Standard ISO 27001

Predrag Skundric

Svrha minimalnim standardima upravljanja infomrmacionim sistemima finansijskih institucija

Svrha odluke je da se definišu sledeći aspekti informacionih sistema finansijskih institucija:

- Definišu pojmovi u okviru informacionog sistema finansijske institucije
- Definiše okvir za upravljanje informacionim sistemom
- Definiše okvir za upravljanje rizikom informacionog sistema
- Definiše ovir za upravljanje revizijom informacionog sistema
- Definišu okviri za bezbedno korišćenje informacionog sistema
- Definišu okviri za upravljanje konitnuitetom poslovanja i oporavka od u slučaju katastrofa
- Definiše okvir za razvoj i održavanja informacionog sistema
- Definiše okvir za poveravanje aktivnosti u vezi sa trećim licima po pitnju informacionih sistema
- Definiše okvir za upravljanjem elektronskim bankarstvom

Namena

Ovaj međunarodni standard pripremljen kako bi se sistem menadžmenta bezbednošću informacija:

- **Uspostavio**
- **Implementirao**
- **Koristio**
- **Pratio**
- **Preispitivao**
- **Održavao**
- **Poboljšavao**

ISO 27001 standard - uvod

ISO 27001:

- Koristi procesni pristup (Procesni pristup predstavlja primenu procesa unutar organizacije, zajedno sa identifikacijom i medjusobnim delovanjem svih uključenih procesa kao i njihovim upravljanjem)
- PDCA pristup (**P**lan – **D**o – **C**heck - **A**ct)
- Može se primeniti na sve vrste i tipove organizacija
- Je projektovan tako da obezbedi izbog odgovarajućih i srazmernih bezbednosnih kontrola (mera) koje štite informacionu imovinu i pružaju poverenje zainteresovanim stranama

Procesni pristup za menadžement bezbednošću informacija ohrabruje korisnike da naglase važnost:

- Razumevanja zahteva za bezbednost informacija u organizaciji i potrebe za uspostavljanjem politike i ciljeva za bezbednost informacija
- Kontrola implementacije i primene radi menadžmenta rizicima bezbednosti informacija u organizaciji u kontekstu ukupnih poslovnih rizika u organizaciji
- Praćenja i preispitivanja performansi i efikasnosti sistema za menadžment informacijama
- Stalnog poboljšanja zasnovanog na objektivnom merenju

ISO 27001 standard – PDCA

Planirati (uspostaviti ISMS) - **PLAN**	Uspostaviti ISMS politiku, ciljeve, procese i procedure bitne za menadžment rizikom i poboljšavanje bezbednosti informacija da bi se postiglirezultati u skladu sa ukupnom politikom i ciljevima organizacije
Uraditi (implementirati i primenjivati ISMS) - **DO**	Implementirati i primenjivati ISMS politiku, kontrole, procese i procedure
Proveravati (pratiti i preispitivati ISMS) - **CHECK**	Ocenjivati, i kada je primenljivo, meriti performanse procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo i izveštavati o rezultatima koji se odnose na preispitivanje od strane rukovodstva
Delovati (održvati i poboljšavati ISMS) - **ACT**	Preduzimati korektivne i preventivne mere, zasnovane na rezultatima interne provere ISMS-a i preispitivanjima od strane rukovodstva ili drugim relevantnim informacijama, za postizanje stalnog poboljšanja ISMS-a

Organizacija mora da dokumentovani ISMS u kontekstu ukupne poslovne aktivnosti organizacije i rizika sa kojima se suočava:

- Uspostavi
- Implementira i primenjuje
- Prati i preispituje
- Održava i poboljšava

Orgaizacija mora da:

- **Definiše područje primene i granice ISMS-a u odnosu na karakteristike poslovanja, organizaciju, njenu lokaciju, imovinu i tehnologiju uključujući i detalje o svim izostavljanjima i obrazloženjima za ta izostavljanja iz područja primene**

- **Definiše politiku ISMS-a u odnosu na karakteristike poslovanja, organizaciju njenu lokaciju, imovinu i tehnologiju koja**:

  a) obuhvata okvir za postavljanje ciljeva i uspostavljanje opšteg pravca i principa za aktivnosti u odnosu na bezbednost informacija

  b) uzima u obzir poslovanja i zahteve iz zakona i propisa i ugovorne obaveze koje se odnose na bezbednost

  c) je usaglašena sa strateškim menadžmentom rizikom u organizaciji u kojoj će se organizovati uspostavljanje i održavanje ISMS-a

  d) uspostavlja kriterijume u odnosu na koje će se rizik proceniti

  e) je odobrena od strane rukovodstva

- **Definiše pristup ocenjivanju rizika u organizaciji**

  a) identifikuje metofologiju ocenjivanja rizika koja odgovara ISMS-u i da identifikuje poslovnu bezbednost informacija, zahteve zakona i propisa

  b) razvije kriterijum za prihvatanje rizika i identifikuje prihvatljive nivoe rizika

