HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Upravljanje sigurnošću informacijskih sustava prema BS7799 standardu

CCERT-PUBDOC-2003-12-55

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

**CARNet CERT**, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

**LS&S**, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

Standard BS 7799 opisuje proces uvođenja sustava upravljanja sigurnošću informacija, "Information Security Management System (ISMS)". Takav proces pruža sistematski pristup upravljanju osjetljivim informacijama s ciljem očuvanja njihove sigurnosti. Cilj procesa je postići sigurnost informacija u tri glavna aspekta: povjerljivost, integritet i dostupnost, uključivši pritom relevantne organizacijske resurse organizacijske politike, procedure i informacijske sustave. Ovaj dokument opisuje ciklus uvođenja sustava upravljanja sigurnošću informacija u skladu sa sigurnosnim i poslovnim zahtjevima pojedine organizacije. U dokumentu su analizirane prednosti i nedostaci uvođenja takvog sustava, kao i problemi koji se javljaju prilikom izvođenja procjene rizika kao sastavnog dijela uvođenja sustava upravljanja sigurnošću informacija.

# 2. Informacijska tehnologija i BS 7799 standard

Protok velikih količina informacija među informacijskim sustavima pridonosi formiranju "društva bez granica", ali istovremeno otvaraju informacijske sustave zlonamjernim napadima neovlaštenih korisnika. Napadači prodiru u informacijske sustave uzrokujući velike štete cjelokupnom poslovanju organizacije. Unutar samih organizacija, zaposlenici su putem svojih računala spojeni direktno na Internet, što otvara mogućnosti namjernih i nenamjernih otkrivanja povjerljivih podataka kao i otvaranja potencijalnih sigurnosnih ranjivosti sustava. Uzrok tome je često neupućenost, nedovoljna obrazovanost o problemima sigurnosti informacijskih sustava, ili jednostavno nepažnja.

Brzim razvojem informacijskih tehnologija okruženje informacijskih sustava se u velikoj mjeri mijenja. Upotrebom operacijskih sustava opće namjene i distribuiranog procesiranja, te proširenjem izvora pristupa sustavu dodatno se povećavaju i izvori potencijalnih ranjivosti sustava. Kao rezultat ovih pojava, organizacije prepoznaju potrebu za implementiranjem i dokumentiranjem sustava upravljanja sigurnošću informacija.

Sustav upravljanja sigurnošću informacija može se jednostavno protumačiti kao sigurnosna mjera kojom se smanjuju mogućnosti napadača, bilo vanjskog ili unutarnjeg. Sustav upravljanja sigurnošću informacija je isto tako i sredstvo pomoću kojeg više poslovodstvo organizacije prati i nadzire sigurnost informacijskih sustava organizacije, svodeći poslovni rizik na minimum i osiguravajući da sigurnosni zahtjevi poslovanja ispunjavaju korporacijske, kupčeve i pravne obveze.

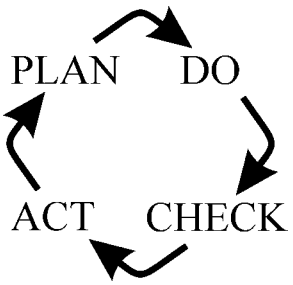
Sustav upravljanja sigurnošću informacija kao integrirani sustav upravljanja kvalitetom opisan je u drugom dijelu britanskog standarda BS 7799. Prvi dio standarda, poznatiji pod imenom ISO 17799, predstavlja široki spektar smjernica za implementaciju sigurnosnih kontrola, te pokriva sigurnosne politike, pravne, organizacijske, fizičke i ljudske komponente informacijskih sustava. Drugi dio standarda predstavlja specifikaciju s postupcima korištenja i implementiranja sustava upravljanja sigurnošću informacija, dajući pri tome upute što je sve potrebno napraviti kako bi se uspostavila prihvatljiva razina informacijske sigurnosti unutar organizacije. Implementacija sustava upravljanja sigurnošću informacija vrlo je specifična za svaku organizaciju i ovisi o organizacijskim karakteristikama i specifičnim poslovnim zahtjevima.

