Sustav upravljanja sigurnošću informacija sukladno normi ISO/IEC 27001:2013 u financijskim institucijama

Sporiš, Danijel

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić
Specijalistički diplomski stručni studij
Projektni menadžment

DANIJEL SPORIŠ

SUSTAV UPRAVLJANJA SIGURNOŠĆU INFORMACIJA SUKLADNO NORMI ISO/IEC 27001:2013 U FINANCIJSKIM INSTITUCIJAMA

SPECIJALISTIČKI ZAVRŠNI RAD

Zaprešić, 2020. godine

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić
Specijalistički diplomski stručni studij
Projektni menadžment

SPECIJALISTIČKI ZAVRŠNI RAD

SUSTAV UPRAVLJANJA SIGURNOŠĆU INFORMACIJA SUKLADNO NORMI ISO/IEC 27001:2013 U FINANCIJSKIM INSTITUCIJAMA

Mentor:
dr. sc. Dragutin Funda, prof. v.š.

Student:
Danijel Sporiš

Naziv kolegija:
Strategijski menadžment

JMBAG studenta:
0200008477

SADRŽAJ

SAŽETAK

Zaštita informacija postaje sve značajnija u svakodnevnom poslovanju i životu, budući otkrivanje klasificiranih informacija može prouzročiti velike štete, bilo financijske, političke ili druge, te dovesti do bitno otežanih uvjeta poslovanja ili u potpunosti uništiti subjekt.

Namjera je stručnog završnog rada opisati sustav upravljanja sigurnošću informacija sukladno normi ISO/IEC 27001:2013, na praktičnom primjeru Financijske agencije, jer navedena norma omogućava unifikaciju pristupa i olakšava postupanja savjetnika za informacijsku sigurnost i sigurnosnih koordinatora po organizacijskim cjelinama.

Ključne riječi: informacija, informacijska sigurnost, norma ISO/IEC 27001:2013, norma ISO/IEC 17799:2005, Fina.

TITLE IN ENGLISH: INFORMATION SECURITY MANAGEMENT SYSTEM IN ACCORDANCE WITH ISO/IEC 27001:2013 IN FINANCIAL INSTITUTIONS

ABSTRACT

Information security is becoming increasingly important in everyday business and life, as the disclosure of classified information can cause great damage, whether financial, political or otherwise, and lead to significantly more difficult business conditions or completely destroy the entity.

The intention of the professional thesis is to describe information security management system in accordance with ISO / IEC 27001: 2013, the case of FINA, since this standard allows unification of access and facilitates the actions of information security advisers and security coordinators by organizational units.

Keywords: information, information security, standard ISO/IEC 27001:2013, standard ISO/IEC 17799:2005, Fina.

1. UVOD

U današnjem svijetu informacija predstavlja jedno od najvećih bogatstava. "U informacijama je znanje, u znanju je moć. Čovjek iz informacija mora izvući znanje da bi mogao utjecati na svoju budućnost, budućnost ljudske zajednice, da bi znalački živio i radio, stvarao i poslovao, rješavao probleme, razvijao se te spoznavao sebe i svoje mikro i makrookruženje. Zato treba stalno učiti, promatrati informacije kao fenomen i kao izvor znanja o nečemu, treba naučiti pomoću njih stjecati znanje i spoznaje – o njima i o sebi, i o svemu drugome, treba se informacijama koristiti kao sredstvom za lakše, bolje i uspješnije djelovanje na svim područjima ljudskog zanimanja" (Javorović, Bilandžić, 2007).

Kad organizacija namjerava uvesti sustav upravljanja informacijskom sigurnošću, to znači da će ISMS u potpunosti biti usklađen sa Zakonom o informacijskoj sigurnosti (Narodne novine, broj 79/07), Zakonom o provedbi opće uredbe o zaštiti podataka (Narodne novine, broj 42/18), Uredbom o načinu pohranjivanja i mjerama tehničke zaštite posebnih kategorija osobnih podataka (Narodne novine, broj 139/04), kao i s međunarodnim normama ISO/IEC 27001:2013 i ISO/IEC 17799:2005.

U stručnom završnom radu opisuje se norma ISO/IEC 27001:2013 i radnje koje treba poduzeti prilikom uvođenja sustava upravljanja sigurnošću informacija.

Opisano je što organizacija treba učiniti u pojedinom koraku. Praktični način uvođenja opisuje utvrđivanje postojećeg stanja, organizacijskih promjena, definiranja opsega, definiranja sigurnosne politike i metodologije upravljanja rizikom te obaveze menadžmenta. Opisana je nužnost planiranja kontinuiteta poslovanja te temeljne sastavnice koje plan kontinuiteta poslovanja mora sadržavati.

U konačnici poduprijeti su razlozi uvođenja sustava upravljanja sigurnošću informacija s obzirom na moguće štete po organizaciju ukoliko se istom ne posvećuje potrebita pozornost.

2. ZAČECI NIZA NORMA ISO 27000

Začetkom današnjih niza norma serije ISO 27000 možemo smatrati zadaće koje su postavljene Centru za sigurnost komercijalnih računala (Commercial Computer Security Centre - CCSC) u sastavu britanskog Ministarstva trgovine i industrije. Centar za sigurnost komercijalnih računala dobio je zadaću stvaranja kriterija za sigurnosnu procjenu sigurnosnih proizvoda informacijskih tehnologija i stvaranja pravila dobre sigurnosne prakse za informacijsku sigurnost. Postavljeni kriteriji za sigurnosnu procjenu razvili su se u ono što je danas poznato kao IT sigurnost.

Postavljena pravila dobre sigurnosne prakse vodili su do objave dokumenta DISC PD 0003 koji je kasnije razvijan po Nacionalnom računalnom centru iz Manchestera i konzorciju korisnika računala. PD 0003 je bio organiziran u deset sekcija od kojih svaka naglašava skup ciljeva i kontrola te njegov format i sadržaj jako podsjećaju na današnju važeću ISO/IEC 27002 normu.

PD 0003 se nastavio razvijati pod nadzorom Britanske standardizacijske oorganizacije (British Standards Institution – BSI) te konačno 1995. godine postaje standard pod nazivom BS 7799. Paralelno s razvojem navedenog standarda BSI započinje razvoj novog standarda, specifikaciju sustava upravljanja informacijskom sigurnošću, odnosno BS 7799-2.

BS 7799-2, budući je bio u velikom suglasju s pristupom koji koriste ostale ISO specifikacije kao što je ISO 9000, 2005. godine biva prihvaćen kao ISO/IEC 27001 norma.

Približno u isto vrijeme kada započinje razvoj BS 7799-2, BS 7799 dolazi u fokus ISO-a te ubrzo, u prosincu 2000. godine, postaje ISO/IEC 17799 norma. Usprkos prihvaćanju u 2000. godini već slijedeće godine na sastanku ISO/IEC JTC 1/SC27 – IT Security Tehniques radne skupine u Oslu potiče se revizija. Tijekom narednih godina i sastanaka radnih skupina (Seoul 2001., Berlin i Waršava 2002., Quebec i Pariz 2003. godine) prikupljani su komentari i primjedbe. Nakon sastanka u Singapuru 2004. godine predložena je nova revidirana verzija norme. Nakon procesa ratifikacije konačno je u lipnju 2005. godine objavljena nova verzija norme ISO/IEC 17799.

U drugoj polovini 2007. godine, sa ciljem usklađivanja serijskih brojeva, ISO/IEC 17799 je preimenovana u ISO/IEC 27002.

3. UVOĐENJE SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA SUKLADNO NORMI ISO/IEC 27001:2013

"Usvajanje ISMS-a treba biti strateška odluka organizacije. Zamisao i primjena organizacijskog ISMS-a uvjetovani su njezinim potrebama i ciljevima, sigurnosnim zahtjevima, uključenim procesima te veličinom i strukturom organizacije." (Funda, 2012:114)

Norma ISO/IEC 27001:2013 razvijena je na temelju BS 7799-2 standarda. Prilikom uspostave sustava upravljanja sigurnošću informacija sukladnog smjernicama norme ISO/IEC 27001:2013, organizacija ili tvrtka koja želi uvesti sustav treba poduzeti sljedeće korake, podijeljene na nekoliko etapa.

3.1. USPOSTAVA SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

1. Odrediti opseg Sustava te opravdanje za sve što se isključuje iz ovog opsega.

2. Definirati Politiku Sustava.

3. Procjena rizika.

2. Identificirati rizike.

4. Analizirati i vrednovati rizike.

5. Identificirati i vrednovati opcije za obradu rizika.

6. Odabrati kontrolne ciljeve i kontrole za obradu rizika.

7. Dobiti odobrenje uprave za predložene rezidualne rizike.

8. Dobiti odobrenje uprave za implementaciju i izvršavanje ISMS-a.

9. Pripremiti Izjavu o primjenjivosti (SoA).

3.2. UVOĐENJE I PROVEDBA SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

Organizacija treba učiniti sljedeće.

1. Formirati plan za obradu rizika koji uključuje odgovarajuće akcije uprave, resurse, odgovornosti i prioritete za upravljanje rizicima informacijske sigurnosti.

2. Implementirati plan za obradu rizika kako bi se postigli odabrani kontrolni ciljevi, što uključuje razmatranje financiranja i raspodjele uloga i odgovornosti.

3. Implementirati odabrane kontrole kako bi se postigli kontrolni ciljevi.

4. Odrediti način mjerenja učinkovitosti odabranih kontrola ili grupa kontrola i definirati način na koji će ta mjerenja biti korištena u procjeni učinkovitosti kontrola, tako da rezultiraju usporedivim i ponovljivim rezultatima.

5. Pokrenuti program obuke i podizanja svijesti o informacijskoj sigurnosti,

6. Upravljati izvršavanjem Sustava.

7. Upravljati resursima.

8. Implementirati procedure i druge kontrole koje će omogućiti pravovremenu detekciju sigurnosnih događaja i odgovor na sigurnosne incidente.

3.3. NADZOR I PROVJERA SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

Organizacija treba učiniti sljedeće:

1. Nadzirati i provjeravati procedure i druge kontrole.

2. Izvoditi redovitu provjeru učinkovitosti Sustava (uključujući ispunjavanje politike i ciljeva te provjeru sigurnosnih kontrola) uzimajući u obzir rezultate sigurnosnih ispitivanja, incidente, rezultate mjerenja učinkovitosti, prijedloge i povratne informacije svih zainteresiranih strana.

