Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

11. UPRAVLJANJE SISTEMOM I PROGRAMOM ZAŠTITE INFORMACIJA

Ciljevi

- **Razumeti** :
  - **metodologiju** (principe, odgovornost) upravljanja SZI
  - proces **integralnog upravljanja** SZI
  - upravljačke **kontrole najbolje prakse** zaštite (ISO/IEC 27001)
  - **metrički sistem** za evaluaciju upravljanja SZI
  - **preporuke** (ISO/IEC 27001) **otvorene probleme** u oblasti upravljanja zaštitom
  - **generičku strukturu** dokumenta *program zaštite*
  - **obim i strukturu** *plana, politike i procedure zaštite*
  - **opštu metodologiju** za implementaciju programa/sistema zaštite
  - **tok procesa implementacije programa/sistema** zaštite
  - ključne komponente procesa implementacije SZI/programa
- **Naučiti:**
  - samostalno razviti *politiku i proceduru zaštite*

Upravljanje sistemom zaštite informacija (SZI)

- **Bezbednost/zaštita informacija** nije odredište, nego neprekidna kritična funkcija koja podržava misiju organizacije.
- **Bezbednost informacija** je integralni deo upravljanja poslovanjem koji zahteva podršku menadžmenta na najvišem nivou
- **Menadžer sistema zaštite** je toliko efektivan koliko ga podržava menadžment organizacije
- **Stretegijska podrška menadžmenta** je ključni faktor uspeha programa zaštite informacija
- **Program zaštite informacija** mora biti rentabilan

Razvoj menadžment sistema zaštite informacija

Metodologija:

- **Principi: GAISP**
- **Politika:** ISMS **(***ISO/IEC 27001, NIST***),** zaštite informacija
- **Proces upravljanja rizikom (UR) (NIST):**
  - implementiran se sa 16 *osnovnih aktivnosti*
  - *približno jednak* **procesu upravljanja SZI***:*
    1. Uspostavljanje sistema za centralno UR/SZI
    2. Procena rizika i određivanje bezbednosnih zahteva
    3. Implementacija rentabilnih kontrola zaštite
    4. Promovisanje svesti o potrebi i obuka
    5. *Revizija* sistema zaštite i evaluacija efektivnosti i usklađenosti

Razvoj menadžment sistema zaštite informacija (1)

Uloge i odgovornosti

1. **Definisane i dodeljene svim učesnicima (*ISO 27001*)**
2. **Odgovorno lice za ISMS (*ISO 27001*) :**
   - ***Imenovano***: **CIO** (*Corporate Information Officer*)
   - ***Puno radno vreme***: **CISSO** (*Corporate Information System Security Officer*) za zaštitu informacija u celoj organizaciji
   - ***Trend profesionalni profil***: **CIAO** *(Corporate Information Assurance Officer)* ovlašćen i za **sertifikaciju sistema zaštite**
3. **Tim** obučenih specijalista zaštite:
   - **CISP** (*Certified Information Security Professionals*)
   - ***digitalni forenzičar?***
   - ***etički haker****? ltd.*

Razvoj menadžment sistema zaštite informacija (2)

Implementacija principa zaštite

- Ako ne postoji implementirane komponente ili **s/z, uključiti najmanje sledeće U** kontrole:
  - *politike zaštite*
  - *obuku i razvoj svesti o potrebi zaštite*
  - *AC i elementarnu praktičnu obuku o GAISP*
  - *razmenu informacija o incidentima*
  - *definisanje uloga i saradnja u zaštite*

Razvoj menadžment sistema zaštite informacija (3)

Struktuirani pristup ISMS-u

- ***Prvi pristup***:
  - **upravljanje određenim brojem infrastrukturnih servisa** za normalan rad IKTS i SZI
  - **Osnovni nedostatak**:
    - *kompleksnost dovodi do postepene degradacije efektivnosti servisa IKTS i SZI*
    - *procesi upravljanja zaštitom i IKTS moraju biti dobro organizovani i sinhronizovani*
- ***Drugi pristup:***
  - **integrisano upravljanje IKTS i SZI**, pogodan za manje organizacije
  - *mehanizmi zaštite obezbeđuju visoku raspoloživost IKTS servisa*
  - *zahteva usklađeno funkcionisanje pod kontrolom administratora*

Razvoj menadžment sistema zaštite informacija (4)