# 3. Implementacija sustava upravljanja sigurnošću informacija

Implementacija sustava upravljanja sigurnošću informacija temelji se na "Plan-Do-Check-Act" (PDCA) ciklusu. Faze implementacije osnovane na ovom modelu su sljedeće:

- "Plan" – planiranje i uspostava sustava,
- "Do" – upotreba sustava,
- "Check" – praćenje i revizija sustava,
- "Act" – poboljšanje sustava.

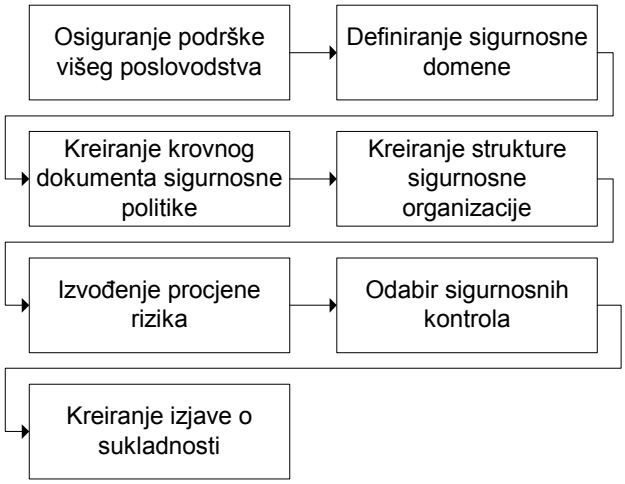
Ovaj model ističe važnost pažljivog planiranja programa uspostave sustava, što rezultira efikasnim mjerama za njegovo trajno poboljšanje i pravilnu upotrebu. Simbolički je model prikazan na Slici 1.




**Slika 1:** PDCA ciklus

## 3.1. "Plan" faza PDCA ciklusa

Planiranje implementacije sustava upravljanja sigurnošću informacija uključuje definiciju poslovne politike organizacije i njenih ciljeva u smislu zahtjeva na sigurnost informacija, procjenu opsega sustava upravljanja sigurnošću, odlučivanje i skupljanje resursa za izvedbu procjene rizika, te definiranje pristupa kontinuiranom analiziranju i procjeni rizika. Ovaj proces prikazan je Slikom 2.

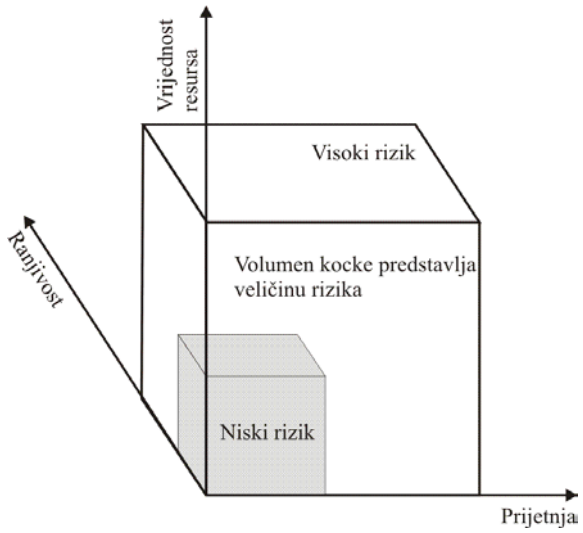



**Slika 2:** "Plan" faza PDCA ciklusa

1. Podrška višeg poslovodstva
   Prije implementacije bilo kojeg efikasnog sustava upravljanja kvalitetom, najvažnije je da više poslovodstvo u potpunosti razumije koristi uvođenja sustava te podržava njegovo uvođenje, svjesno mogućih problema i prepreka koje se mogu pojaviti. Sigurnost, kao i sve druge interne kontrole, potaknuta je od vrha organizacije. Kako bi se uspješno ispunili ciljevi i zahtjevi informacijske sigurnosti, važno je da izvršno tijelo organizacije preuzme inicijativu u promicanju informacijske sigurnosti, te pruži punu potporu timu ili vanjskim suradnicima koji će provoditi proces.
2. Definiranje sigurnosne domene
   Drugi korak je definiranje područja koje će pokrivati implementirani sustav upravljanja sigurnošću informacija. To može biti područje cijelog informacijskog sustava organizacije, ili samo jedan njegov dio. Također, sustav može pokrivati samo jednu specifičnu uslugu – npr. Internet bankarstvo. Područje opsega sustava upravljanja sigurnošću informacija pokriva sve one domene za koje organizacija smatra da trebaju adekvatnu informacijsku zaštitu.
3. Kreiranje krovnog dokumenta sigurnosne politike
   Krovni dokument sigurnosne politike je relativno kratak dokument (1-3 stranice), potpisan od strane izvršnog tijela organizacije, te prezentiran svim zaposlenicima. Namjena dokumenta je iskazivanje potpune potpore poslovodstva uvođenju sustava upravljanja sigurnošću informacija. Dokumentom se nedvojbeno izražava politika organizacije da će osigurati tajnost informacija, štititi njihov integritet, te osiguravati njihovu dostupnost samo autoriziranim korisnicima. Svi

