, i praćenje (engl. *monitoring*) i mjerenje, mogu biti upotrebljivi za upravljanje informacijskom sigurnošću [6]. Cilj je dobivanje potrebnih mjerenih veličina o stanju sigurnosti, a u svrhu donošenja odluka o usmjeravanju sigurnosnog programa (strateška razina) ili njegovom

upravljanju (taktičko-operativna razina), sukladno Sl.24.



Slika 24. Korporativno upravljanje informacijskom sigurnošću

Slično kao i u mnogim drugim znanstvenim područjima, IT metrika općenito, a posebno sigurnosna IT metrika, područje je koje je u nastajanju i u velikoj mjeri se i dalje oslanja na kvalitativne usporedbe pojedinih veličina. U praksi je još uvijek uobičajena primjena metoda u okviru kojih se subjektivno procjenjuje određena stanja ili veličine. Primjer je penetracijsko ispitivanje koje traži specijalizirana znanja osoblja koje ga provodi te na temelju dobivenih rezultata procjenjuje stanje sigurnosti u nekoj organizaciji. Ovakve metode ili mjerenja koja uključuju specijalizirane vještine u osnovi nisu ponovljive već se oslanjaju na znanje, talent i iskustvo procjenitelja te su subjektivni rezultati očekivani [44]. Upravo područje upravljanja rizicima najpodložnije je ovim slabostima subjektivnog procjenjivanja [28].

Metrike možemo podijeliti na više načina, kao što je podjela po tome što mjere (proces, performanse, rezultate, kvalitetu, trendove, uskladivost, …), ili po tome kako mjere (metode zrelosti, uravnotežene kartice postignuća, vrednovanje, statistička analiza, …), odnosno na temelju izmjerenih vrijednosti kao kvantitativne, kvalitativne i hibridne metode [45]. Jedna od tipičnih metrika performansi su ključni indikatori ciljeva (engl. *Key Goal Indicator - KGI*) i ključni indikatori procesa (engl. *Key Process Indicator - KPI*), koji se općenito koriste za praćenje ostvarenja ciljeva (strateško praćenje), odnosno za praćenje djelotvornosti različitih procesnih aktivnosti u poslovnom ili sigurnosnom segmentu. Često puta je ove indikatore teško svrstati u upravljanje organizacijom ili projektom, odnosno upravljanje sigurnošću, kao što je to slučaj za poslovni cilj održavanja tržišnog ugleda, pri čemu je ključni indikator cilja broj incidenata koji narušavaju tržišni ugled. Takav indikator cilja može se tretirati i kao poslovni, strateški indikator, ali i kao sigurnosni indikator, a predstavlja primjer poveznice strateške (poslovne) i taktičke (sigurnosne) razine prema Sl.24. Prema [47] temeljna obilježja metrike moguće je opisati odgovorima na pitanja sa Sl.25., čime se može provesti i kategorizacija različitih metrika. Uobičajena podjela metrika tako je prema [48] na tehničku (tehnički objekti – algoritmi, uređaji, projekti, …), organizacijsku (procesi i programi) i operativnu kategoriju metrika (opisuje kakvi su sustavi, operativne prakse i specifična okruženja).

Slika 25. Obilježja sustavskih metrika

Iako je područje metrike u sustavskom inženjerstvu, kao i u sigurnosnom inženjerstvu, već dosta dugo prisutno, ova grana razvoja još je uvijek dosta nerazvijena i postoji dosta nejasnoća i nerazumijevanja u korištenju pojmova metrike, mjerenja ili indikatora. Suštinski razlog leži u obilježjima discipline sustavskog inženjerstva, koju za razliku od primjerice fizikalnih zakona, nije moguće tako strogo matematički opisati te samim time nije moguće postići jednostavnu dokazivost ispravnosti određene mjerne tehnike. Tehnike estimacije ili procjenjivanja budućeg ponašanja ili trendova, do određene mjere se oslanjaju na povijesno praćenje pojedinih odabranih veličina, pri čemu povijesno i buduće ima korelaciju koja je poznata ili se može utvrditi. U sigurnosnom, sustavskom i programskom inženjerstvu to ne mora biti točno. Primjerice, podaci o tome da je neka strategija zaštite dobro služila organizaciji u prošlosti, govore vrlo malo o snazi i mogućnostima primjene te strategije u budućnosti, jer je potrebno promatrati sustav u okruženju koje se može potpuno promijeniti [47] [48].