Procesni pristup ISMS-u

- **Sistem upravljanja zaštitom informacija** – **ISMS** (*Information Security Managament Systemt*):
  - definisan standardom **ISO/IEC 27001:2013**
  - implementiran **PDCA** (*Plan-Do-Check-Act*) procesnim modelom
  - osnovni upravljački mehanizam je ***ISMS politika zaštite***
- **U PDCA procesima ISMS od posebnog značaja** je:
  - određivanje *uloga i odgovornosti* u zaštiti
  - *uspostavljenje SMF okvira, implementacija ISMS, nadzor i **provera** rada i poboljšavanje procesa* ISMS-a
- **Kontrole zaštite** su opisane u standardima:
  - ISO/IEC 27001: Anex A (lista), ISO/IEC 27002 katalog
  - NIST SP 800–53 A, B, C, katalog osnovnih i poboljšanih

Procesni pristup ISMS-u

- **Najznačajniji resurs za ISMS-a**:
  - **tim** specijalista zaštite (**CIRT**) sa **specifičnim znanjima**, **veštinama** i **iskustvima i neprekidnim usavršavanjem**
- ***Proaktivno* delovanje**:
  - samo **jedinstven i dobro obučen tim** garantuje postizanje strateških bezbednosnih ciljeva
  - **apsolutno je potrebno?**
- **Važno je praviti razliku** između:
  1. **znanja** i **veština** na tržištu (*opšta praksa zaštite, edukacija, CISSP*...) i
  2. **specifičnih veština i iskustava** (*forenzička, hakerska...*)
- **Obe kategorije podjednako su značajne** u zaštiti:
  - specifična znanja teže je pronaći, zaposliti i zadržati

Generički proces ISMS-a

- **PDCA je ciklički ponovljiv i sadrži 4 potprocesa**:
  1. *pripremu*, ***upravljanje rizikom (SoA)***, ***politika zaštite*** *ISMS-a*
  2. *primenu,* ***implementacija plana tretmana rizika***
  3. *proveru*, ***upravljanje promenama, upravljanje konfiguracijom*** *i*
  4. *poboljšavanje* ***korektivne i preventivne akcije***
- **Proces upravljanja rizikom ≡ upravljanja reaktivnim SZI**
- **Upravljanje promenama** - identifikuje bezbednosne zahteve za promene u IKTS i okruženju posle **incidenta/VD**
- **Upravljanje konfiguracijom** - održava *trag promena u IKTS- formalna provera* (*audit) i menadžerska provera*
- **Primarni cilj ISMS- da**:
  - promene u sistemu ne smanjuju efektivnost sistema zaštite i ukupnu bezbednost organizacije

Generički proces ISMS-a (1)

- **Dobro je definisan *klasom upravljačkih kontrola zaštite (NIST):***
  - *upravljanje programom zaštite,*
  - *bezbednosnu procena i autorizacija,*
  - *planiranje sistema zaštite,*
  - *analizu i procenu rizika,*
  - *akviziciju sistema i servisa zaštite*
- **U IKTS gde nije implementiran ISMS, treba uključiti (NIST)**:
  - *politiku zaštite,*
  - *obuku i razvoj svesti o potrebi zaštite*
  - *upravljanje korisničkim nalozima*
  - *izveštavanje o incidentima i*
  - *definisanje odgovornosti i saradnje u oblasti zaštite*

Generički procesi ISMS-a (2)

(a) Na taktičkom nivou - PDCA modelom procesa:

- *identifikovanje vrednosti imovine, pretnji, ranjivosti i uticaja*
- *procena rizika*
- *uspostavljanje politike zaštite i*
- *implementacija kontrola zaštite za ublažavanje rizika*

(b) Na strateškom nivou – *ISBS:**

- na bazi **konzistentne primene politike zaštite**
- predstavlja **preporučeni nivo izvršavanja politike zaštite**
- **garantuje implementaciju dobrog sistema zaštite**
- ISBS usaglašenost **garantuje dobru procenu rizika** i
- implementaciju adekvatnih kontrola zaštite za ublažavanje rizika

***ISBS** (*Information Security Benchmark System)*

Primer:: Generički procesi ISMS-a

Identifikovanje pretnji

Procena rizika

Uspostavljanje politike zaštite

Implementacija kontrola zaštite

a.