3. Mjeriti učinkovitost kontrola kako bi se provjerilo da li su ispunjeni sigurnosni zahtjevi.

4. Provjeravati procjene rizika u planiranim intervalima i provjeriti rezidualne rizike te ustanovljene prihvatljive razine rizika.

5. Provoditi interna ispitivanja u planiranim intervalima.

6. Uprava treba redovito provoditi provjeru Sustava kako bi se osiguralo da je opseg i dalje primjeren i da su identificirana poboljšanja u procesima.

7. Nadopunjavati sigurnosne planove pri čemu treba uzeti u obzir rezultate ispitivanja i provjere Sustava.

8. Bilježiti akcije i događaje koji bi mogli imati utjecaj na učinkovitost i izvođenje Sustava.

3.4. ODRŽAVANJE I POBOLJŠAVANJA SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

Organizacija treba redovito činiti sljedeće:

1. Implementirati uočena poboljšanja Sustava.

2. Poduzeti odgovarajuće korektivne i preventivne mjere te primjenjivati znanja i iskustva iz drugih organizacija i iz vlastite organizacije.

3. Obavijestiti sve zainteresirane strane o aktivnostima i poboljšanjima s prikladnom detaljnošću te, prema potrebi, usuglasiti način daljnjeg postupanja.

4. Osigurati da poboljšanja postignu ciljeve.

3.5. POTREBNA DOKUMENTACIJA

Norma zahtjeva da se dokumentiraju odluke uprave, kako bi se poduzete akcije mogle uskladiti s politikama i odlukama uprave. Dokumentacija treba sadržavati:

1. Izjavu o sigurnosnoj politici i njezinim ciljevima.

2. Opseg Sustava.

3. Procedure i kontrole na koje se Sustav oslanja.

4. Opis metodologije za procjenu rizika.

5. Izvještaj o procjeni rizika.

6. Plan obrade rizika.

7. Procedure potrebne organizaciji za planiranje, održavanje i kontroliranje sigurnosnih procesa.

8. Izjavu o primjenjivosti.

4. PLANIRANJE SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

Prije samog kretanja u projekt implementacije Sustava upravljanja sigurnošću informacija treba se utvrditi stanje u organizaciji:

1. Jesu li temeljni poslovni procesi kvalitetno funkcioniraju te je li implementiran sustav upravljanja kvalitetom?
2. Je li sigurnost informacija relevantna za poslovanje u dovoljnoj mjeri (*integrity, availability, confidentiality*), dokumentirana/da li postoje iskustveni pokazatelji?
3. Sudjeluje li menadžment u projektu (uključujući najviše strukture upravljanja)?
4. Jesu li spremni učiti?
5. Je li formiran implementacijski tim koji može provesti promjene, određen proračun?
6. Ima li se dovoljno kvalitetnh ljudi koji ne rade ništa, pa možete *sami* provesti implementaciju?

Nakon što su utvrđeni rizici neispunjenja ovih čimbenika kreće se na implementaciju.

4.1. ETAPA IMPLEMENTACIJE

Nakon prepoznavanja vlastitih procesa kreće se na analizu rizika i klasifikaciju dobara zahtijevanih normom. Treba prepoznati informacijska dobra, prijetnje na ta dobra, izvore prijetnji te sukladno izračunatim rizicima definirati zaštitne mjere.

Kako bi se odredio prag na kojem se primjenjuju zaštitne mjere potrebno je napraviti *cost/benefit* analizu isplativosti primjene određene zaštitne mjere.

Kad se definira rizik u terminima vrijednosti za kompaniju – možemo definirati i cijenu nastupanja rizika u novčanim terminima. Usporedbom te vrijednosti i vrijednosti investicije u zaštitnu mjeru dolazimo do prihvatljive točke. Mora se imati na umu kako investicija nije samo izračun uloga u *hardware* već i troškovi implementacije.

Primjena zaštitnih mjera je zadnji dio izgradnje Sustava koji se svojim *Plan-Do-Check-Act* krugom neprestano nadopunjuje.

4.2. ORGANIZACIJSKE PROMJENE

Implementacija ima utjecaj na samu organizaciju. Međutim implementacija zahtjeva i neke formalne promjene. U samoj organizaciji moraju početi funkcionirati tijela koja će se baviti sigurnošću informacija.

Odbor ili tim za informacijsku sigurnost (eng. Information Security Committee): odlučuje o postojećim sigurnosnim rizicima i njihovom tretmanu.

Voditelj ili *manager* za informacijsku sigurnost (eng. Chief Information Security Officer – CISO) – uloga mu je slična ulozi *Quality managera* za ISO 9001 samo za područje sigurnosti.

Radna skupina za formuliranje politike (eng. Policy Formulating Workgroup) – za svaku novu zaštitnu mjeru definira se skupina koja će kreirati primjenjivu politiku – ovo nije stalno tijelo već se formira prema potrebi.

U svakoj organizacijskoj jedinici mora postojati osoba zadužena za aspekte sigurnosti kako bi sustav zaživio.

5. IZVEDBA I RAD SUSTAVA UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

Prema normi ISO/IEC 27001:2013, prvi korak u uspostavi sustava upravljanja sigurnošću informacija je definiranje opsega i granica Sustava. Opseg ovisi o karakteristikama poslovanja, organizaciji, njezinoj lokaciji, resursima i tehnologijama koje se upotrebljavaju.

Zaštita organizacije je bitna za uspjeh poslovnog procesa te se iz toga razloga uspostavlja i sustav upravljanja informacijskom sigurnošću. Svrha informacijske sigurnosti organizacije je izgradnja sustava koji u obzir uzima sve moguće sigurnosne rizike i prijetnje po informacijska dobra te implementacija i provedba svih zaštitnih mjera i postupaka koji umanjuju sve vrste neprihvatljivih sigurnosnih rizika i prijetnji.

Sustav upravljanja informacijskom sigurnosti organizacije će jasno definirati sve prihvatljive i neprihvatljive načine sigurnosnog ponašanja i odgovornosti. Informacijska sigurnost ima za cilj zaštitu zaposlenika, podataka, integriteta i ugleda organizacije od mogućih rizika i prijetnji.

Sukladno temeljnim principima informacijske sigurnosti posebna pažnja se pridaje i zaštiti:

- informacija i podataka, pohranjenih u bilo kojem obliku (usmena komunikacija, pismena komunikacija, sva ostala komunikacija bilo u elektroničkom, audio, video ili digitalnom obliku, uzorci, predmeti i dr.)

- računalnom *hardware*-u i *software*-u

- mrežnim sustavima

- korisnicima informacijskog sustava

- radnim procesima

- međuovisnostima.

5.1. SMJERNICE ZA DEFINIRANJE OPSEGA

Sa ciljem olakšavanja procesa definiranja opsega dobara koje Sustav upravljanja sigurnošću informacija treba obuhvatiti, korisno je prilikom definiranja polaznih vrijednosti učiniti sljedeće:

1. Dobro je napraviti slikovni prilaz ili dijagram organizacije kako bi se lakše definirao opseg.

2. Nužno je producirati dokument s opisom opsega. Dokument treba odgovarati slikovnom prikazu.

3. Dobro je napraviti popis sklopovske i programske opreme koja je uključena u opseg.

4. Ukoliko postoji složena mrežna infrastruktura koja je dio opsega, preporuča se izraditi mrežni dijagram.

5.2. DEFINIRANJE SIGURNOSNE POLITIKE

Sigurnosna politika treba odražavati stavove rukovoditelja i definirati koncept upravljanja sigurnosti informacija. Dokument politike treba sadržavati iskaze koje se odnose na:

1. Definicije sigurnosti informacija, njezine sveobuhvatne ciljeve i djelokrug te važnost sigurnosti kao temeljnog mehanizma dijeljenja informacija.

2. Stavove rukovoditelja, podržavajući ciljeve i principe informacijske sigurnosti u skladu s poslovnom strategijom.

3. Okvire uspostave kontrolnih ciljeva i kontrola, uključujući načela procjene rizika.

4. Jezgrovito objašnjenje sigurnosne politike, načela i standarda.

5. Suglasnost sa zakonodavnim, nadzornim i ugovornim zahtjevima.

6. Zahtjevima za educiranje po sigurnosti.

7. Posljedicama nepridržavanja pravila sigurnosne politike.

8. Definicije općih i specifičnih odgovornosti rukovoditelja informacijske sigurnosti, uključujući izvještavanje o sigurnosnim incidentima

9. Reference na dokumentaciju koja može podržati politiku.

Norma preporuča kako sigurnosna politika treba biti kratak dokument koji će se prenijeti svim članovima organizacije. Sigurnosna politika predstavlja krovni dokument u odnosu na sve ostale politike, standarde, smjernice i procedure. Dokument se treba referencirati na druge adekvatne politike, standarde, procedure i smjernice.

5.3. PROCES PROSUDBE VJEROJATNOSTI RIZIKA

Procjena rizika (eng. Risk Assesment) je prva faza procesa upravljanja sigurnosnim rizicima. Proces upravljanja sigurnosnim rizicima podrazumijeva:
- dentifikaciju rizika
- analizu rizika
- uklanjanje rizika.

Sa ciljem stvaranja uvjeta za pokretanje kontinuiranog poboljšanja u području informacijske sigurnosti kao i uklanjanja, prijenosa i smanjenja rizika ugrožavanja informacijske sigurnosti na prihvatljivu razinu, organizacija procjenjuje rizike i definira procedure, upute, normativne akte i druge interne propise kako bi se obradilo i kontroliralo sve aktivnosti koje mogu imati utjecaj na informacijsku sigurnost.

Procjena rizika vezana je isključivo uz određeni sigurnosni rizik za pojedino informacijsko dobro. Pod procjenom rizika podrazumijevamo detaljnu analizu svih prijetnji i ranjivosti, vjerojatnosti realizacije rizika i mogućih posljedica. Također, u postupku procjene rizika potrebno je provesti i *cost/benefit* analizu na temelju koje rukovodstvo organizacije donosi odluke o načinu na koji će se odgovoriti na identificirane sigurnosne rizike.

Procjena rizika je složen i zahtjevan postupak koji uključuje cjelokupan proces analize rizika i njegovog vrednovanja, na osnovu čega se odlučuje na koji način i gdje isti treba umanjiti. Cilj procjene rizika je identificirati informacijska dobra organizacije s pripadajućim prijetnjama i ranjivostima te na temelju toga odrediti sigurnosni rizik koji je prisutan u sustavu.