4. Zaključak

Upravljanje informacijskim sustavom i upravljanje sigurnošću informacijskog sustava uobičajeno se promatra u okviru životnog ciklusa informacijskog sustava te ih je nužno promatrati integrirano.

Gledano iz kuta projekta razvoja ili uvođenja informacijskog sustava, sigurnost također nije moguće promatrati izdvojeno kao dodatnu funkcionalnost, već su sigurnosni elementi integralni dio arhitekture informacijskog sustava. U tom smislu niti arhitekturu informacijskog sustava nema smisla promatrati kao isključivo funkcionalnu ili isključivo sigurnosnu, već to mogu biti samo kutovi gledanja na sveobuhvatni model arhitekture informacijskog sustava, koji ovise o interesima korisnika ili drugih zainteresiranih strana.

Skup sigurnosnih mjera koji je optimalan za određenu organizaciju i njen informacijski sustav, ovisi o sigurnosnim ciljevima, tehničkim, organizacijskim i operativnim potrebama te financijskim, ljudskim i tehničkim potencijalima koji su raspoloživi. Svi ovi faktori predstavljaju parametre koji jednako tako utječu i na projektiranje i upravljanje informacijskim sustavom, ali i na poslovne ciljeve organizacije u širem smislu. U tom smislu i koncept upravljanja rizikom, bilo iz kuta informacijske sigurnosti ili informacijske tehnologije, odnosno sustavskog inženjerstva, uglavnom počiva na zajedničkom konceptu operativnih rizika i u konačnici sličnoj metodi pristupa upravljanju rizicima.

Sigurnosne mjere u suvremenim informacijskim sustavima, predstavljaju u velikoj mjeri podskup discipline sustavskog inženjerstva, a slijedom razvoja informacijske i komunikacijske tehnologije, u velikoj mjeri su povezane i sa programskim inženjerstvom.

Literatura

[1] Fertalj, K., *Upravljanje informacijskim sustavima, predavanja šk.g. 2007/08*, FER, Zagreb

[2] Pressman, R.S., *Software Engineering, A Practitioner's Approach*, 3rd Ed., 1994, McGraw-Hill

[3] Peltier, T.R., *Information Security Risk Analysis*, 2nd Ed., 2005, Auerbach Publications

[4] HRN ISO/IEC 27001:2005, HRN ISO/IEC 17799:2005

[5] National Institute of Standards and Technology (NIST), *Risk Management Guide for Information Technology Systems, SP 800-30*, July 2002

[6] Sherwood, J., Clark, A., Lynas, D., *Enterprise Security Architecture*, CMP Books, 2005

[7] Anderson, R., *Security Engineering*, John Willey & Sons, Inc., 2001

[8] Avison, D.E., Fitzgerald, G., *Information Systems Development: Methodogies, Techniques and Tolls*, The McGraw-Hill Companies, University Press, Cambridge, 1998

[9] Moxley, F.I., Simon, L., Wells, E.J., *Laying the Foundation for Coalition Interoperability through NATO's C3 Technical Architecture*, 2000 http://handle.dtic.mil/100.2/ADA461323

[10] Buckman, T., NATO Network Enabled Capability, Feasibility Study, V2.0, 2005, antigo.mdn.gov.pt/.../NNEC%20FS%20Executive%20Summary_2.0__NU_.pdf

[11] Harris, S., CISSP, All-in-One, 3rd Ed., 2005, McGraw-Hill/Osborne

[12] National Institute of Standards and Technology (NIST), *Information Security, Security Consideration in the System Life Cycle, SP 800-64 Rev 2*, October 2008

[13] Department of Defence, *Global Information Grid, Architectural Vision*, June 2007, V1.0, DoD CIO, http://cio-nii.defense.gov/docs/GIGArchVision.pdf

[14] Farah, G., *Information System Security Architecture*, SANS Institute, September 2004, www.sans.org/.../information-systems-security-architecture-approach-layered-protection_1532

[15] Network Applications Consortium (NAC), *Enterprise Security Architecture, a Framework and Template for Policy Driven Security*, 2004

[16] Klaić, A., Perešin, A., *Koncept regulativnog okvira informacijske sigurnosti*, Međunarodne studije, časopis za međunarodne odnose, vanjsku politiku i diplomaciju (u postupku objave), siječanj 2010.