Benčmark sistem

Uspostavljanje politike zaštite

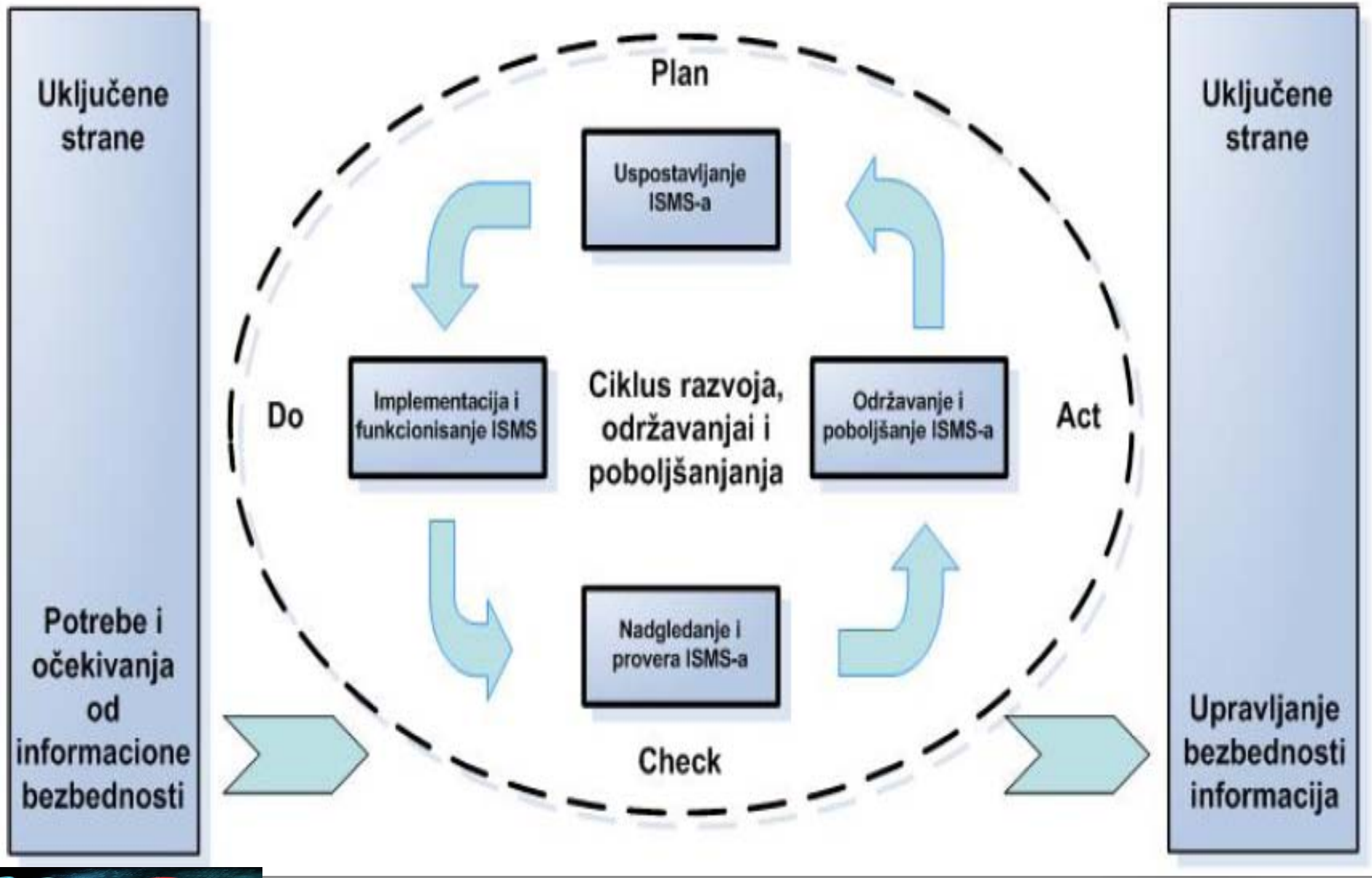
Implementacija kontrola zaštite

b.

Uspostavljanje ISMS-a (ISO/IEC 27001)

- **Zajednički elemenati uspostavljanja ISMS-a**:
  - primenom **PDCA (***Plan, Do, Check, Act***)** modela procesa:
    - *planiranje, primena, provera, poboljšavanje*
- **Faza planiranja -** kontekst, obim i granice ISMS-a, ianaliza i procena rizika, izrada ISMS i politika zaštite
- **Faza implementacije –** realizuje politiku za uspostavljanje i implementaciju projekta ISMS-a
- **Faza provere** – pratiti aktivnosti u praksu ISMS-a, otkriva propuste i slabosti internom i formalbnom proverom i definiše neophodne promene
- **Faza poboljšavanja -** realizuje korektivne i preventivne promene na osnovu utvrđenih propusta

Primer: Primena PDCA modela na ISMS (ISO/IEC 27001)



Primena PDCA modela na ISMS (ISO/IEC 27001)