Unutar organizacije za potrebe prosudbe vjerojatnosti rizika za sigurnosne zahtjeve informacijskih dobara potrebno je utemeljiti skalu za vrednovanje rizika. Preporučljivo je

odabrati više od tri vrijednosti kako bi se izbjegla opasnost dodjele srednje vrijednosti većini dobara. Primjer skale prosudbe rizika dan je u tablici 1.

Tablica 1.: Prosudba vjerojatnosti rizika za sigurnosne zahtjeve informacijskih dobara organizacije (uradak autora)

Vjerojatnost	Stupanj	Napomena
Vrlo visoka	5	Informacijska dobra kod kojih je vrlo visoka vjerojatnost ranjivosti. Postojeće sigurnosne kontrole nisu dostatne, odnosno nisu dovoljno jake za sprečavanje iskorištavanja ranjivosti i čine vrlo vjerojatnim mogući prodor.
Visoka	4	Informacijska dobra kod kojih je visoka vjerojatnost ranjivosti. Postojeće sigurnosne kontrole nisu dostatne, odnosno nisu dovoljno jake za sprečavanje iskorištavanja ranjivosti i čine vjerojatnim mogući prodor.
Srednja	3	Informacijska dobra kod kojih je srednja vjerojatnost ranjivosti. Postojeće sigurnosne kontrole otežavaju iskorištavanje ranjivosti i mogući prodor.
Niska	2	Informacijska dobra kod kojih je niska vjerojatnost ranjivosti. Postojeće sigurnosne kontrole onemogućuju iskorištavanje ranjivosti i umanjuju mogući prodor.
Vrlo niska	1	Informacijska dobra kod kojih je vrlo niska vjerojatnost ranjivosti. Postojeće sigurnosne kontrole onemogućuju iskorištavanje ranjivosti i bitno umanjuju mogući prodor.

5.4. UČINAK PRODORA

Učinak prodora, odnosno moguće posljedice koje nastanu iskorištavanjem ranjivosti također će se izraziti stupnjevito, a pri tome je naročito važno voditi računa o:

a) Namjeni i ulozi dobara u poslovnom procesu odnosno funkciji koju informacijsko dobro ima u poslovnom procesu organizacije,
b) Kritičnosti informacijskih dobra i njegovom značaju unutar organizacije,
c) Osjetljivosti podataka i dobara, odnosno njihovoj povjerljivosti.

Potencijalni gubitci kao rezultat učinka prodora izraziti će se na sljedeći način (tablica 2.):

Tablica 2.: Prosudba potencijalnih gubitaka za sigurnosne zahtjeve informacijskih dobara organizacije (uradak autora)

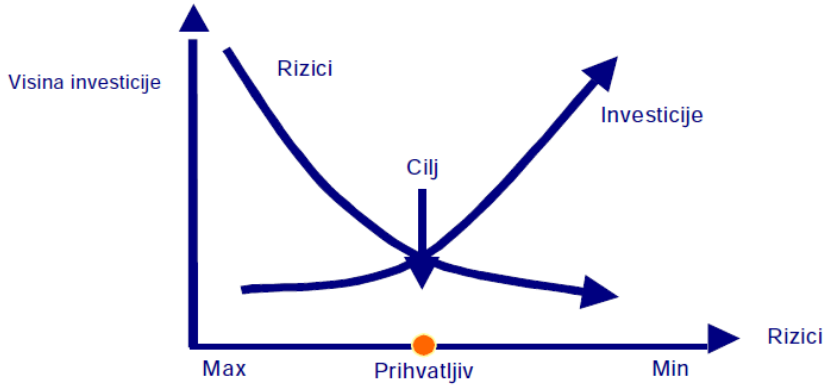
Gubitak	Stupanj	Napomena
Visok	3	Informacijska dobra kod kojih učinak prodora može uzrokovati trajni gubitak ili uništenje, dugotrajnu nesposobnost, veliku štetu u obavljanju svakodnevnih radnih procesa, ozbiljno ugrožavanje ljudskih resursa ili ozbiljan gubitak ugleda u javnosti.
Srednji	2	Informacijska dobra kod kojih učinak prodora može uzrokovati djelomični gubitak ili nesposobnost, djelomičnu štetu u obavljanju svakodnevnih radnih procesa ili djelomično ugrožavanje ljudskih resursa.
Nizak	1	Informacijska dobra kod kojih učinak prodora može uzrokovati lakše oštećenje, lakšu nesposobnost, manju štetu u obavljanju svakodnevnih radnih procesa ili lakše ugrožavanje ljudskih resursa.

5.5. PRIHVATLJIVI RIZIK

Neki od načina na koje je moguće umanjiti sigurnosne rizike jesu:

- umanjivanje rizika
- transfer rizika
- prihvaćanje rizika
- odbacivanje rizika.

Prihvatljiv rizik u organizaciji je onaj koji se prihvaća kao takav bez implementacije sigurnosnih kontrola. Ukoliko *cost/benefit* analiza (slika 1.) pokaže da je veći trošak ulagati u zaštitu informacijskih dobara nego što predstavlja njihov gubitak, tada se taj rizik prihvaća. Odluku o prihvaćanju pojedinog rizika donosi čelnik organizacije, a o svakom takvom riziku se obavezno sastavlja izvješće koje sadrži podatke o tome tko je za isti odgovoran i zašto sigurnosne kontrole nisu implementirane.



Slika 1. Utvrđivanje prihvatljivog rizika (Uradak autora)

U sklopu procjene rizika potrebno je provesti i vrednovanje dobara organizacije s obzirom na vrijednost koju ista predstavljaju za organizaciju. Primjer vrednovanja dobara organizacije s obzirom na moguće štete dan je u tablici 3.

Tablica 3.: Procjena vrednovanja informacijskih dobara organizacije (uradak autora)

Vrijednost	Stupanj	Napomena
Vrlo visoka	4	Vrijednost dobra je vrlo visoka, gubitak ili kompromitacija informacijskog dobra može predstavljati vrlo veliku materijalnu ili nematerijalnu štetu za organizaciju.
Visoka	3	Vrijednost dobra je visoka, gubitak ili kompromitacija informacijskog dobra može predstavljati veliku materijalnu ili nematerijalnu štetu za organizaciju.
Srednja	2	Vrijednost dobra je srednja, gubitak ili kompromitacija informacijskog dobra može predstavljati određenu materijalnu ili nematerijalnu štetu za organizaciju.
Niska	1	Vrijednost dobra je niska, gubitak ili kompromitacija informacijskog dobra predstavlja malu materijalnu ili nematerijalnu štetu za organizaciju.

5.6. PROCJENA RIZIKA

Procjena rizika započinje identifikacijom informacijskih dobara koja su u sklopu opsega Sustava upravljanja sigurnošću informacija. Svaki rizik promatra se na način procijene štete koja bi nastala ukoliko dođe do povrede povjerljivosti, integriteta, raspoloživosti i ostalih faktora koji su vezani na informacijsko dobro. Svakom narušavanju sigurnosti dodjeljuje se razina rizika određena njegovom vjerojatnošću i utjecajem na organizaciju.

Prikaz procjene rizika za najvažnija informacijska dobra organizacije dan je u tablici 4.

Tablica 4. Procjena rizika za najvažnija informacijskih dobara u organizaciji (uradak autora)

Informacijsko dobro	Povjerljiv	Integritet	Raspoloži	Napomena
Sklopovska oprema				Uključuje poslužitelje, vatrozide, osobna i prijenosna računala, mrežnu opremu, perifernu opremu i slično.
Programska oprema				Uključuje aplikacije, operativne sustave, pomoćne programe sustava, sigurnosne zakrpe i slično.
Podaci i dokumenti				Uključuje informacije u bilo kojem obliku, npr. pisanom, elektroničkom, video zapisi i slično.
Ljudski resursi				Uključuje sve zaposlenike koji na bilo koji način sudjeluju u procesu.
Komunikacije				Uključuje sve vrste komunikacija, npr. telefonske, elektroničku poštu i slično.
Općenito				Uključuje sve resurse koji se ne mogu svrstati u jednu od prethodnih kategorija, npr. vanjski partneri.

Ukupna vrijednost dobara (označava se s **AV** – eng. Asset Value*)* dobiva se kao maksimum vrijednosti resursa u odnosu na povjerljivost **C** (eng. Confidentiality*)*, integritet **I** (eng. Integrity*)* i raspoloživost **A** (eng. Availability*):*

$$AV = max\ (C, I, A)$$

Procijenjeni rizik je:

$$R = f\ (AV, P(T), I(T))\ ,$$ odnosno

$$R = AV^{*}\ P(T)^{*}\ I(T)$$

gdje je **R** oznaka za rizik resursa (eng. Risk*)*, **P(T)** oznaka za vjerojatnost (eng. Threat Probality*)*, a **I(T)** oznaka za gubitak odnosno posljedicu (eng. Threat Impact*).*

Dakle, minimalna vrijednost rizika iznosi:

$$Rmin = AVmin*P(T)min*I(T)min = 1*1*1 = 1,$$

Dok maksimalna vrijednost rizika iznosi:

$$Rmax = AVmax*P(T)max*I(T)max = 4*5*3 = 60.$$

Na temelju podataka koji se dobiju iz tablice prosudbe vjerojatnosti rizika za sigurnosne zahtjeve informacijskih dobara, ukupne vrijednosti informacijskih dobara i tablice potencijalnih gubitaka kreira se matrica rizika koja opisuje razine sigurnosnih rizika prisutnih u sustavu. Slijedom navedenoga dobiva se skala sigurnosnog rizika (tablica 5.) koja je definirana na sljedeći način:

Tablica 5.: Skala sigurnosnog rizika organizacije (uradak autora)

Skala sigurnosnog rizika		
Vrlo visoki rizik	45-60	Procijenjeni rizik je vrlo visok i nužno ga je umanjiti
Visoki rizik	30-45	Procijenjeni rizik je visok i nužno ga je umanjiti
Srednji rizik	15-30	Procijenjeni rizik je srednji
Nizak rizik	5-15	Procijenjeni rizik je nizak
Vrlo nizak rizik	1-5	Procijenjeni rizik je vrlo nizak

5.7. IZJAVA O POVJERLJIVOSTI

Izjava o primjenjivosti treba sadržavati:

1. Kontrolne ciljeve, kontrole i razlog njihovog odabira.

2. Kontrolne ciljeve i kontrole koje su već implementirane.

3. Sve kontrolne ciljeve i kontrole koje su isključene te razlog za njihovo isključenje.

Izjava o primjenjivosti pokriva sve vrste organizacija. Njime se definiraju zahtjevi za uspostavljanje, implementaciju, rad, nadzor, provjeru, održavanje i unapređivanje dokumentiranog sustava upravljanja sigurnošću informacija u kontekstu cjelokupnih poslovnih rizika organizacije. Izjava o promjenjivosti mora biti izrađena prije same revizije. Ovaj dokument pruža opravdanje o primjenjivosti ili neprimjenjivosti svake od ISO 27001 kontrola Sustava upravljanja sigurnošću informacija za koji se vrši revizija. Dokument također uključuje, ukoliko je već primijenjena, implementacijski status svake kontrole. U ovom dokumentu su označeni ciljevi, odabrane kontrole i razlozi za njihov odabir, kao i razlozi izuzimanja bilo koje od kontrola propisanih normom ISO 27001.