drugi relevantni dokumenti, pravne i zakonske odredbe od specifične važnosti za organizaciju, kao i ostali dokumenti sigurnosne politike namijenjene određenim aspektima informacijskog sustava, trebaju biti navedeni u krovnom dokumentu sigurnosne politike.

4. Kreiranje strukture sigurnosne organizacije
   Organizacija mora uspostaviti upravljačku strukturu za provedbu mjera i strategija sustava upravljanja sigurnošću informacija. Struktura se brine za provedbu, kreiranje i održavanje ažurnosti sigurnosnih politika, kao i relevantnih standarda, procedura i planova. Struktura se sastoji od različitih tijela i timova zaduženih za specifične sigurnosne aspekte.
   Konačnu odgovornost za provedbu sigurnosnih mjera preuzima glavni službenik za informacijsku sigurnost. Njegove odgovornosti i ovlaštenja moraju biti jasno definirane, kao i odgovornosti i ovlaštenja svakog zaposlenika u upravljačkoj strukturi za sigurnost informacija. Na taj način postiže se adekvatna provedba sigurnosnih mjera unutar organizacije.
5. Izvođenje procjene rizika
   Kako bi se donijela odluka o tome koje je informacijske resurse potrebno zaštititi, nužno je provesti detaljnu analizu organizacije u cilju utvrđivanje lokacije, načina postupanja i odgovornosti za pojedine informacijske resurse. Informacijski resursi svakog dijela organizacije trebaju se klasificirati unutar aspekata tajnosti, integriteta i dostupnosti. Procjena veličine rizika za pojedini resurs može se predočiti pomoću kocke ilustrirane u prijetnja-resurs-ranjivost sustavu, kao što je prikazano na Slici 3.

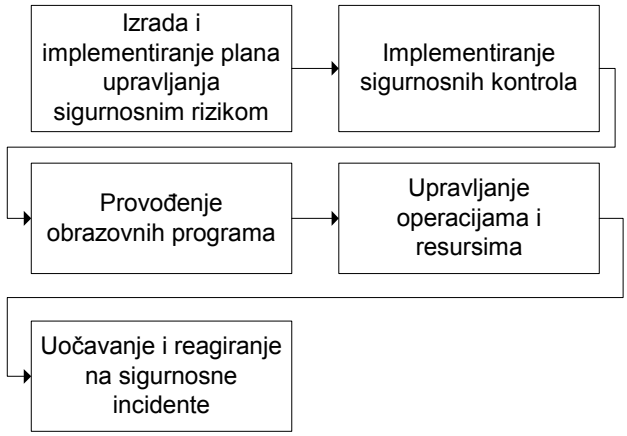



**Slika 3:** Procjena veličine rizika

6. Odabir sigurnosnih kontrola
   Drugi dio BS 7799 standarda sadrži 127 sigurnosnih kontrola. Podrazumijeva se da nisu sve kontrole primjenjive na sve organizacije. Preporučuje se upotreba samo onih kontrola koje su u procesu analize rizika identificirane kao nužne za primjenu. Nakon odabira sigurnosnih kontrola, specifične sigurnosne politike definiraju se za svaku pojedinu kontrolu, kako bi se osigurala željena razina sigurnosti. Preporuke i procedure za implementaciju sigurnosnih politika specificiraju se u posebnoj dokumentaciji o implementaciji sigurnosne politike, te se sama implementacija mjera definiranih politikama provodi u "Act" fazi PDCA ciklusa.
7. Kreiranje izjave o sukladnosti
   Drugi dio BS 7799 standarda zahtijeva postojanje dokumenta zvanog "Izjava o sukladnosti" (engl. **S**tatement **O**f **A**pplicability, SOA), koji sadrži popis sigurnosnih kontrola s objašnjenjima zašto su pojedine kontrole uključene odnosno isključene iz sustava. Standard podrazumijeva da je opseg sustava upravljanja sigurnošću informacija specifičan za svaku pojedinu organizaciju i samim tim je opravdano isključivanje pojedinih kontrola iz sustava.