- **Kritični faktori implementacije ISMS–a :**
  - *usaglašenost politike/ciljeva/prakse zaštite* sa ciljevima poslovanja
  - *konzistentnost sa kulturom rada* i korisnička prihvatljivost ISMS,
  - *integrisanje svih uloga u ISMS* u redovno poslovanje organizacije,
  - *menadžerska podrška* ISMS-a
  - *razumevanje zaposlenih* o značaju zaštite i uticaju na poslovanje
  - *razvoj svesti* svih zaposlenih o potrebi zaštite i rizicima
  - *potpuna komunikacija* između tima za uvođenje ISMS i drugih
  - *neprekidna obuka i edukacija* zaposlenih u oblasti zaštite
  - *procesni pristup, upravljanje i poboljšavanje* procesa PDCA i ISMS

Implementacija ISMS-a (pristup *odozgo-nadole*)

- ***Glavni zadaci:***
  - *Precizno uspostaviti uloge*
  - *Definisati dužnosti i odgovornosti*
  - *Identifikovati specifične zadatke*
  - *Definisati standard za kvalitet implementacije*
  - *Implementirati proces merenja/validacije*

Razvoj metrike ISMS-a

- **Kriterijumi za izbor:**
  - *broj novih implement. kasni iz bezb. razloga,*
  - *broj kritičnih poslova koji se oslanjaju na IS,*
  - *broj kritičnih objekata infrastrukture IS,*
  - *poboljšanje svesti zaposlenih,*
  - *puna usaglašenost, ili dopuštena odstupanja,*
  - *procenat razvijenih i dokumentovanih plan./pol.zaštite*
  - *procenat plan./pol. zaštite sa kojima su upoznati zaposleni*

Razvoj metrike ISMS-a (1)

- **Metrika *SSE CMM (ISO/IEC 21827):***
  - **Skala sazrevanja/kapaciteta ISMS procesa :**

  0. **Ne postoji** — proces U/Z nije primenjen,
  1. **Inicijalni proces** — procesi U/Z *ad hoc* i neregularni
  2. **Ponovljiv** — procesi U/Z planirani i ponovljivi,
  3. **Definisan** — procesi U/Z planirani, ponovljivi, dokumentovani, implementirani i o njima upoznata organizacija,
  4. **Upravljan** — procesi U/Z ponovljivi, dobro definisani, nadzirani i kvantitativno **mereni**
  5. **Optimizovan** —procesi U/Z ponovljivi, dobro definisani, nadzirani, kvantitativno mereni i primenjuju se najboljom praksom U/Z

Izlazni rezultati procesa ISMS-a

1. ***Strategijsko usklađivanje:***

- bezb. zahtevi definišu se u skladu sa poslovnim,
- rešenja sistema zaštite uklapaju se u procese org.,
- investiranje u zaštitu usklađeno sa strategijom razvoja i prihvaćeno na bazi procene rizika.

2. ***Nove vrednosti (kvalitet):***

- standardan set praksi zaštite,
- određeni prioriteti za oblasti koje daju najveće poslovne rezultate
- rešenja zaštite su primenjena u celoj organizaciji,
- neprekidnost poboljšanja kulture zaštite

Izlazni rezultati procesa ISMSa -1

3. Upravljanje rizikom:

- prihvaćen i usaglašen profil rizika,
- razumevanje o izloženosti faktorima rizika,
- svest o prioritetu upravljanja rizikom.

4. Merenje performansi:

- definisan set metrika,
- proces merenja sa povratnom spregom za progresivno poboljšanje,
- nezavisna bezbednosna garancija

Preporuke za implementaciju ISMS-a

1. *Razvoj svesti, obuka i obrazovanje u oblasti zaštite*
2. *Izrada dokumenta Politika zaštite*
3. *Alociranje odgovornosti za zaštitu*
4. *Upravljanje bezbednosnim incidentom i izveštavanje*
5. *Kontrola malicioznih programa*
6. *Plan upravljanja VD i kontinuitetom poslovanja (BCP)*
7. *Zaštita intelektualne svojine*
8. *Zaštita baza podataka*
9. *Zaštita CIA podataka i informacija*
10. *Usklađenost prakse sa politikom zaštite*

Program zaštite

Program zaštite:

- sve što neka organizacija čini da zaštiti inf. imovinu
- dokumentuje se kroz **programsku (ISMS) politiku**

Programska politika (struktura**):**

- kratak dokument (1-2) stranice koja ističe nameru organizaije da zaštiti svoj IKTS i informacije
- **struktura programske politike**:
  - namena,
  - obim,
  - odgovornost
  - usaglašenost