- **Identifikuje rizike**

  a) identifikuje imovinu unutar područja primene ISMS-a i vlasnike te imovine

  b) identifikuje pretnje za tu imovinu

  c) identifikuje ranjivosti koje mogu nastati usled pretnji

  d) identifikuje uticaje koje gubitak poverljivosti, integriteta i raspoloživosti mogu imati na imovinu

- **Analizira i procenjuje rizike**

  a) ocenjuje poslovne uticaje na organizaciju koji mogu da proisteknu iz otkaza bezbednosti, imajući u vidu posledice gubitka poverljivosti, integriteta ili raspoloživosti imovine

  b) ocenjuje realnu verovatnoću pojave otkaza bezbednosti uzimajući u obzir preovlađujuće pretnje ranjivosti, uticaje povezane sa tom imovinom i već implementirane kontrole

  c) proceni nivoe rizika

  d) odredi kada su rizici prihvatljivi ili se zahteva postupanje sa njima tako što će se koristiti uspostavljeni kriterijumi za prihvatanje rizika

- **Identifikuje i proceni opcije za postupanje sa rizicima**

  Moguće mere: a) primena odgovarajućih kontrola

  b) prihvatanje rizika sa punim znanjem i objekivno, obezbedjujući da oni jasno zadovoljavaju politike organizacije i kriterijume za prihvatanje rizika

  c) odredi nivoe i kada su rizici prihvatljivi ili se zahteva postupanje sa njima tako što će se korsititi uspostavljeni kriterijumi za prihvatanje rizika

ISO 27001 standard – uspostavljanje (nastavak)

- **Izabere ciljeve kontrola i kontrole za postupanje sa rizicima**
- **Dobije odobrnje rukovodstva za predloženi preostali rizik**
- **Dobije autorizaciju rokovodstva za implementaciju i primenu ISMS-a**

Organizacija mora da:

- **Formuliše plan postupanja sa rizikom u kojem su identifikovane odgovarajuće mere rukovodstva, resursi, odgovornosti i prioriteti za upravljanje rizicima za bezbednost informacija**
- **Implementira plan postupanja sa rizikom kako bi se dostigli identifikovani ciljevi kontrola, koji obuhvata razmatranje finansiranja i podelu uloga i odgovornosti**
- **Implementira kontrole na osnovu ciljeva i kontrole za postupanje sa rizicima**
- **Definiše kako se meri efektivnost izabranih kontrola ili grupa kontrola i specificira kako se ta merenja koriste da bi se ocenila efektivnost kontrola i da bi se postigli uporedivi rezultati**
- **Implementira programe obuke i podizanja svesti**
- **Upravlja primenom ISMS-a**
- **Implementira procedure i ostale kontrole pogodne da omoguće trenutno otkrivanje događaja u vezi sa bezbednošću i odgovore na incidente i narušavanja bazbednosti**

Organizacija mora da:

- **Sprovede procedure za praćenje i preispitivanje i ostale kontrole radi:**

  a) brzog otkrivanja grešaka u rezultatima procesa

  b) brzog identifikovanja pokušaja i uspešnih narušavanja bezbednosti i incidenata

  c) omogućavanja rukovodstvu da odredi da li se bezbednosne aktivnosti dodeljene ljudima ili one koje implementiraju informacione tehnologije izvode kako se očekuje

  d) pomoći u otkrivanju događaja u vezi sa bezbednošću i na osnovu toga sprečavanja incidenata narušavanja bezbednosti koristeći pokazatelje

  e) određivanja da li su mere preduzete za rešavanje narušavanja bezbednosti efektivne

- **Preduzima redovna preispitivanja efektivnsoti ISMS-a uzimajući u obzir rezultate provera bezbednosti, incidente, rezultate merenja efektivnsoti, predloge i povratne informacije od svih zainteresovanih strana**