## 3.2. "Do" faza PDCA ciklusa

Pri implementaciji sustava upravljanja sigurnošću informacija nužno je fokusirati se na potrebu za dugoročnim i ispravnim mehanizmom održavanja funkcionalnosti sustava. Ovaj mehanizam može biti izveden i automatiziranim i ručnim procesima. Idealno rješenje je pronalaženje ravnoteže u uključivanju oba procesa. Izvođenje tih procesa provodi se u "Do" fazi implementacije sustava upravljanja sigurnošću informacija, prikazanoj na Slici 4.




**Slika 4:** "Do" faza PDCA ciklusa

1. Izrada i implementiranje plana upravljanja sigurnosnim rizikom
   Plan upravljanja sigurnosnim rizikom je projektni plan kojim se uključuju eventualne dodatne sigurnosne kontrole u sustav upravljanja sigurnošću informacija ukoliko se za tim otkrije potreba prilikom izvođenja procjene rizika. Uslijed promjene informacijskih resursa ili promjene veličine rizika za pojedine informacijske resurse, potrebno je ponovno provesti postupak procjene rizika te revidirati i ažurirati sigurnosnu politiku za relevantne sigurnosne kontrole. Pri formulaciji mjera za postizanje željene razine sigurnosti, formulira se plan za upravljanje sigurnosnim rizikom tako da se veličina rizika nastoji svesti na minimalan iznos.
   Svi zapisi o provedenoj analizi sigurnosnih rizika moraju se strogo kontrolirano nadzirati i čuvati na točno određenim lokacijama i unutar definiranih odgovornosti, jer ti dokumenti sadrže osjetljive informacije o ranjivosti sustava i samim tim su vrlo interesantni potencijalnim napadačima unutar i izvan organizacije.
2. Implementiranje sigurnosnih kontrola
   Dok se definiranjem sigurnosnih politika za odabrane sigurnosne kontrole opisuje koje mjere bi trebalo poduzeti za postizanje i održavanje željene razine sigurnosti, njihova implementacija podrazumijeva specifikaciju kako je potrebno implementirati definirane sigurnosne mjere opisane dokumentima sigurnosne politike. Nužno je redovito provjeravati sigurnosne politike i metode njihove implementacije, kako bi se na vrijeme odredila optimalna metoda suočavanja s novim sigurnosnim prijetnjama. Budući da su sposobnosti napadača sve sofisticiranije i štete koje mogu nastati njihovim djelovanjem sve veće, važno je često provjeravati i ažurirati sigurnosne politike i metode njihove implementacije.
3. Provođenje obrazovnih programa
   Dio implementacije sustava upravljanja sigurnošću informacija može se realizirati automatski putem tehničkih procedura ugrađenih u informacijski sustav. Međutim, veći dio implementacije ovisi o odlukama i aktivnostima ovlaštenih osoba kao i svih korisnika informacijskog sustava organizacije. Kako bi se podigla svijest o važnosti pridržavanja sigurnosnih mjera implementiranih kroz sustav upravljanja sigurnošću informacija, važno je provoditi odgovarajuću i planiranu izobrazbu zaposlenika o važnosti sigurnosti, te pridržavanju sigurnosnih politika i procedura.
4. Upravljanje operacijama i resursima
   Kako bi se upravljanje operacijama i resursima sustava upravljanja sigurnošću informacija pravilno i efikasno provodilo, važno je uspostaviti takav tip sigurnosne organizacije koji se ne

oslanja pretjerano na pojedinačne zaposlenike. Također, nužno je uspostaviti sustav brzog reagiranja na incidente kako bi se osigurao kontinuirani rad informacijskog sustava i poslovanja organizacije.