Dokument je rezultat upravljanja rizicima u sklopu planiranja sustava upravljanja informacijskom sigurnošću organizacije. Specificira koje mjere zaštite (nadzora) iz aneksa A norme su primjenjive za organizaciju obzirom na rezultate procjene rizika i druge važeće zakonske i podzakonske akte koji reguliraju ustroj i rad organizacije. Izvješće o primjenjivosti predstavlja temelj za provedbu mjera zaštite (kontrola) u praksi.

Cilj izjave o primjenjivosti je ispunjavanje zahtjeva norme te prelazak iz faze planiranja u fazu primjene pojedinih mjera zaštite u organizaciji. Dokument je namijenjen rukovodstvu, voditeljima organizacijskih jedinica, zaposlenicima organizacije i svima koji sudjeluju u planiranju, implementaciji i održavanju Sustava upravljanja sigurnošću informacija. Na temelju navedenog, ovlaštena osoba određuje primjerene mjere zaštite (kontrole) za zaštitu informacija.

5.8. PRIBAVLJANJE ODOBRENJA MENADŽERA

Posljednji korak u procesu izvedbe i rada Sustava upravljanja sigurnošću informacija predstavlja pribavljanje odobrenja rukovodstva organizacije. Isto se provodi nakon što je sva dokumentacija sastavljena i upotpunjena. Odobravanjem rukovodstvo potvrđuje kako je upoznato sa sustavima upravljanja informacijskom sigurnošću koji će se primjenjivati, kao i s načinom kontrole rizika, odnosno prihvaćenim rizicima.

Uobičajeno, dokaz svojeg opredjeljenja rukovodstvo organizacije će pružiti kroz:

1. Uspostavljanje politike Sustava upravljanja sigurnošću informacija.

2. Osiguranje da su uspostavljeni ciljevi i planovi Sustava upravljanja sigurnošću informacija.

3. Uspostavljanje odgovornosti i ovlaštenja za informacijsku sigurnost.

4. Obavještavanje svih zaposlenika organizacije o važnosti ispunjavanja ciljeva informacijske sigurnosti i usklađivanja s politikom informacijske sigurnosti, njihovim odgovornostima pred zakonom i potrebom za kontinuiranim poboljšanjem.

5. Osiguravanje dovoljno resursa potrebnih za uspostavljanje, implementaciju, rad, nadzor, provjeru, održavanje i unapređivanje Sustava upravljanja sigurnošću informacija.

6. Određivanje kriterija za prihvaćanje rizika i za prihvatljiv stupanj rizika.

7. Osiguravanje izvršavanja internih pregleda Sustava upravljanja sigurnošću informacija.

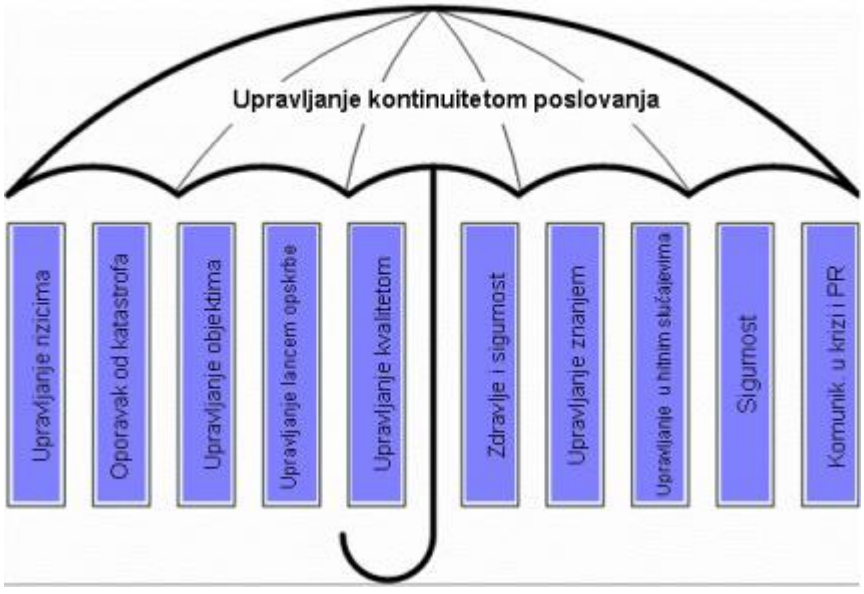
8. Provođenje ocjene Sustava upravljanja sigurnošću informacija.

6. PLANIRANJE KONTINUITETA POSLOVANJA

Osnovna ideja jest zaštititi informacije od izvora ugroze koje mogu biti prirodne (elementarne nepogode, gljivice, glodavci i slično), a zahtijevaju tehničke mjere zaštite i ljudskih (nenamjernih: neznanje, nepažnja, neodgovornost i namjernih: krađe, brisanje podataka, izmjena sadržaja) te tehničko-tehnoloških grešaka nastalih na opremi i objektima, a zahtijevaju organizacijske, edukacijske i softverske mjere zaštite.

Ni jedna organizacija nije imuna na prekide u poslovanju. Organizacije uglavnom nemaju spremne i testirane planove za slučaj prekida koji bi osigurali oporavak sustava, odnosno kontinuitet poslovanja. Prekidi u poslovanju, odnosno odvijanju poslovnog procesa povlače za sobom troškove te sprječavaju organizaciju u obavljanju uobičajenih aktivnosti, smanjuju prihode te rezultiraju prelaskom klijenata konkurentskim organizacijama

Uspostavu sustava upravljanja kontinuitetom poslovanja (eng. Business Continuity Management System, BCMS) (Slika 2.), moguće je provesti po normama BS 25999-1:2006 kodeks prakse i BS 25999-2:2007 specifikacija, koje se u poslovanje integriraju kao cjeloviti poslovni proces usklađen s potrebama i ciljevima organizacije.



Slika 2: BCMS – objedinjavanje procesa (uradak autora)

Faze uspostave BCMS-a uključuju:

1. Analizu zahtjeva za kontinuitetom poslovanja i utvrđivanje interesa (očekivanja) zainteresiranih strana.

2. Određivanje opsega sustava (projekta).

3. Dodjelu uloga i odgovornosti za BCMS (organizacijsko strukturiranje programa).

4. Analizu utjecaja na poslovanje (eng. Business Impact Analysis).

5. Procjenu i planiranje obrade rizika.

6. Određivanje strategija kontinuiteta poslovanja.

7. Razvoj BCMS reakcije / izradu planova kontinuiteta poslovanja.

8. Edukaciju, uvježbavanje i podizanje svijesti (eng. awareness) o kontinuitetu poslovanja.

9. Ispitivanje (uvježbavanje) planova kontinuiteta poslovanja.

10. Provjeru, održavanje i poboljšavanje BCMS-a.

Norma BS 25999 je objavljena u dva dijela:

1. BS 25999-1:2006 – propisuje pravila za upravljanje kontinuitetom poslovanja.

2. BS 25999-2:2007 – propisuje sustav upravljanja kontinuitetom poslovanja.

BS 25999-1 utvrđuje procese, načela i nazive za upravljanje kontinuitetom poslovanja pružajući osnovu za razumijevanje, razvoj i provedbu kontinuiteta poslovanja unutar organizacije.

BS 25999-2 utvrđuje zahtjeve za uspostavljanje, implementaciju, upravljanje, praćenje, reviziju, vježbanje, održavanje i unapređivanje dokumenata sustava upravljanja kontinuitetom poslovanja. Norma propisuje kako je potrebno odrediti potrebna znanja i vještine za osoblje, odrediti koje su obuke potrebne, provesti takve obuke, provjeriti da li su postignuta potrebna znanja i vještine te da je potrebno održavati zapise. BS 25999-2 također zahtijeva da se provode programi podizanja svijesti, ali i da se prema djelatnicima komunicira važnost upravljanja kontinuitetom poslovanja. Zahtjevi navedeni u BS 25999-2 namijenjeni su za sve organizacije (ili njihove dijelove) bez obzira na vrstu, veličinu i prirodu poslovanja. Opseg primjene tih zahtjeva ovisi o operativnom okruženju organizacije i složenosti.

Prema normama plan kontinuiteta poslovanja mora se sastojati od plana odaziva na incident i plana oporavka.

Osnovne faze izrade plana kontinuiteta poslovanja (slika 3.) obuhvaćaju pripremne aktivnosti i određivanje poslovnih zahtjeva koji se moraju osigurati očuvanjem kontinuiteta poslovanja. Započinje se analizom, odnosno izradom Politike kontinuiteta poslovanja na razini organizacije, a zatim slijedi ocjena rizika te analiza utjecaja neželjenih događaja na poslovne procese kao temelj za sve elemente plana koji se izrađuje u kasnijim etapama.

Slika 3.: Faze izrade plana kontinuiteta poslovanja (uradak autora)

Opcionalno, a u ovisnosti o dotadašnjem statusu planiranja kontinuiteta poslovanja u organizaciji, provodi se i početna ocjena stupnja usklađenosti sadašnjeg plana kontinuiteta poslovanja, poslovnih zahtjeva te prakse koja se u organizaciji provodi.

Drugi korak je donošenje strategije kontinuiteta poslovanja. Donosi se na razini cjelokupne poslovne cjeline te na razini pojedinih poslovnih procesa. Također, donosi se i strategija obnove kritičnih resursa nakon nepogode.

U trećem se koraku donosi plan kontinuiteta poslovanja te započinje njegova provedba. Planiraju se svi postupci za upravljanje kriznim situacijama te se donose planovi kontinuiteta poslovanja, kao i planovi za obnovu pojedinih poslovnih procesa. Ujedno, započinje i pripremna aktivnost za provedbu mjera koje se provode kod nastupanja izvanrednih situacija, kao i provedba svih preventivnih mjera.

Po donošenju planova, provodi se edukacija zaposlenika o planu kontinuiteta poslovanja unutar organizacije te priprema svih osoba koje sudjeluju u provedbi ovog plana.