  Politika bezbednosti XY organizacije

Plan zaštite

- **Usaglašen sa**:
  - zakonskim propisima, poslovnim ciljevima i arhitekturom IS
  - konzistentan i ima formu *biznis plana*
- **Struktura:**

1.Uloge i odgovornosti:

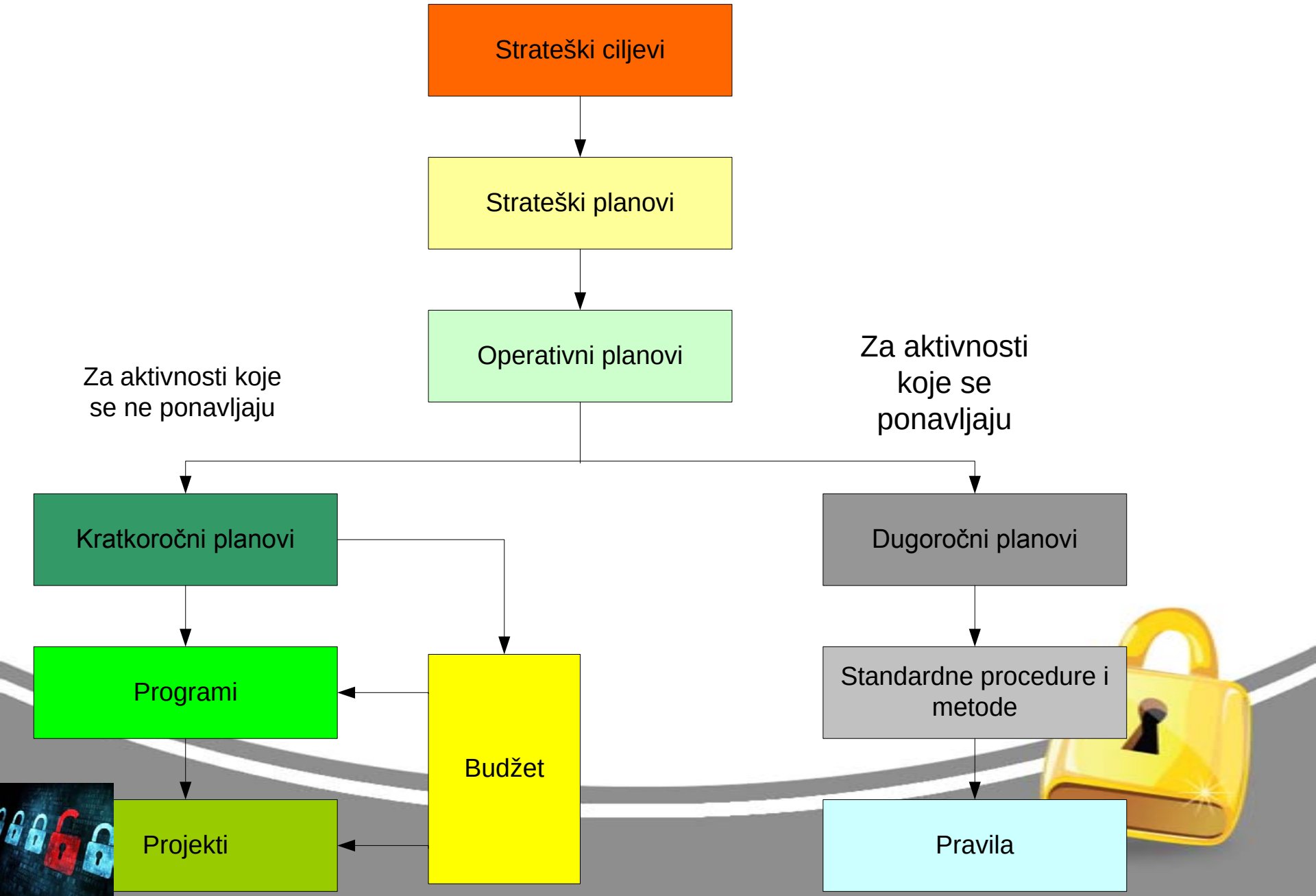
- menadžerske strukture i upravnih odbora organizacija
- internog rukovodstva organizacije
- zaposlenog osoblja