[17] Aagedal, J.O., *Summary of IEEE 1471*, heim.ifi.uio.no/~mmo/generic/papers/IEEE.pdf

[18] Ellis, W. J., Hilliard, R. F., Poon, P. T., *Toward a Recomended Practice for Architectural Description*, In Proceedings 2nd IEEE International Conference on Engineering of Complex Computer Systems, Montreal, Quebec, Canada, October 21–25, 1996

[19] Perešin, A., Klaić, A., *Zaštita klasificiranih podataka u okviru nacionalne kritične infrastrukture*, Konferencija o zaštiti i spašavanju, Vlada RH i DUZS, studeni 2009., Zagreb, zbornik DUZS, str. 60-64

[20] Wilkes, J., Mogul, J., Suermondt, J., *Utilification*, Proceedings of the 11th ACM SIGOPS European Workshop, 19–22 September 2004, Leuven, Belgium, www.e-wilkes.com/john/papers/Utilification-final.pdf

[21] Gerić, S., *Security of Web Services based on Service-oriented Architectures*, MIPRO 2010/ISS, Opatija 2010, Proceedings Vol. V., p. 208-213

[22] Erl, T., *Service-Oriented Architecture, Concepts, Technology, and Design*, Prentice Hall, December 2005

[23] Systems Security Engineering Capability Maturity Model, www.sse-cmm.org

[24] Software Engineering Institute, Capability Maturity Model, www.sei.cmu.edu

[25] International System Security Engineering Association (ISSEA), www.issea.org

[26] Cabinet Office and CESG, *HMG Information Assurance Maturity Model and Assesment Framework*, 27 May 2010, www.cesg.gov.uk

[27] Cabinet Office, *HMG Security Policy Framework*, December 2008, www.cabinetoffice.gov.uk

[28] Klaić, A., Pregled stanja i trendova u suvremenoj politici informacijske sigurnosti i metodama upravljanja informacijskom sigurnošću, FER, travanj 2010., kvalifikacijski doktorski ispit, www.fer.hr

[29] Standards Australia and Standards New Zealand, *AS/NZS 4360:2004, Risk Management*

[30] National Institute of Standards and Technology, *Managing Risk from Information Systems, An Organizational Perspective*, April 2008, NIST SP 800-39 (2nd Public Draft)

[31] National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, July 2002, NIST SP 800-30

[32] Hrvatska narodna banka - HNB, http://www.hnb.hr/propisi/hpropisi.htm

[33] HM Treasury, *The Orange Book – Management of Risk – Principles and Concepts*, UK, October 2004, www.hm-treasury.gov.uk

[34] Standards Australia and Standards New Zealand, *AS/NZS 4360:2004, Risk Management*

[35] National Institute of Standards and Technology, *Managing Risk from Information Systems, An Organizational Perspective*, April 2008, NIST SP 800-39 (2nd Public Draft)

[36] HRN ISO/IEC 27001:2005, HRN ISO/IEC 17799:2005, www.hzn.hr, www.iso.org

[37] BS 7799-3:2006, *Information Security Management System, Guidelines for information security risk management*

[38] National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, July 2002, NIST SP 800-30

[39] GTAG, *Information Technology Controls*, The Institute of Internal Auditors (IAA), USA, 2005, www.theiaa.org

[40] Committee of Sponsoring Organisations for the Commission on Fraudulent Financial Reporting (The Committee of Sponsoring Organizations Treadway Commission), www.coso.org

[41] IT Governance Institut, COBIT Mapping, Overview of International IT Guidance, 2nd Edition, 2006, www.isaca.org

[42] Jaquith, A., *Security Metrics*, Addison-Wesley, 2007

[43] CARNet CERT, LS&S, *Sigurnosna metrika*, CCERT-PUBDOC-2008-07-235, 2008.

[44] Jansen, W., *Directions in Security Metrics Research*, National Institut of Standards and Technology, NIST, NISTIR 7564, April 2009

[45] Brotby, W. Krag, Information Security Management Metrics, CRC Press, Auerbach, 2009

[46] Sajko, M., *Mjerenje i vrednovanje učinkovitosti informacijske sigurnosti*, FER, svibanj 2010., kvalifikacijski doktorski ispit, www.fer.hr

[47] Vaughn, R.B., Henning, R., Siraj, A., *Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy*, Preceedings oft he 36th Hawaii International Conference on System Sciences, IEEE Computer Society, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.4446&rep=rep1&type=pdf

[48] Proceedings from the *Workshop on Information Security System Scoring and Ranking*, May 2001, Williamsburg, Virginia, The MITRE Corporation, 2002

[49] Klaić A., Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies, MIPRO 2010/ISS, p.136-141, Opatija, 2010