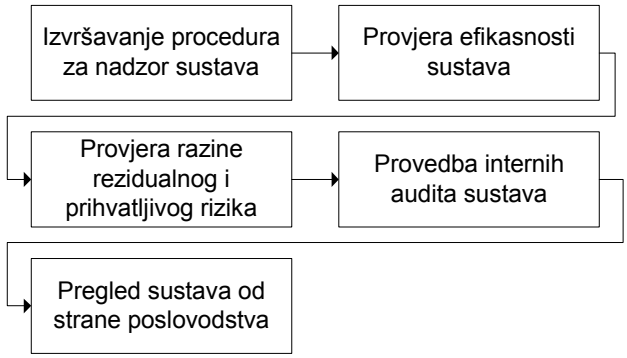
Svaki novi informacijski resurs treba biti provjeren i testiran prije uključivanja u informacijski sustav. Specifikacije resursa moraju se nadzirano pohranjivati i kontrolirati. Ukoliko je određeni uređaj uništen ili je na njemu izveden popravak, odgovarajuća procedura treba se provoditi pri rukovanju uređajem s ciljem sprečavanja otkrivanja osjetljivih informacija zlonamjernim korisnicima.

5. Uočavanje i reagiranje na sigurnosne incidente

   Svaki zaposlenik dužan je o uočenom sigurnosnom incidentu izvijestiti osobu nadležnu za provedbu sigurnosnih mjera, bez pokušaja samostalnog rješavanja incidenta. Za rješavanje sigurnosnih incidenata potrebno je kreirati posebnu proceduru i slijediti metode i odgovornosti definirane procedurom. Također je prilikom rješavanja sigurnosnih incidenata nužno proizvesti izvještaj o riješenim sigurnosnim incidentima. Na taj način postiže se kontrolirano i efikasno reagiranje na incidente i sprečavanje nastajanja još većih indirektnih šteta uzrokovanih nespretnim rukovanjem incidentima.

## 3.3. "Check" faza PDCA ciklusa

Implementacija ove faze podrazumijeva kontinuirano praćenje efikasnosti sustava upravljanja sigurnošću informacija s perspektive zadovoljavanja poslovnih potreba organizacije i njegove praktične upotrebe i provedbe unutar organizacije. Ovaj proces prikazan je Slikom 5.




**Slika 5:** "Check" faza PDCA ciklusa

1. Izvršavanje procedura za nadzor sustava

   Osiguranje željene razine sigurnosti informacijskog sustava održava se primjenom pravila i procedura za nadzor sustava upravljanja sigurnošću informacija.

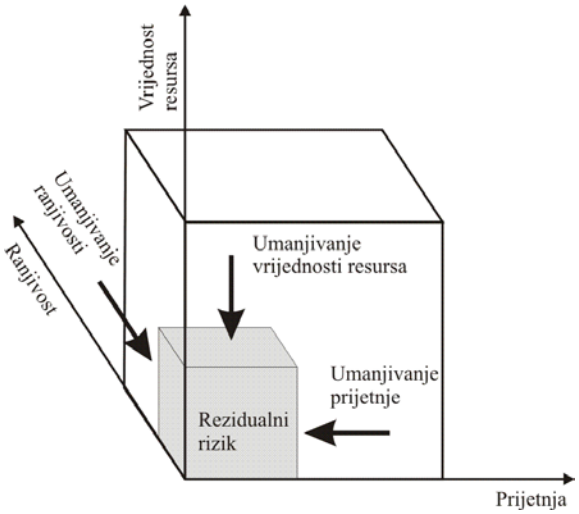
   Budući da se nove sigurnosne prijetnje otkrivaju na dnevnoj bazi, nužno je pratiti izvore informacija o sigurnosnim prijetnjama i redovito ažurirati sigurnosne mehanizme za sprečavanje tih prijetnji. Izvori takvih informacija obično su organizacije namijenjene upravo pravodobnom informiranju zainteresiranih o novim sigurnosnim prijetnjama i analiziranju postojećih prijetnji, kao što je npr. CERT (Computer Emergency Response Team).