Završni korak u provedbi plana kontinuiteta poslovanja je uvježbavanje svih postupaka te provjera stupnja pripremljenosti svih zaposlenika koji sudjeluju u provedbi plana. Ujedno, treba predvidjeti i promjenu plana kontinuiteta poslovanja uslijed bilo kakvih promjena unutar organizacije ili uslijed utjecaja na temelju promjena u poslovnom okruženju.

7. POLITIKA INFORMACIJSKE SIGURNOSTI FINANCIJSKE AGENCIJE

7.1. OKVIR POLITIKE

Financijska agencija *(u daljnjem tekstu***:** Fina), kao pravna osoba od posebnog državnog interesa, kroz povijest svog poslovanja, tradiciju i nacionalnu pokrivenost osigurala je poseban status među vodećim poduzećima u djelatnosti ostalih usluga financijskog posredovanja. Svoju snagu pokazuje u realizaciji velikih projekata u uslugama podrške državi, provedbi zakonskih odrednica, informatizaciji i unaprjeđenju državne administracije te pružajući svoja znanja i stručnost u elektroničkim, računovodstvenim, gotovinskim i drugim servisima. Fina je prvi partner državi i ključnim klijentima u provedbi nacionalnih projekata i reformi, a kompetencije svojih radnika stavlja u službu otvorenog pristupa građanima i poslovnim subjektima.

Temeljna odrednica Finina poslovanja, kao i razvoja financijskih usluga i proizvoda jest stvaranje dodatne vrijednosti za sve klijente, od banaka i poslovnih subjekata do građana, državnih tijela i jedinica lokalne samouprave.

Politikom Uprava izražava svoj stav da je informacijska sigurnost, kao područje sigurnosti, od strateškog značaja za Finu. Kako bi se informacije s kojima Fina postupa tijekom pružanja svojih usluga na primjereni način zaštitile, nužno je uspostaviti i održavati sustav informacijske sigurnosti prema normi ISO/IEC 27001.

Politika predstavlja polazište učinkovitog sustava informacijske sigurnosti te se njom iskazuje potreba za takvim sustavom, definiraju principi i okosnica sigurnosti, opći ciljevi sigurnosti, upućuje na način ostvarivanja ciljeva, postavlja okvir za sigurnosne mjere te način upravljanja.

Uprava Fine Politikom iskazuje svoju potpunu predanost zadovoljenju svih primjenjivih zahtjeva po pitanju informacijske sigurnosti, uključujući zakonske i ugovorne obveze te zahtjeve norme ISO/IEC 27001, kao i posvećenost kontinuiranom poboljšavanju sustava upravljanja sigurnošću.

Sigurnost, koja je predmet Politike, predstavlja sve aspekte povezane s definiranjem, postizanjem i održavanjem povjerljivosti, cjelovitosti, raspoloživosti cjelokupne imovine Fine. Kako bi se postigle i održavale sve navedene karakteristike sigurnosti, nužno je voditi brigu o cjelokupnoj imovini:

1. Informacije: informacije pohranjene u papirnatom obliku, informacije pohranjene u podatkovnim datotekama, baze podataka,
2. Programska oprema: aplikacije, sistemski i upravljački softver, pomoćni softver,
3. Fizička imovina: računalna i komunikacijska oprema, mediji, zgrade, prostorije, itd.
4. Usluge: interne i vanjske usluge,
5. Ljudski resursi: zdravlje, znanje, iskustvo i vještine osoblja,
6. Nematerijalna imovina: reputacija odnosno vanjska slika organizacije.

Nad imovinom postoje brojne prijetnje koje se mogu pojaviti uslijed organizacijskih propusta, nenamjernih i namjernih ljudskih postupaka i pogrešaka, tehničkih razloga, više sile, nesukladnosti s regulativom, politikama, procedurama i slično. Prijetnje, kao potencijalni uzrok neočekivanih i neželjenih sigurnosnih incidenata, mogu uzrokovati različite poslovne štete kao i prekid poslovanja.

Pojam sigurnosti označava zaštitu imovine od prijetnji kako bi se spriječili prekidi u operativnom radu, zlouporabe, pogreške i propusti te osigurao kontinuitet poslovanja i smanjili mogući rizici. Primjerena razina sigurnosti uspostavlja se primjenom odgovarajućih sigurnosnih mjera uvažavajući temeljne principe sigurnosti.

Temeljna načela sigurnosti jesu: poštivanje svih pravnih obveza i zahtjeva poslovne sukladnosti; procjena i postupanje s rizicima; definirane sigurnosne uloge i odgovornosti; uspostavljene potrebne suglasnosti unutar organizacije; definirani opći ciljevi; upravljanje životnim ciklusom sustava upravljanja informacijskom sigurnošću i kontinuirano poboljšavanje istog. Smjernice za izradu politike i principa sigurnosti, promicanje kulture sigurnosti te iniciranje aktivnosti unaprjeđenja sigurnosti na razini Fine daje Uprava.

Odabir sigurnosnih mjera proizlazi iz pravnih obveza (zakoni, uredbe, ugovori, drugi pravni akti), zahtjeva poslovnih sukladnosti, norme ISO/IEC 27001, procjene rizika informacijske sigurnosti te sigurnosnih zahtjeva koji proizlaze iz poslovne strategije. Fina redovito provodi

procjene rizika informacijske sigurnosti, a ostvarenje poslovne strategije uvjetovano je ostvarenjem sigurnosnih ciljeva.

Sigurnosni rizik je ugrožavanje povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine Fine te predstavlja mogućnost da neka prijetnja može iskoristiti moguću ranjivost, zbog čega mogu nastati poslovne štete.

Sa ciljem ostvarenja odgovarajuće razine sigurnosti, određene su sve potrebne sigurnosne uloge i odgovornosti, postavljeni su sigurnosni ciljevi te se provodi upravljanje svim važnim promjenama koje se događaju u okruženju ili proizlaze iz poslovne strategije Fine.

Kako bi imovina na primjereni način bila zaštićena od mogućih prijetnji, potrebno je uspostaviti, primijeniti i neprestano razvijati sustav informacijske sigurnosti temeljen na normi ISO/IEC 27001. Značaj ovog sustava od ključne je važnosti za Finu, jer se njime ostvaruju preduvjeti za očuvanje povjerljivosti, cjelovitosti, dostupnosti i pouzdanosti informacija, a time i poslovanja.

U svrhu navedenog Fina je uspostavila učinkoviti sustav sigurnosti koji će pružiti odgovarajuću razinu sigurnosti informacijske imovine Fine od prijetnji iz fizičkog i kibernetičkog prostora. Politika se primjenjuje u svim organizacijskim jedinicama Fine. Dio Politike koji se odnosi na sustav upravljanja informacijskom sigurnošću (ISMS Fine), primjenjuje se u opsegu istog.

7.2. OPĆI CILJEVI SIGURNOSTI

Opći ciljevi sigurnosti jesu:

- Postići visoku razinu svijesti o sigurnosti

Oblikovati i neprekidno podizati svijest o potrebi očuvanja sigurnosti imovine Fine. Poticati spoznaju da sigurnost proizlazi iz poslovne strategije Fine. Provoditi potrebna osposobljavanja u području primjene norma sustava sigurnosti. Prenijeti opće ciljeve sigurnosti na niže razine. Mjeriti njihova ostvarenja na odgovarajući način.

- Uspostava učinkovite organizacije sigurnosti u Fini

Oblikovati organizaciju sigurnosti na način da je učinkovita te da u cijelosti zadovoljava zahtjeve zakonske regulative i ISO/IEC 27001 norme po pitanju sigurnosti. Precizno definirati sigurnosne uloge, prenijeti ih na kvalificirane osobe te osigurati potrebna prava i resurse.

- Upravljanje sigurnosnim rizicima

Identificirati svu imovinu koja ulazi u opseg primjene sustava upravljanja informacijskom sigurnošću, klasificirati je, prepoznati prijetnje, vjerojatnosti ostvarenja i moguće posljedice. Identificirati rizike i odijeliti prihvatljive od neprihvatljivih rizika. Načiniti izbor potrebnih sigurnosnih mjera. Procijeniti preostale rizike po krovnoj *Metodologiji procjene i postupanja s rizicima* i *Proceduri upravljanja rizicima informacijske sigurnosti.* Potrebno je osigurati kontinuirano upravljanje rizicima.

- Uporaba učinkovitih sigurnosnih mjera

Odabir sigurnosnih mjera potrebno je provoditi uzimajući u obzir njihovu opravdanost, funkcionalnost i isplativost. Popis svih sigurnosnih mjera, primijenjenih na opseg naveden je u Izjavama o primjenjivosti (Statement of Applicability - SOA) svakog servisa koji je u opsegu sustava upravljanja informacijskom sigurnošću.

- Ostvarenje aspekata sigurnosti kontinuiteta poslovanja

Kvaliteta Fininih usluga nalaže visoku raspoloživost svih resursa koji u tome sudjeluju. Slijedom navedenog, nužno je osigurati odgovarajuće upravljanje sigurnosnim aspektima kontinuiteta poslovanja, kako bi se ključni dijelovi sustava zaštitili od mogućeg „efekta katastrofe" kao i od namjerno ili nenamjerno uzrokovane štete. Sigurnosne aspekte kontinuiteta poslovanja potrebno je kontinuirano nadzirati te provoditi potrebne prilagodbe.

- Sigurno postupanje s klasificiranim podacima

Sa svim podacima zaprimljenim od državnih tijela i klasificiranim prema *Zakonu o tajnosti podataka* postupa se sukladno zakonu i pripadajućom podzakonskom regulativom. Način postupanja propisan je *Pravilnikom o primjeni mjera informacijske sigurnosti u Financijskoj agenciji,* a osnovni je cilj u cijelosti zadovoljiti zakonsku regulativu i zaštititi klasificirane podatke.

- Sigurno postupanje s poslovnom tajnom

Podaci od osobitog interesa za Finu čije priopćavanje neovlaštenoj osobi može uzrokovati štetu za poslovanje, financijski gubitak, gubitak ugleda Fine te povrede zakona, drugih propisa i ugovora, predstavljaju poslovnu tajnu Fine te se s istima postupa se sukladno *Pravilniku o poslovnoj tajni.* Propisanim postupanjem postiže se primjerena razina sigurnosti poslovnih informacija.

- Zaštita osobnih podataka

Osobni podaci s kojima Fina postupa u svom poslovanju, štite se sukladno zakonskoj regulativi te internim aktima koji propisuju način postupanja s osobnim podacima. Fina izražava svijest, znanje i predanost za poštivanje prava i sloboda pojedinaca pri obradi osobnih podataka u svom poslovanju što je u funkciji zakonite obrade osobnih podataka.