2. Upravljanje promenama:

- **U, O i T** kontrole zaštite

Prilozi\PRILOG 10A.doc

Opšti model planiranja u organizaciji



Plan zaštite -uloga menadžmenta

1. **Eksplicitna (**princip**) i ima vodeću ulogu i odgovornost** u kreiranju ***programa, plana i politike*** zaštite:
   - **Obezbeđuje**:
     - superviziju sprovođenja programa zaštite
     - izradu politike zaštite
     - uvođenje standarda zaštite
     - angažovanje odgovornih, stručnih i iskusnih lica u zaštiti
     - smernice za upravljanje politikom nadzora i provere (revizije) sistema zaštite

Plan zaštite
-Uloga internog tima organizacije-

- **Odgovoran za**:
  - implementaciju programa zaštite
  - razvoj i reviziju plana, politike i procedura zaštite
  - upravljanja rizikom
  - analizu usklađenosti prakse i politike/procedura zaštite
  - analizu rezultata nadzora i kontrole sistema zaštite
  - analizu rezultata upravljanja incidenatom i VD
  - analizu rezultata obuke u zaštiti
  - reviziju programa zaštite i (GAISP principa)

Plan zaštite
-Uloga korisnika-

- učestvuju u razvoju plana, politike i procedura zaštite (po potrebi)
- implementiraju politiku/procedure zaštite
- koriste mehanizme i protokole zaštite
- sprovode procedure zaštite
- obaveštavaju o greškama i incidentima
- prate i poznaju poslovne procese i ranjivosti sistema
- učestvuju u razvoju svesti o potrebi zaštite

Plan zaštite
-Upravljanje promenama-

- Mandatna obaveza (**princip, standard**)
- **Sistemski način uvođenja svih vrsta promena** IKTS
- **Obuhvata**:
  - faktore promene okruženja, tehnologija zaštite i IKTS
  - regularnu reviziju plana, politike i procedura zaštite
  - izradu procedure za upravljanje promenama
  - kontrolu primene *kontrola* zaštite (U, O, T) za upravljanje promenama

Politika zaštite

- **zasniva se na proceni rizika**
- **izjava na visokom nivou relativno nepromenljiva u datom periodu!?**
- **smernice uprave** org. da se izradi program zaštite, uspostave bezbednosni ciljevi i pripišu odgovornosti
- **sadrži specifična pravila** (izjave, saopštenja) zaštite (e-mail, AC, udaljeni pristup, IAA...)
- ključna komponenta plana zaštite
- **okvir** očekivanja,obaveza, tehnologija i procesa
- **utvrđuje ciljeve**, očekivanja i verifikovane zahteve
- **koristi:** *instrukcije, procedure, uputstva, pravce aktivnosti i principe* zaštite
- Ima tipične i specifične elemente (saopštenja)

Problemi nedostatka politike zaštite?

- >25% zaposlenih nije pročitalo ni jednu politiku zaštite u 2007.*
- ≈ 50% nije pročitalo namenjenu politiku zaštite u 2007.
- <30% nije imalo obuku ni razvoj svesti o potrebi zaštite u 2007.
- ≈ 65% organizacija ne prati da li zaposleni čitaju politiku zaštite (potpišu izjavu o prihvatanju i razumevanju politike)
- > 75% zaposlenih ignoriše politiku čak i kad znaju da postoji *
- 46% routinski deli pasvorde *
- 50% organizacija nema politiku za izveštavanje o bezbednosnom incidentu i ranjivostima sistema
- ≈ 67% organizacija ističe da je ključni prioritet u sledećoj (2009) podizanje svesti o potrebi zaštite
- ≈ 22% organizacija imaju program za razvoj svesti o potrebi zaštite
- ≈ 13% organizacija ima časove obuke iz oblasti zaštite informacija

*CSI/FBI & Information Security shield anketa

Uputstvo za zaštitu

1. Za menadžere, admin. i specijaliste zaštite:

- **uopšten i sveobuhvatan**, dovoljno detaljan, **poverljiv** dokument
- definiše komponente s/z i upravljanje programom zašt.
- definiše sadržaj i strukturu za izradu **programa/plana/ politika/procedura zaštite** (**PPPPZ**)
- definiše načine projektovanja arhitektura i kontrola s/z
- sadrži reference na kataloge **U, O i T** kontrola zaštite

2. Za korisnike IKT sistema

- orijentisano na određenu grupu korisnika
- obrađuje određenu komponentu zaštite

Prilozi\PRILOG 10 D.doc

Pregled i ažuriranje dokumenata zaštite (ISO/IEC 27001)