2. Provjera efikasnosti sustava

   Konstantno provjeravanje sigurnosnih mjera i mehanizama implementiranih sustavom upravljanja sigurnošću informacija nužno je kako bi se osigurala njegova efikasnost. Provjeru je dužan provoditi svaki zaposlenik u svakom aspektu svog rada, a osim toga nužno je provoditi i periodičke provjere ranjivosti sustava. Periodičke provjere ranjivosti mogu se provoditi unutar same organizacije ili se za to mogu angažirati osposobljeni stručnjaci izvan organizacije kako bi provjera bila što je moguće objektivnija. Uzimajući u obzir rezultate takvih provjera, provode se mjere za poboljšanje sustava upravljanja sigurnošću informacija.

3. Provjera razine rezidualnog i prihvatljivog rizika

   Efektom sigurnosne mjere smatra se njezina sposobnost umanjivanja prijetnje, ranjivosti ili čak vrijednosti informacijskog resursa kako bi se postigao minimalan rizik. Ovo nas dovodi do koncepta rezidualnog rizika, prikazanog na Slici 6.




**Slika 6:** Procjena rezidualnog rizika

Za umanjivanje ranjivosti informacijskog sustava mogu se upotrijebiti sljedeće strategije:

- uklanjanje svih ranjivosti,
- uklanjanje onih ranjivosti koje zahtijevaju najmanje financijskih sredstava a zatim onih unutar dozvoljenih sredstava,
- uspostava i odabir ravnoteže između tehničkih i ne-tehničkih metoda za uklanjanje ranjivosti,
- prioritetno uklanjanje onih ranjivosti koje uzrokuju najveću štetu.

Pokušaj uklanjanja svih ranjivosti najvjerojatnije neće umanjiti rizik na nulu. Štoviše, takva je metoda obično skupa i vremenski zahtjevna, te rijetko donosi očekivane rezultate. Ostale metode mogu se kombinirati u cilju dobivanja najboljeg rezultata, odlukom o odabiru određenog odnosa troška i učinka.

Osim umanjivanja ranjivosti, kao metoda umanjivanja sigurnosnog rizika može se koristiti umanjivanje prijetnje ili vrijednosti informacijskih resursa, kao npr. umanjivanje vrijednosti podataka njihovom enkripcijom.

4. Provedba internih audita sustava

   Interni auditi igraju važnu ulogu u održavanju kontinuiranog poboljšanja sustava. Cilj internih audita je provjera efikasnosti, ispravne implementacije i održavanja sigurnosnih kontrola s ciljem potvrde da se sustav upravljanja sigurnošću informacija ponaša onako kako se to od njega očekuje.

   Audit se sastoji od slijedećih aktivnosti:

   - definicija ciljeva audita,
   - pregled dokumentacije sustava upravljanja sigurnošću informacija,
   - plan audita,
   - audit,
   - izvještaj o rezultatima audita,
   - specifikacije dodatnih audita ukoliko za njima postoji potreba.

   Organizacije koje već imaju implementiran sustav upravljanja kvalitetom mogu jednostavno kombinirati interni audit sustava upravljanja sigurnošću informacija s internim auditima sustava upravljanja kvalitetom.

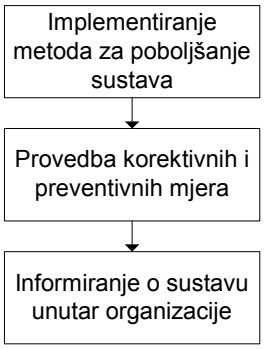
5. Pregled sustava od strane poslovodstva

   Poslovodstvo obavlja pregled i ocjenu sustava upravljanja sigurnošću informacija s ciljem potvrde kontinuirane adekvatnosti i efikasnosti sustava. Ulazni podaci za pregled poslovodstva su rezultati provedenih audita i kontrola, izvršene korektivne i preventivne akcije, preporuke za unapređenje sustava te nove tehnologije i metode koje se koriste u informacijskim sustavima.

   Rezultati pregleda poslovodstva su prijedlozi za korekcije sustava, njegovo unapređenje kao i osiguranje potrebnih resursa za provedbu specificiranih korektivnih i preventivnih mjera.

### 3.4. "Act" faza PDCA ciklusa

U ovoj fazi provode se korektivne i preventivne akcije predložene kao rezultat pregleda sustava od strane poslovodstva. Cilj ove faze je postizanje stalnog unapređenja sustava upravljanja sigurnošću informacija. Proces je prikazan Slikom 7.