- **Meri efektivnost kontrola radi verifikacije da su zahtevi za bezbednost ispunjeni**
- **Preispituje ocenjivanje rizika u planiranim intervalima, preispituje preostali rizik i i dentifikuje prihvatljive nivoe rizika uzimajući u obzir promene:**

  a) organizacije

  b) tehnologije

  c) ciljeva poslovanja i procesa

  d) identifikovanih pretnji

  e) efektivnosti implementiranih kontrola

  f) spoljašnjih dogadjaja kao što su promene zakona i propisa, izmenjene ugovorne obaveze i promene u društvu
- **Sprovodi interne provere ISMS-a u planiranim intervalima**
- **Preduzima reodvno preispitivanje ISMS-a od strane rukovodstva da bi se obezbedilo dapodručje primene ostane odgovarajuće i da se identifikuju poboljšanja procesa ISMS-a**
- **Ažurira planove bezbednosti uzimajući u obzir rezultate praćenja i preispitivanja**
- **Zapisuje aktivnosti i događaje koji mogu imati uticaj na eketivnost ili performanse ISMS-a**

Organizacija mora redovno da:

- Implementira i identifikuje poboljšanja u ISMS-u
- Preduzima odgovarajuće korektivne i preventivne mere sa ciljem poboljšanja ISMS-a primenjujući znanja stečena iz iskustva o bezbednosti drugih organizacija i onih sopstvenih
- Saopštava mere poboljšanja svim zainteresovanim stranama onoliko detaljno koliko to odgovara okolnostima i ako je odgovarajuće dogovara kako nastaviti te aktivnosti
- Osigurava da poboljšanja dostignu predviđene ciljeve

Opšti zahtevi vezani za dokumentaciju:

- Dokumentacija mora da obuhvati zapise o odlukama rukovodstva, obezbedi da su aktivnosti sledljive prema odlukama rukovodstva i politici i da omogući da se zapaisani rezultati mogu ponoviti

- Neophodno je da se može demonstrirati odnos između izabranih kontrola prema rezultatima procesa ocenjivanja rizika i postupanja sa rizikom kao i ISMS politici i ciljevima

ISMS dokumentacija mora da obuhvati sledeće:

a) Dokumentovane izjave o ISMS politici i ciljevima
b) Područje primene ISMS-a
c) Procedure i kontrole za podršku ISMS-u
d) Opis metodologije ocenjivanja rizicima
e) Izveštaj o ocenjivanju rizika
f) Plan za postupanje sa rizikom
g) Dokumentovane procedure potrebne organizaciji da bi se omogućilo efektivno planiranje, primena i kontrola njenih procena bezbednosti informacija i opis kako se meri efektivnost kontrola
h) Zapise zahtevane ovim međunarodnim standardom
i) Izjavu o primenljivosti

Obaveze

Rukovodstvo more da obezbedi dokaze o svojoj opredeljenosti za uspostavljanje, implementaciju, primenu, praćenje, preispitivanje i poboljšavanje ISMS-a time što:

a) Uspostavlja ISMS politiku

b) Osigurava da su uspostavljeni ISMS ciljevi i planovi

c) Uspostavlja uloge i odgovornosti za bezbednost informacija

d) Informiše organizaciju o bažnosti ispunjavanja ciljeva bezbednosti informacija i usaglašenosti sa politikom bezbednosti informacija, njenoj odgovornosti prema zakonu i potrebi stalnog poboljšanja

e) Obezbeđuje dovoljne resurse za uspostavljanje, implementaciju, primenu, praćenje, preispitivanje, održavanje i poboljšavanje ISMS-a

f) Odlučuje o kriterijumima za prihvatanje rizika i prihvatljivih nivoa rizika

g) Osigurava da se sprovode internet provere ISMS-a

h) Sprovodi preispitivanja ISMS-a od strane rukovodstva

Menadžment resursima

Organizacija mora da definiše i obezbedi resurse potrebne za:

- Uspostavljanje, implementaciju, primenu, praćenje, preispitivanje, održavanje i podboljšavanje ISMS-a
- Osiguravanje da procedure o bezbednosti inforamcija podržavaju zahteve poslovanja
- Identifikovanje i ispunjavanje zahteva iz zakona i propisa i ugovornih obaveza koji se odnose na bezbednost
- Održavanje odgovarajuće bezbednosti ispravnom primenom svih implementiranih kontrola
- Izvođenje preispitivanja kada je nophodno i odgovarajuće reagovanje na razultate tih preispitivanja
- Kada se zahteva, poboljšavanje efikasnosti ISMS-a