- Kibemetička sigurnost

Učinkoviti sustav zaštite informacijskih sustava Fine i jačanje svijesti o ugrozama digitalnog okruženja primami je cilj sustavnih organizacijskih i tehničkih mjera koje će osigurati kibernetičku otpornost i zaštitu kibernetičkog okruženja Fininog poslovanja.

- Jačanje individualne odgovornosti za sigurnost .

Svi radnici i vanjski suradnici Fine koji su na bilo koji način uključeni u provedbu Politike odgovorni su za sigurnost imovine Fine koja im je povjerena.

- Uspostava učinkovite dokumentacije o sigurnosti

Sustav upravljanja sigurnošću mora biti odgovarajuće dokumentiran. Sve relevantne informacije o sustavu kao što su politike, procedure, radne upute, određeni zapisi, izvješća i drugo, moraju biti propisane te na odgovarajući način klasificirane i ažurne.

- Interne procjene - auditi

Potrebno je provoditi interne procjene kako bi se provjeravalo da se sustav upravljanja sigurnošću učinkovito koristi i neprekidno poboljšava.

Politikom se obvezuju odgovorne osobe u Fini da u svom djelokrugu rada provode opće ciljeve te ih učine mjerljivim i dostupnim neposrednim izvršiteljima.

Uprava Fine odgovorna je za uspostavu organizacije sigurnosti. Upravljanje sigurnošću kao i uloge i odgovornosti određene su *Odlukom o unutarnjoj organizaciji Financijske agencije.*

Uloge i odgovornosti za upravljanje informacijskom sigurnošću određene su dokumentom Organizacija informacijske sigurnosti Financijske agencije.

7.3. NAČIN REALIZACIJE

Uprava Fine je uspostavom učinkovite organizacije sigurnosti stvorila preduvjete za primjenu Politike kao i svih ostalih dokumenata koji iz nje proizlaze. Time je osigurala preduvjete za kontinuiranu provedbu poboljšanja u području sigurnosti te ostvarenje svih ciljeva sigurnosti.

Ciljeve sigurnosti potrebno je ostvariti primjerenim procjenama sigurnosnih rizika i identifikacijom neprihvatljivih rizika, temeljem čega se provodi odabir potrebnih sigurnosnih mjera. Prihvatljiva razina sigurnosnih rizika definirana je u *Metodologiji procjene i postupanja s rizicima.* Odabir sigurnosnih mjera provodi se uzimajući u obzir njihovu opravdanost, funkcionalnost i isplativost.

Sustav informacijske sigurnosti se temelji na zahtjevima norme ISO/IEC 27001 i Politikom Uprava iskazuje svoju potpunu predanost i potporu uspostavi, implementaciji te svakodnevnom funkcioniranju i unaprjeđenju sustava upravljanja informacijskom sigurnošću. Politika predstavlja temeljni okvir sustava sigurnosti i na temelju nje se donose ostali dokumenti sigurnosti u definiranom opsegu primjene.

Primjena sigurnosnih mjera mora biti usklađena s važećim zakonskim i ugovornim obvezama Fine. Pri tome se koriste i preporuke navedene u normi ISO/IEC 27002. Za svaku mjeru informacijske sigurnosti, propisanu Anexom A ISO/IEC 27001 norme, u Izjavi o primjenjivosti (SOA-i) mora biti jasno vidljivo je li ista implementirana u definiranom opsegu primjene te u slučaju da nije, koji su razlozi za to. Sve mjere koje su posljedica zakonske obveze ili poslovnih zahtjeva korisnika Fine, ne mogu se isključiti.

Sustav sigurnosti potrebno je kontinuirano nadzirati i provjeravati. Također, sustav informacijske sigurnosti je potrebno najmanje jedanput godišnje procjenjivati od strane internih procjenitelja. Sve informacije dobivene u postupku interne procjene treba koristiti za kontinuirano poboljšanje sustava informacijske sigurnosti. '

Uprava Fine se obvezuje osigurati potrebne resurse za razvoj, implementaciju, primjenu, nadzor, provjeru, održavanje i poboljšavanje sustava upravljanja informacijskom sigurnošću.

Uprava Fine najmanje jedanput godišnje provodi ocjenu sustava informacijske sigurnosti i nalaže mjere za poboljšanje.

Predsjednik Uprave odobrava Politiku kao i sve njene revizije. Odjel za informacijsku sigurnost upravlja Politikom, brine o redovitim provjerama njene aktualnosti najmanje jedanput godišnje, predlaže potrebne dopune i revizije te skrbi o dostupnosti važeće Politike svim radnicima Fine. Politika je objavljena na lntrawebu te je dostupna svim radnicima Fine. Po potrebi, zainteresiranim stranama Politika je dostupna u izjavnom obliku.

Nepridržavanje propisanih mjera informacijske sigurnosti prema Politici smatra se povredom obveza iz radnog odnosa sukladno važećim aktima Fine. U slučaju povreda odredbi Politike od strane ugovornih partnera i trećih strana primjenjuju se sigurnosne odredbe i odredbe o zaštiti tajnosti podataka iz ugovora s ugovornim partnerima i drugih akata kojima se trećoj strani omogućuje pristup imovini Fine.

8. UPRAVLJANJE RIZICIMA KONTINUITETA POSLOVANJA

8.1. PROCES UPRAVLJANJA RIZICIMA

Procedure upravljanja rizicima kontinuiteta poslovanja (u daljnjem tekstu: Procedura) definira proces upravljanja rizicima kontinuiteta poslovanja u okviru cjelokupnog upravljanja rizicima u Fini te opisuje način provedbe svih pojedinih faza tog procesa.

Cilj je osigurati jasne smjernice za provedbu procjene i postupanja s rizicima kontinuiteta poslovanja, poštujući sve ono što je po pitanju upravljanja rizicima definirano u *Metodologiji procjene i postupanja s rizicima u Fini.* Procedura se primjenjuje u opsegu implementiranog sustava upravljanja kontinuitetom poslovanja Fine (BCMS-a).

Rizik - učinak neizvjesnosti na postizanje zadanih ciljeva **(ISO 22301:2012)**
Apetit za rizik (risk appetite) - količina i tip rizika koji je organizacija spremna prihvatiti ili zadržati (ISO 22301:2012)

Procjena rizika - sveukupni proces identifikacije, analize i vrednovanja rizika **(ISO 22301:2012)** Upravljanje rizicima - koordinirane aktivnosti za upravljanje i nadzor koje organizacija provodi po pitanju rizika (ISO 22301:2012)

Cilj procesa upravljanja rizicima kontinuiteta poslovanja je upravljanje i kontrola nad rizicima koji narušavaju odvijanje prioritetnih procesa i aktivnosti Fine uslijed katastrofe ili velikog ispada, a koji su unutar opsega BCMS-a

Proces upravljanja rizicima kontinuiteta poslovanja slijedi *Politiku upravljanja rizicima. Načela upravljanja rizicima u Fini* i *Metodologiju procjene i postupanja s rizicima u Fini.* Sukladno potrebi detaljnije i preciznije identifikacije rizika kontinuiteta poslovanja, u okviru sustava upravljanja kontinuitetom poslovanja prema normi ISO 22301 (BCMS), propisana je Procedura.

Proces upravljanja rizicima kontinuiteta poslovanja uključuje sljedeće faze:

1. **Identifikacija rizika;** Prepoznavanje rizika koji narušavaju odvijanje prioritetnih procesa i aktivnosti Fine, definiranih unutar opsega BCMS-a, te ugrožavaju sustave, informacije, ljude, imovinu, usluge dobavljača i druge resurse koji podržavaju odvijanje tih procesa. Identifikacija rizika može proizaći iz: . . .

- *Specifičnih prijetnji,* koje se mogu opisati kao događaji ili aktivnosti koje mogu ugroziti aktivnosti i resurse (vatra, poplava, ispad napajanja, gubitak osoblja, virusi, kvar opreme i drugo)

- *Ometajućih incidenata,* koji mogu proizaći iz ranjivosti resursa (neodgovarajuća kontrola pristupa, neodgovarajuća zaštita od požara neodgovarajuća edukacija radnika, neodgovarajuća fizička sigurnost sistemskog prostora i drugo).

2. Analiza rizika: Razumijevanje prirode rizika i određivanje njegove razine.

3. Vrednovanje rizika: Određivanje koji od rizika narušavaju odvijanje prioritetnih procesa i aktivnosti Fine, te zahtijevaju implementaciju neke od opcija postupanja s rizicima.

4. **Identifikacija opcija postupanja s rizicima:** Određivanje opcija postupanja s rizicima koje mogu osigurati ostvarenje ciljeva kontinuiteta poslovanja i koje su u skladu s Fininim apetitom za rizik. Procjena rizika kontinuiteta poslovanja provodi se nad servisima u opsegu primjene sustava upravljanja kontinuitetom poslovanja u Fini.

Procjena rizika kontinuiteta poslovanja provodi se na radionicama koje organizira vlasnik servisa, odnosno nadležni rukovoditelj organizacijske jedinice koji je i odgovoran za upravljanje rizicima u svom djelokrugu rada. Procjena rizika kontinuiteta poslovanja provodi se jedanput godišnje te po većim promjenama u sustavu.

Koordinator upravljanja kontinuitetom poslovanja koordinira izradu i objedinjava sva izvješća o procjeni rizika kontinuiteta poslovanja i planove postupanja s rizicima od svih vlasnika rizika te iste dostavlja Predsjedniku Uprave na odobrenje.

8.2. RIZICI KONTINUITETA POSLOVANJA

Identifikacija rizika kontinuiteta poslovanja provodi se prepoznavanjem specifičnih prijetnji ili ometajućih incidenata. Temeljem prepoznatog, vlasnici servisa su dužni identificirati ključne rizike kontinuiteta poslovanja za njihov servis. Kao pomoć u identifikaciji rizika može se koristiti lista primjera scenarija rizika kontinuiteta poslovanja, koja se daje u nastavku:

- nedostupnost glavne lokacije pružanja servisa uslijed prirodne katastrofe - zemljotres
- nedostupnost glavne lokacije pružanja servisa uslijed prirodne katastrofe - poplava
- nedostupnost glavne lokacije uslijed terorističkog napada, pljačke ili blokade zgrade
- nedostupnost glavne lokacije pružanja servisa uslijed požara većih razmjera
- nedostupnost IT infrastrukture uslijed uništene IT infrastrukture na glavnoj lokaciji
- nedostupnost IT infrastrukture na glavnoj lokaciji uslijed kvara HW ili SW većih razmjera
- nedostupnost IT infrastrukture uslijed neovlaštenog upada u sustav/napada hackera virusa većih razmjera
- nedostupnost IT infrastrukture uslijed dugotrajnog ispada napajanja
- nedostupnost ključnih radnika Fine uslijed pandemije
- nedostupnost ključnih radnika Fine uslijed uličnih nemira, prosvjeda
- prekid ključnih usluga dobavljača.