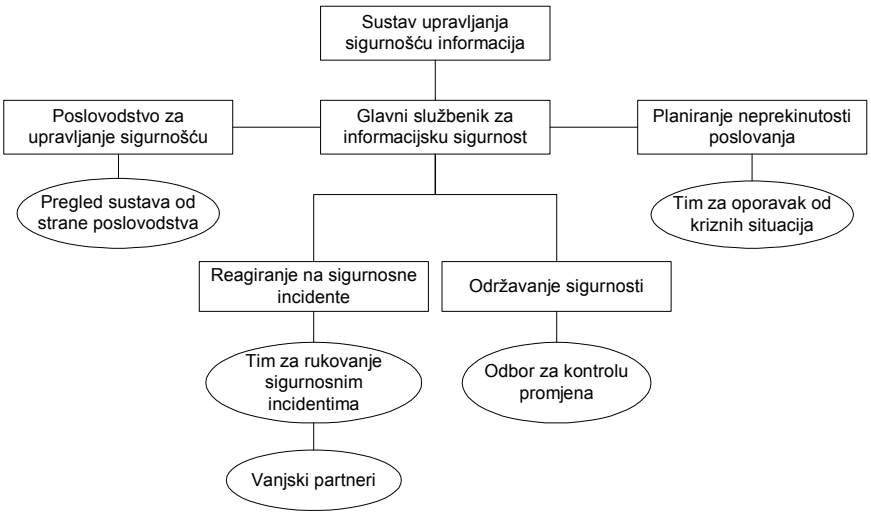

**Slika 7:** "Act" faza PDCA ciklusa

1. Implementiranje metoda za poboljšanje sustava
   Kontinuirana težnja unapređenju koja nije bazirana isključivo na aktualnom problemu vrlo je važna odlika svakog uspješnog sustava upravljanja organizacijom. Ona predstavlja napredak iz reaktivnog na proaktivno upravljanje. Metode kontinuiranog poboljšavanja sustava su sljedeće:
   – identifikacija potencijalnih unapredivih područja,
   – analiza i opravdanje potrebnih akcija,
   – odluka o provođenju mjera za poboljšanje,
   – implementacija poboljšanja,
   – mjerenje utjecaja poboljšanja na organizaciju,
   – analiza rezultata poboljšanja na pregledu poslovodstva,
   – stalna potraga za novim metodama poboljšanja.

   Znanja i informacije prenesene iz drugih organizacija koje imaju uspješno implementiran sustav upravljanja sigurnošću informacija mogu biti vrlo korisna u procesu stalnog poboljšanja sustava. Također, dodatna korisna znanja mogu se dobaviti angažmanom stručnjaka za područja informacijske sigurnosti koji redovito poznaju najnovije informacije i procedure upravljanja sigurnošću informacijskih sustava.
2. Provedba korektivnih i preventivnih mjera
   Korektivne mjere provode se nakon ostvarenog sigurnosnog rizika kako bi se spriječila ponovna pojava rizika u budućnosti. Preventivne mjere se koriste za umanjivanje vjerojatnosti pojave rizika i umanjivanje potencijalnih šteta.
3. Informiranje o sustavu unutar organizacije
   Provedba sigurnosnih politika i upoznavanje svih zaposlenika sa sustavom upravljanja sigurnošću informacija mora se provoditi planirano i bez osjećaja opterećenja među zaposlenicima organizacije. Potrebno je također provoditi redovitu izobrazbu poslovodstva, korisnika i partnera o načinu primjene i pridržavanja implementiranih sigurnosnih politika. Pri tome od pomoći mogu biti raznorazne kreativne i poticajne metode kao što su posteri, prezentacije, web stranice i ostali lako dostupni sadržaji koji pružaju aktualne informacije o ispravnom i sigurnom korištenju informacijskih resursa.

## 6. Rezultati implementacije sustava upravljanja sigurnošću informacija

Nakon što je uspješno implementiran, sustav upravljanja sigurnošću informacija donosi pozitivne promjene u odnosu organizacije prema sigurnosnim aspektima i zahtjevima informacijskog sustava. Organizacija se mora prilagoditi novim zahtjevima pomoću uspostave sigurnosne organizacijske strukture. Ova struktura oblikuje se prema karakteristikama implementiranog sustava upravljanja sigurnošću informacija kao i prema osnovnim poslovnim karakteristikama i potrebama organizacije. Najvažniji elementi sigurnosne organizacijske strukture prikazani su Slikom 8.