- Bezbednost i zaštita su dinamičke kategorije
- Nove hw/sw metode napada (**85 000** malvera/dnevno) i iskorišćenja ranjivosti
- Regularni pregled - najmanje 1/g
- Za veći stepen zaštite – češći pregled
- **Interna/eksterna revizija**:
  - *efikasnosti, usaglašenosti i ranjivosti (program zaštite)*
  - *tehnoloških promena IKTS i sistema zaštite*
  - *promena u arhitekturi IKTS*
  - *promena u poslovima, upravi i kulturi rada organizacije*

Procedure zaštite

- Redosled i načini primene precizno definisanih aktivnosti procesa zaštite - **dokumentuju procese zaštite**
- **spuštaju politiku zaštite na operativni nivo**
- značajno **smanjuju ljudske greške** (proboje s/z)
- obezbeđuju **usklađenost prakse i politike** zaštite

Primer: Pristup dijagnostičkim izveštajima

- specificira zahtevani proces autentifikacije i autorizacije
- definiše zahteve za mere fizičke zaštite
- definiše način unošenja dijagnostičke informacije
- definiše kriptološki algoritam
- identifikuje primaoce informacija
- sugeriše načine izbegavanja tipičnih grešaka i.t.d

PRIMERI : **Prilozi\PRILOG 10C.doc**

Opšti metod implementacije programa/SZ

1. Ublažavanjem ukupnog rizika na prihvatljivi nivo

- dugoročan i zahtevan proces
- podrazumeva sveobuhvatni sistemski pristup
- smanjenje svih faktora rizika na prihvatljiv nivo
- implementacijom rentabilnih U,O,T k/z

2. Procesom 4-fazne tranzicije bezbednosnog stanja

- alternativni (*cik-cak*) metod implementacije
- metod 4 - fazne tranzicije IS iz jednog u drugo (više) bezbednosno stanje
- treba poći od zaštite najkritičnijih objekata IS

Primer: Faze implementacije programa zaštite

Metod OCTAVE

Faza	Kritični objekti za misiju	Kritični objekti	Primarni objekti	Opšti objekti
1.	20 glavnih faktora rizika (FR.)	0	0	0
2.	50 glavnih faktora rizika	20 glavnih FR	0	0
3.	100 glavnih faktora rizika	50 glavnih FR	20 glavnih FR	0
4.	200 glavnih faktora rizika	100 glavnih FR	50 glavnih FR	20 glavnih FR

Proces implementacije programa zaštite

1. ***Izbor tima*** za koordinaciju i monitorisanje.
2. ***Identifikovanje bezbednosnih faktora rizika***
3. ***Obavezna kontrola toka procesa***
4. ***Integracija i prilagođavanje programa***

- **Obavezne komponente sadržaja procesa**:
  - *obuku zaposlenih*
  - *kontrolu usklađenosti*
  - *nametanje obaveze izvršavanja* politika i procedura zaštite

Obuka zaposlenih

- ***Svi zaposleni*** - izgraditi svest o potrebi zaštite
- ***Tehničko osoblje*** – obuka za korišćenje i održavanje opreme
- ***Sistem administratori i članovi CIRT*** - specijalizovanu obuku
- ***Upravna struktura*** - razume svoju ulogu
- ***Izvršni menadžeri*** - o svojim odgovornostima
- ***Operativno osoblje*** - dodatnu obuku (plan zaštite)

Kontrola usaglašenosti

- Stepen integracije implementiranog programa/SZ meri se stepenom ***opšte i specifične*** uskl.:

1. Kontrola opšte usaglašenosti - upravna struktura:

  – Monitoringom zaposlenih o korišćenju IKT

  – Primene *Zakona i standarda zaštite*

2. ***Kontrola specifične usaglašenosti*** – zaposleni

- Verifikuje:

  – *poslovne procese*

  – *operativno korišćenje tehnologija zaštite*

Interni nadzor i provera -1

Obezbeđuje:

- ključnu ulogu u zaštiti kibernetičkog prostora
- ključne inf. za nezavisnu procenu rizika
- analizu kompetentnosti interne kontrole
- ispitivanje nivoa usklađenosti sa normativima
- evaluaciju adekvatnosti i efikasnosti zaštite na Internetu
- *proaktivno* aktiviranje uprave za ublažavanje rizika

Interni nadzor i provera -2

1. Vrste:

- interna revizija ISMS
- posebni nadzor sistema zaštite mrežne infrastrukture
- procena adekvatnosti IDS/IPS, ili
- procena kapaciteta upravne strukture itd.

2. Učestanost monitoringa:

- treba da se zasniva na zdravoj logici

3. Metod monitoringa:

- skeneri ranjivosti RS i RM

4. Obim monitoringa:

- uspostavljena odgovornost, prava i ograničenja
- provera postojanja ostalih komponenti zaštite...