Za identifikaciju rizika mogu se primijeniti alati koji su prilagođeni mogućnostima i potrebama u području procjene te koristiti raspoložive obrasce, dokumente i izvore informacija. U postupku identifikacije rizika kontinuiteta poslovanja sudjeluju osobe s odgovarajućim znanjem iz područja u kojem se provodi upravljanje rizicima.

U fazi analize rizika provodi se ocjena vjerojatnosti pojave rizika kontinuiteta poslovanja i njegovog utjecaja na ostvarenje ciljeva servisa. U postupku analize rizika potrebno je uzeti u obzir postojeće mjere za smanjenje odnosno ublažavanje rizika te njihovu efikasnost i učinkovitost.

Razina rizika određuju se na temelju sljedeće formule.

Razina rizika = Vjerojatnost ostvarenja rizika (scenarija) + Utjecaj na ostvarenje ciljeva servisa

Analiza rizika kontinuiteta poslovanja pruža ulazne podatke za fazu vrednovanja rizika i donošenje odluke o prihvatljivosti istog te primjeni odgovarajućih opcija postupanja s rizikom.

Vrednovanje rizika uključuje uspoređivanje razine određenog rizika kontinuiteta poslovanja ustanovljenog tijekom faze analize s kriterijima prihvatljivosti rizika, odobrenim od strane predsjednika Uprave, a definiranim matricom rizika,

Postupanje s rizicima kontinuiteta poslovanja uključuje izbor i implementaciju jedne ili više opcija utjecanja na rizik. Postupanje s rizicima, identificiranim u procesu procjene rizika, moguće je provesti kroz sljedeće opcije:

1. *Izbjegavanje rizika* - postupak koji podrazumijeva prekidanje ili nepokretanje aktivnosti unutar organizacije koje mogu izazvati određeni rizik. To se može primijeniti u slučaju kad se ukidanjem takvih aktivnosti ne utječe značajnije na rezultate poslovnih procesa organizacije ili kad postoji neki drugi način realizacije tih aktivnosti.
2. *Smanjenje rizika* - pristup koji podrazumijeva implementaciju odgovarajućih mjera za smanjenje odnosno ublažavanje rizika koje umanjuju identificirani rizik kroz:
    - uklanjanje izvora rizika,
    - promjenu vjerojatnosti pojave rizika,
    - promjenu utjecaja rizika na ostvarenje ciljeva servisa,

3. *Prenošenje rizika* - rizik i troškovi se prenose na treću stranu, primjerice osiguravajuću kuću ili dobavljača koji može preuzeti neki od prepoznatih rizika te pružiti podršku organizaciji u odvijanju određenog poslovnog procesa,

4. *Prihvaćanje rizika* - postupak kojim se identificirani rizik prihvaća bez implementacije ikakvih mjera za smanjenje odnosno ublažavanje rizika. Ovaj pristup se primjenjuje ukoliko analize pokažu da je veći trošak ulagati u zaštitu resursa, nego što predstavlja njegov gubitak.

Plan postupanja s rizicima kontinuiteta poslovanja vlasnik rizika dužan je iskomunicirati svim relevantnim zainteresiranim stranama.

9. PLAN KRIZNOG MENADŽMENTA I ODGOVORA NA KRIZNE SITUACIJE

Svrha plana kriznog menadžmenta i odgovora na krizne situacije je uspostava sustava nadležnosti i odgovornosti te definiranje procedura u slučaju krizne situacije (incidenta) većih razmjera Plan je izrađen neovisno o tipu, uzroku i opsegu incidenta, te obuhvaća široki spektar mogućih događaja. Opisani postupci dovoljno su općeniti da mogu biti primijenjeni u svim slučajeva Konkretne odluke o postupcima donose se na licu mjesta, a ovise o stanju na terenu - vrsti odnosno uzroku incidenta (požar, poplava, potres, teroristički napad i si.), širini zahvaćenog područja (dio zgrade čitava zgrada, zgrada s okolicom i si.), stupnju oštećenja, trajanju samoga incidenta i sličnome.

Cilj je plana ponajprije zaštita ljudi, a potom zaštita imovine, opreme, informacija i ostalih resursa te sprječavanje i ograničavanje štete. Također, cilj je uspostavljanje uvjeta za početak obnove kritičnih procesa i servisa, odnosno provođenje planova kontinuiteta poslovanja servisa i plana oporavka IT infrastrukture Fine u što kraćem vremenu. Za izradu i provedbu plana kriznog menadžmenta i odgovora na krizne situacije te njegovu reviziju odgovoran je koordinator upravljanja kontinuitetom poslovanja Fine.

Svakom timu određen je voditelj. Ukoliko voditelj tima nakon pojave incidenta iz bilo kojeg razloga nije dostupan, njegovu ulogu preuzima zamjenik ili najiskusniji raspoloživi član tima. Svi zaposlenici Fine trebaju imati pristup relevantnom planu evakuacije i spašavanja koji se objavljuje na intrawebu.

Po završetku evakuacije (u slučaju da je bila potrebna), odnosno nakon što zaposlenici više nisu izravno ugroženi, različiti zaposlenici preuzimaju zadatke vezano za brigu za zaposlenike, ograničavanje štete, procjenu štete i slično. Kontakt podatke vanjskih dobavljača, bitnih u slučaju incidenta i katastrofe većih razmjera posjeduju i vode članovi tima za incidente, svatko u svojoj domeni.

1. Odbor za krizni menadžment (Crisis Management Team)

Ukoliko je stanje na terenu takvo da obnavljanje kritičnih poslovnih funkcija unutar definiranog RTO-a nije izgledno, Odbor za krizni menadžment proglašava katastrofu.

Proglašavanje katastrofe automatizmom povlači aktiviranje planova kontinuiteta poslovanja u kojima su opisane procedure i postupci koji se primjenjuju u cilju obnove kritičnih poslovnih procesa i servisa te definirane uloge i odgovornosti pojedinaca.

Odbor za krizni menadžment koji se sastoji od predsjednika, zamjenika te članova je zadužen za proglašavanje katastrofe, aktivaciju planova za kontinuitet poslovanja, provođenje pojedinačnih procedura, te koordinaciju timova na terenu. Također, Odbor za krizni menadžment po potrebi donosi odluke na visokoj razini.

Ako je u pitanju neposredna opasnost za ljude i imovinu, potrebno je uzbuniti sve zaposlenike Fine i obavijestiti ih o prijetnji i neposrednoj opasnosti. Eskalacija u vezi informiranja sudionika BCMS-a i reakcije na kriznu situaciju provodi se na temelju neposredne odluke predsjednika Odbora za krizni menadžment, odnosno njegovog zamjenika.

Najvažnija zadaća Odbora je proglašavanje katastrofe, koje za sobom povlači aktivaciju BCP planova i Plana oporavka IT infrastrukture (DRP)!

Svi timovi odgovaraju izravno Odboru za krizni menadžment. Odbor za krizni menadžment okuplja se u kriznom stožeru s mogućnošću da članovi operativne koordinacije djeluju sa terena.

Predsjednik Odbora za krizni menadžment je predsjednik Uprave. Članovi Odbora za krizni menadžment su direktori Sektora, voditelj Ureda sigurnost, koordinator sustava upravljanja kontinuitetom poslovanja i koordinator sustava informacijske sigurnosti.

2. **Tim za odgovor na incidente (Incident Response Team)**

Ulogu Tima za odgovor na incidente preuzimaju rukovoditelji i imenovane osobe koje u djelokrugu rada opisu poslova upravljaju poslovnim i operativnim procesima i incidentima te se bave operativnom koordinacijom servisa. Voditelj Tima između ostalog sudjeluju sa članovima Odbora za krizni menadžment u aktivaciji pričuvnog sustava,

Voditelj Tima je direktor Sektora informatike Članovi Tima zaprimaju i evidentiraju informacije o incidentima iz svog djelokruga rada U slučaju da ga mogu riješiti, rješavaju ga interno i izvješćuju po postojećim procedurama **U slučaju da se** procijeni **da** se incident ne

može riješiti u predviđenom RTO, članovi Tima eskaliraju incident prema voditelju Tima za odgovor za incidente te po potrebi dalje prema Odboru za krizni menadžment.

Svaki incident je poseban, tako da ga je nemoguće unaprijed odrediti najprikladnije radnje koje je potrebno poduzimati u vremenu nakon izbijanja. Odluke o tome se donose na licu mjesta, a ovise o tipu incidenta, uzroku i području koje je incidentom zahvaćeno. Tim za odgovor na incidente ima zadaću razmjene informacija i nadzora nad razvojem situacije na terenu te u slučajevima kada je to moguće, zaustavljanja širenja incidenta.

3. HR tim (Human Resources Team)

Direktor Službe upravljanja ljudskim potencijalima je ujedno i voditelj HR tima. Zadužen je za evidenciju zaposlenika zahvaćenih incidentom, te komunikaciju sa zaposlenicima. Tim obavještava zaposlenike o odlukama koje donosi Odbor za krizni menadžment, situaciji na terenu i sličnome.

4. Tim za procjenu štete (Damage Assessment Team)

Tim za procjenu štete *(Damage Assessment Team)* obavlja inicijalnu procjenu štete i utvrđuje stupanj oštećenja imovine. Nadalje, Tim provodi procjenu je li moguće obnoviti kritične poslovne funkcije unutar RTO-a i obavještava Odbor za krizni menadžment o nalazima. Izvještaj Tima za procjenu štete ima veliku važnost prilikom odluke o proglašenju katastrofe.

U svrhu obnove lokacije i uspostave procesa na početnoj 100%-tnoj razini izvršenja, poziva se vanjskog procjenitelja iz osiguravajuće kuće da napravi procjenu štete i utvrdi stupanj oštećenja imovine. Direktor Sektora financijskog i strateškog upravljanja koji je voditelj Tima, koordinira procjenu štete i provodi postupak podnošenja odštetnog zahtjeva osiguravajućoj kući. Na temelju procjene određuje se očekivano vrijeme povratka na primarnu lokaciju (MAO) i poduzimaju daljnje aktivnosti za normalno poslovanje s primarne lokacije ili druge primjerene lokacije.