**Slika 8:** Sigurnosna organizacijska struktura

Prikazana struktura predstavlja uspostavljene organizacijske elemente namijenjene efikasnom radu implementiranog sustava upravljanja sigurnošću informacija. Svi elementi su pod direktnom odgovornošću glavnog službenika za informacijsku sigurnost.

Poslovodstvo za upravljanje sigurnošću pruža kontinuiranu potporu najviših tijela organizacije sustavu upravljanja sigurnošću informacija kao i konstantan nadzor nad sigurnosnim procesima. Na pregledu sustava od strane poslovodstva definiraju se ciljevi sigurnosti informacijskog sustava te strategije i ciljevi kontinuiranog poboljšanja sustava.

Element reagiranja na sigurnosne incidente uključuje formiranje tima za rukovanje sigurnosnim incidentima. Misija ovog tima je pripremanje, kontroliranje i učenje iz sigurnosnih incidenata. Tim može surađivati s vanjskim partnerima te uspostaviti veze s lokalnim organima vlasti i zakona radi sprečavanja ozbiljnih sigurnosnih incidenata.

Element održavanja sigurnosti namijenjen je praćenju i izvještavanju o relevantnim sigurnosnim problemima glavnom službeniku za sigurnost. Ovaj element također uključuje odbor za kontrolu promjena čija funkcija je upravljanje procesom promjene, procedurama za nadogradnju sustava, te tijekom dokumentacije sustava upravljanja sigurnošću informacija.

Element planiranja neprekinutosti poslovanja uspostavljen je s ciljem redukcije šteta i prekida u poslovanju uzrokovanih teškim sigurnosnim incidentima na prihvatljivu razinu. Tim za oporavak od kriznih situacija razvija i implementira plan kontinuiteta poslovanja, koji definira niz procedura koje je nužno provesti kako bi se kontinuitet održao. Nadziranim provođenjem procedura opisanih planom kontinuiteta poslovanja sprečavaju se nove teške posljedice za organizaciju i osigurava brzi povratak u produktivnu razinu poslovanja. Kako ne bi došlo do širenja posljedica nastale krizne situacije na ostale poslovne resurse, preventivne sigurnosne mjere nužno je provoditi i nakon saniranja lokaliziranih oštećenja sustava.

# 7. Zaključak

Ukoliko je informacijski sustav organizacije od neposredne važnosti za uspješnost i kontinuiranost njenog poslovanja, nužno je uspostaviti sustav upravljanja sigurnošću informacija. Istovremeno, organizacije moraju biti svjesne činjenice da je uvijek prisutna određena razina nesigurnosti, što zahtjeva spremnost i sposobnost organizacije da se u svakom trenutku suoči s najnovijim sigurnosnim prijetnjama i na vrijeme reagira na eventualne sigurnosne incidente. Cilj takve orijentacije organizacije je osiguranje neprekinutosti poslovanja i maksimalna zaštita informacijskih i svih poslovnih resursa. Implementacija sustava upravljanja sigurnošću informacija predstavlja provedbu potrebnih mjera za postizanje zadovoljavajuće razine informacijske sigurnosti unutar organizacije, čineći tako bitan faktor u prepoznavanju organizacije kao pouzdanog i modernog poslovnog partnera.

# 8. Reference

[1] ISO, ISO/IEC 17799, Information technology - Code of practice for information security management, First edition, International Organization for Standardization, Geneva, 2000.
[2] BSI, BS 7799-2:2002, Information security management systems - Specification with guidance for use, British Standards Institute, London, 2002.
[3] IUG, ISMS Journal, Issues 1 and 2, International User Group (IUG), 2002.
[4] Tom Carlson, Information Security Management: Understanding ISO-17799, International Network Services (INS), 2003.
[5] Dan VanBelleghem, Tom Hasman, Surviving a Risk Assessment, SRA International, Inc, CSI's 30th Annual Computer Security Conference, 2003.
[6] How 7799 works, Gamma Secure, Systems, 2003, http://www.gammassl.co.uk/bs7799
[7] Guidelines for IT security policy, IT Security Promotion Committee, 2000, http://www.kantei.go.jp/foreign/it/security/2001/guideline.html.