Obuka, svest i kompetentnost

Organizacija mora da osigura da je osoblje kojem je dodeljena odgovornost definisana u ISMS-u kompetentno da ispunjava zahtevne dužnosti pomoću:

a) Definisanje neophodne kompetentnosti za osoblje koje obavlja poslove koje utiču na ISMS

b) Obezbeđivanje obuka ili preduzimanja drugih aktivnosti

c) Ocenjivanja efektivnosti preduzetih mera

d) Održavanje zapisa o orazovanju, obuci, veštinama, iskustvu i kvalifikacijama

ISO 27001 standard – preispitivanje

- Rukovodstvo mora da preispituje ISMS organizacije u planiranim intervalima (najmanje jedanput godišnje) da bi se obezbedila njegova stalna pogodnost, adekvatnost i efektivnost.
- Preispitivanje mora da obuhvati procenjene mogućnsoti za poboljšanje i potrebu za promenama ISMS-a uključujući politiku bezbednosti informacija i ciljeve bezbednosti informacija.
- Rezulati preispitivanj moraju biti jasno dokumentovani i zapisi se moraju održavati
- Preispitivanje se sastoji od: a) ulaznih elemenata
  b) izlaznih elemenata

Ulazni elementi

Ulazni elementi preispitivanja moraju da sadrže:

a) Rezultate provera ISMS-a i preispitivanja
b) Reagovanja zainteresovanih strana
c) Tehnike, proizvode i procedure koji mogu da se koriste u urganizaciji za poboljšanjepreformansi iefektivnosti ISMS-a
d) Status preventivnih i korektivnih mera
e) Ranjivosti ili pretnje neadekvatno uzete u obzir u prethodnom ocenjivanju rizika
f) Rezultate merenja efektivnosti
g) Dodatne mere proistekle iz prethodnih preispitivanja od strane rukovodstva
h) Bilo koje izmene koje bi mogle uticati na ISMS
i) Preporuke za poboljšavanje

Izlazni elementi

Izlazni elementi preispitivanja moraju da sadrže sve odluke i aktivnsoti koje se odnose na sledeće:

a) Poboljšavanje efektivnosti ISMS-a

b) Ažuriranje ocenjivanja rizika i plana postupanja sa rizikom

c) Izmene procedura i kontrola koje imaju uticaj na bezbednosti informacija, kada je potrebno, radi reakcije na unutrašnje i spoljašnje događaje koji mogu uticati na ISMS uključujući promene:

1. zahteva poslovanja
2. zahteva za bezbednost
3. procesa poslovanja koji utiču na postojeće zahteve poslovanja
4. zahteva iz zakona i propisa
5. ugovornih obaveza
6. nivoa rizika i/ili kriterijuma za prihvatanje rizika

d) Potrebe resurse

e) Poboljšanje načina na koji se meri efektivnsot kontrola

Organizacija mora stalno da boboljšava efektivnost ISMS-a korišćenjem:

a) politike bezbednosti informacija,
b) ciljeva bezbednosti informacija,
c) rezultata provera,
d) analize praćenja dogoađaja,
e) korektivnih i preventivnih mera,
f) preispitivanja od strane rukovodstva

Korektivne mere

Organizacija mora da preduzima mere za otklanjanje uzroka neusaglašenosti sa zahtevima ISMS-a da bi se sprečilo njihovo ponavljanje.

Dokumentovana procedura za korektivne mere mora da definiše zahteve za:

a) Identifikovanje neusaglašenosti
b) Određivanje uzroka neusaglašenosti
c) Vrednovanje potreba za merama koje će osigurati da se neusaglašenosti ne ponove
d) Određivanje i implementaciju potrebnih korektivnih mera
e) Zapisivanje rezultata preduzetih mera
f) Preispitivanje preduzetih mera

Preventivne mere

Organizacija more da preduzima mere za otklanjanje uzroka potencijalnih nusaglašenosti sa zahtevima ISMS-a da bi se sprečilo njihovo pojavljivanje.

Preduzete mere moraju da budu odgovarajuće uticaju potencijalnih problema.

Dokumentovana procedura za preventivne mere mora da definiše zahteve za:

a) Utvrđivnje potencijalnih neusaglašenosti i njihovih uzroka
b) Vrednovanje potrebe za merom da bi se sprečilo pojavljivanje neusaglašenosti
c) Određivanje i implementaciju potrebne preventivne mere
d) Preispitivanje preduzete preventivne mere

Prioritet preventivnih mera mora da se odredi na osnovu rezultata ocenjivanja rizika

FALA !!!