Eksterna provera (*auditing*)

1. **Vrši neke dodatne kontrolne funkcije**:
- reinženjering procesa za povećanje efikasnosti
- smanjenje troškova poslovanja
2. **Unosi dodatni bezbednosni rizik**
3. **Treba da ima edukativnu i savetodavnu ulogu**
4. **Vrši se u bezbednom okruženju u atmosferi poverenja**
5. Kontrolori:
- neprekidno prate razvoj tehnologija zaštite, najbolju praksu zaštite, trendove kompjuterskog kriminala, ...

Izveštavanje o proveri-1
-Upotreba-

- ***ISACA*** (*Information System Audit and Control Association*) predlaže da izveštaj treba da:
  - pokaže koji sistem mera je koristio kontrolor (*auditor)*
  - pomogne u planiranju, radu i kontroli rada *auditor*-a
  - olakša TTPS da izvrši reviziju rada kontrolora
  - evaluira sistem kvaliteta programa kontrole
  - obezbedi podršku za naplatu polise osiguranja
  - pomogne profesionalni razvoj specijalista zaštite itd.

Izveštavanje o proveri-2
-Sadržaj izveštaja-

- ***Rezultat:***
  - *Kontrola aplikacija*
  - *Automatizovana kontrola*
  - *Kontrola politika zaštite*
  - *Svest o potrebi zaštite*
  - *Strategijski ciljevi*
  - *Korišćenje pravnih saveta u procesu kontrole*

Izveštavanje o proveri -3
-Format izveštaja o kontroli sistema zaštite-

- plan i pripremne aktivnosti (definisani obim i ciljevi kontrole)
- program kontrole (sadržaj rada)
- faze izvođenja kontrole i dokazi koje treba skupljati
- nalazi kontrole, zaključci i preporuke
- pregled i nalaz supervizorske kontrole.

Nametanje obaveze izvršavanja i izveštavanja

- **Sledi obuku, nadzor** i kontrolu usaglašenosti prakse i politike zaštite
- **Izveštaj o nadzoru i kontroli** - ulazna informacija za reinženjering programa i politike zaštite
- **Kritičan faktor** - implementacija politika/procedure bez represivnih mehanizama za obavezu izvršavanja
- **Sankcije za nesprovođenje** politike zaštite:

➢ dobro i unapred osmišljene,

➢ od upozorenja do otpuštanja sa posla, ili sudskog gonjenja

Implementacija programa zaštite

Ključni faktori uspeha:

- potpuna podrška upravne strukture
- upoznavanje s ciljevima zaštite svih zaposlenih
- prepoznavanje jedinstvenih zahteva organizacije
- uključivanje kompetentnih i stručnih timova org.
- imenovanje odgovornog tima ili pojedinaca
- definisanje i ugradnja mehanizama za detekciju, korekciju i do-obuku i ponovnu edukaciju u slučaju proboja

Zaključci

1. **Glavni cilj** upravljanja zaštitom informacija (ZI):
   - uspostavljanje održivog programa,
   - selekcija i izbor resursa i revizija sistema zaštite
   - za održavanje rizika na prihvatljivom nivou.
2. **GAISP - osnovni skup principa** za *upravljanje sistemom ZI*
3. **Metodologija za upravljanje ZI**: IEC/ISO 27001 (ISMS)
4. **Merenje zrelosti procesa upravljanja ZI** (SSE – CMM)
5. **Osnovni problemi** upravljanja zaštitom:
   - obezbeđivanje podrške menadžerske strukture za program zaštite
   - obezbeđivanje korisničke prihvatljivosti za politiku zaštite
6. **Preporuke z**a efektivno ISMS obezbeđuje standard ISO/IEC 27001:
   - otvoreni su brojni problemi u oblasti usklađivanja i
   - standardizacije tehnika upravljanja i izveštavanja

Zaključci (1)

1. ***Program zaštite*** obuhvata detaljan i sveobuhvatan plan zaštite, politike i procedure zaštite
2. ***Plan zaštite***-sveobuhvatan strateški dokument za implementaciju *programa* zaštite IS
3. ***Politika zaštite je*** izjave na visokom nivou koja obezbeđuje okvir očekivanog ponašanja uprave, zaposlenih, tehnologije i procesa zaštite, a realizuje se kroz instrukcije, procedure i principe rada, obavezne za celu organizaciju
4. ***Procedure zaštite*** precizno definisani načini izvršavanja aktivnosti i praksi zaštite koje se često ponavljaju i dokumentuju procese zaštite

Pitanja