5. **Tim za mobilizaciju javnih službi**

Tim za mobilizaciju javnih službi je zadužen za prijavu incidenta i komunikaciju s javnim službama. Incident i svi relevantni podaci dojavljuju Državnoj upravi za zaštitu i spašavanje te Policijskoj upravi zagrebačkoj.

Voditelj Odjela za informacijsku sigurnost komunicira s javnim službama, a zamjenik voditelja Tima je direktor Službe sigurnosti.

6. **Tim za sigurnost i zaštitu imovine (Safety & Security Team)**

Tim za sigurnost i zaštitu imovine brine o sigurnosti imovine koja je u većem ili manjem obujmu zahvaćena incidentom. Zadaća je Tima da osigura odgovarajuću fizičku zaštitu imovine, opreme, te informacija zahvaćenih incidentom. Također, ovaj Tim surađuje s policijom i vanjskom tvrtkom koja radi održavanje i zaštitu imovine i zgrade u pogledu koordinacije sigurnosti. Direktor Službe sigurnosti koordinira poslove sigurnosti i zaštite imovine interno i prema vanjskim partnerima i institucijama.

7. **Tim za komunikaciju s javnošću**

Tim za komunikaciju s javnošću *(Public Relations Team)* zadužen je za redovito obavještavanje javnosti o situaciji na terenu, radnjama poduzetim u cilju zaustavljanja širenja incidenta, te obnove kritičnih poslovnih funkcija. Tim odlučuje o razini detalja s kojima upoznaje javnost.

Fina funkciju odnosa s javnošću obavlja kroz Ured Uprave i voditelja Ureda, a koordinaciju njihovog djelovanja u slučaju katastrofe provodi predsjednik Odbora za krizni menadžment. U slučaju njegove nedostupnosti, njegovu ulogu preuzima njegov zamjenik.

Izjave za medije daju samo za to ovlaštene osobe, kao što je regulirano internim aktima ili određeno odlukama Odbora za krizni menadžment. Ostalim zaposlenicima strogo je zabranjeno davati izjave. Izjave se pripremaju unaprijed, a trebale bi biti kratke, bez nepotrebnih detalja. Formulacije koje se koriste moraju biti jednostavne, istinite i

nedvosmislene sa informacijama o terminu sljedeće izjave. Izjavama se ne smiju iznositi lažne i neprovjerene informacije, ili u potpunosti odbiti odgovor na neko pitanje.

Tijekom incidenta mediji se mogu koristiti za prenošenje osnovnih informacija zaposlenicima. Eskalacija u vezi informiranja sudionika BCMS-a i reakcije na kriznu situaciju provodi se na temelju neposredne odluke predsjednika Odbora za krizni menadžment.

U pravilu se obavještavanje obavlja na način:

- neposredno obavještavanje osobnim kontaktom
- elektroničkim sredstvima (telefonom, e-mailom, Internet stranicama)
- obavještavanje okružnim pismom
- putem javnih sredstava obavještavanja.

8. Tim za komunikaciju sa zainteresiranim stranama

Tim za komunikaciju sa zainteresiranim stranama zadužen je za komunikaciju s većim korisnicima Fine. Korisnike se obavještava o incidentu te o radnjama koje se poduzimaju u cilju ponovnog uspostavljanja procesa i usluga. Popisima ključnih korisnika s kontaktima upravljaju poslovni sektori, svaki u svojoj domeni.

9. Komunikacije

U razdoblju nakon incidenta postoji velika vjerojatnost da uobičajeni komunikacijski kanali neće biti u funkciji. Zaposlenici se prilikom komunikacije neposredno nakon incidenta najčešće oslanjaju na uporabu mobilnih telefona ukoliko iste posjeduju. Kako se u periodu nakon većih incidenata često događa da mreže mobilne telefonije budu preopterećene te da uspostava poziva bude otežana ili nemoguća, dobra je alternativa komunikacija putem SMS poruka, jer je veća vjerojatnost uspješnog slanja poruke kroz preopterećenu mrežu. Također, moguće je pokušati uspostaviti personaliziranu komunikaciju putem mobilnih društvenih mreža te u slučaju potpune nedostupnosti mobilnih mreža, putem kućnih telefona.

U slučaju nedostupnosti ostalih komunikacijskih kanala, za prenošenje osnovnih informacija zaposlenicima mogu se iskoristiti mediji.

10.ZAKLJUČAK

Količina informacija koje nas okružuju u današnjem svijetu i činjenica kako je današnji život nezamisliv bez informacija te kako se poslovanje bazira na informacijskim sustavima neminovno je dovela do razvoja svijesti o potrebi zaštite informacija i informacijskih sustava. Svjedoci smo brojnih napada na informacijske sustave državnih organizacija, kompanija i tvrtki. Ovih napada nisu pošteđeni niti obični građani te su uobičajene krađe identiteta ili pristupnih kodova za bankarske račune. Navedena djela mogu prouzročiti veće ili manje štete, financijske gubitke, gubitak ugleda, gubitak poslovnih pozicija i političke posljedice.

Iako je uobičajeno vjerovanje kako najveća opasnost po informacijske sustave dolazi izvana, od napada zlonamjernih osoba – hakera, istraživanja pokazuju kako navedeni napadi sudjeluju u ukupnom broju napada u relativno malom broju.

Organizacije pri zaštiti informacijskih sustava pažnju ne mogu usmjeravati samo prema vanjskim prijetnjama, već i prema zlonamjernim zaposlenicima i drugim osobama zbog njihovih nenamjernih pogrešaka. Također, prisutne su i prijetnje od prirodnih i tehničko-tehnoloških uzroka koje također, zbog svoje brojnosti i posljedica, ne možemo zaboraviti. Navedeno iziskuje sveobuhvatan i sustavan pristup zaštiti informacija. Iako se mogu odabrati različiti pristupi, odabir sustava upravljanja informacijskom sigurnošću sukladan normi ISO/IEC 27001 nudi neke prednosti. Osim dobro dokumentiranih postupaka, provjerene razine sigurnosti i široke ponude konzultantskih tvrtki, uvođenje sustava po normi dovodi do podizanja ugleda, konkurentnosti i prihvaćanja u poslovnom svijetu.

U konačnici, uvođenjem sustava upravljanja sigurnošću informacija sukladnom normi ISO/IEC 27001:2013 osigurava se sukladnost s postojećim propisima o zaštiti podataka, marketinške i poslovne prednosti, financijske uštede i uvođenje reda u poslovanje.

11.POPIS LITERATURE

1. BS 7799-2:2002 Information security management. Specification with guidance for use.

2. BS 25999-1:2006 Business continuity management. Code of practice.

3. BS 25999-2:2007 Business continuity management. Specification.

4. Funda, D. (2012). Upravljanje kvalitetom, Velika Gorica, Veleučilište u Velikoj Gorici.

5. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.

6. ISO/IEC 27001:2013 Information technology – Security techniques – Code of practice for Information security controls (second edition)

7. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for Information security management.

8. Javorović B., Bilandžić M. (2007). Poslovne informacije i bussiness intelligence, Zagreb, Golden marketing-Tehnička knjiga.

9. Plan kriznog menadžmenta i odgovora na krizne situacije, 552001, od 8.1. 2020.

10. Politika informacijske sigurnosti financijske agencije 682001, od 26.2. 2018.

11. Procedura upravljanja rizicima kontinuiteta poslovanja, 686048 od 30.9. 2016.

12. Uredba o načinu pohranjivanja i mjerama tehničke zaštite posebnih kategorija osobnih podataka,Narodne novine, broj 139/04.

13. Zakon o informacijskoj sigurnosti, Narodne novine, broj 79/07.

14. Zakon o provedbi opće uredbe o zaštiti podataka, Narodne novine, broj 42/18.

12.POPIS TABLICA I SLIKA

13.IZJAVA

Izjava o akademskoj čestitosti

Ime i prezime studenta: Danijel Sporiš
Matični broj studenta: 02-010/18-I
Naslov rada: Sustav upravljanja sigurnošću informacija sukladno normi ISO/IEC 27001:2013 u financijskim institucijama

Svojim potpisom jamčim:

- Da sam jedini/a autor/ica ovog rada.
- Da su svi korišteni izvori, kako objavljeni, tako i neobjavljeni, adekvatno citirani i parafrazirani te popisani u bibliografiji na kraju rada.
- Da ovaj rad ne sadrži dijelove radova predanih na Veleučilište Baltazar Zaprešić ili drugim obrazovnim ustanovama.
- Da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio nastavnik.

Datum Potpis studenta

_____ _____

ŽIVOTOPIS

OSOBNE INFORMACIJE

Sporiš Danijel

Pristava 129, 49215 Tuhelj (Hrvatska)
098548247
danijel.sporis79@gmail.com

RADNO ISKUSTVO

Referent za poslove naplate osnova za plaćanje u poslovnoj mreži
Financijska agencija(Fina)

Zadaci i odgovornosti:

- Provjera formalne ispravnosti osnova za plaćanje
- Određivanje vrste osnove, te evidentiranje prema njenim elementima
- Zadavanje izračuna kamate i praćenje izvršenja naplate
- Izvještavanje stranaka sukladno propisima o razlozima nepodobnosti
- Praćenje razmjene poruke s bankama
- Obavljanje poslova vezanih uz zaštićena sredstva, otvaranje i zatvaranje zaštićenih računa

OBRAZOVANJE I OSPOSOBLJAVANJE

2000-2009

Stručni studij kriminalist

Visoka policijska škola u Zagrebu

1993-1997

Gimnazija Antuna Gustava Matoša, Zabok

OSOBNE VJEŠTINE

Materinski jezik: hrvatski

Strani jezici

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Govorna interakcija	Govorna produkcija	
engleski	B1	B1	B1	B1	B1

Stupnjevi: A1 i A2: Početnik - B1 i B2: Samostalni korisnik - C1 i C2: Iskusni korisnik
Zajednički europski referentni okvir za jezike

Digitalne vještine

SAMOPROCJENA				
Obrada informacija	Komunikacija	Stvaranje sadržaja	Sigurnost	Rješavanje problema
Iskusni korisnik	Iskusni korisnik	Iskusni korisnik	Iskusni korisnik	Samostalni korisnik

Digitalne vještine - Tablica za samoprocjenu

korištenje Microsoft Office paketa, Citrix

Vozačka dozvola B

Tečajevi Škola za strane jezike Sokrat (2010-2011)