METODE ZA PROCJENU RIZIKA U IMPLEMENTACIJI ISO/IEC 27001:2005 STANDARDA

RISK ASSESSMENT METHODS IN IMPLEMENTATION OF ISO/IEC 27001:2005 STANDARD

Dr. sc. Dževad Zečić
Ekonomski fakultet
Univerzitet u Zenici

Nedim Zečić, student
Elektrotehnički fakultet
Univerzitet u Sarajevu

REZIME
Cilj ovog rada jeste da pruži pojednostavljen i detaljan pregled metoda za upravljanje / procjenu rizika za upotrebu u malim i srednjim preduzećima, kao i vladinim organizacijama. Sve navedene metode su u skladu sa ISO 27001 standardom i primjer su dobre prakse za procjenu rizika prilikom implementacije ISMS-a (Sistema upravljanja informacionom sigurnošću), što je objašnjeno u uvodnom dijelu rada.

Ključne riječi: ISO 27001, ISMS, upravljanje rizikom, procjena rizika, IT sigurnost

SUMMARY
The aim of this document is to provide a simplified and comprehensive view of risk management / risk assessment methods for use within small and medium sized enterprises (SMEs), as well as in government agancies. Mentioned methods are in compliance with ISO 27001 standard and are examples of good practice of risk assessment in implementation of ISMS (Information security management system), which is described in introduction part.

Key words: ISO 27001, ISMS, risk management, risk assessment, IT security

1. UVOD

ISO 27001:2005 usvojen je kao međunarodna norma 15.10.2005. godine. ISO, kao krovna organizacija, većinu standarda preuzela je iz britanskog modela, pa se ovaj standard često dovodi u vezu sa britanskim BS 7799.
Uz ISO 27001 standard spominje se i ISO 27002:2007 (prijašnji naziv ISO 17799:2005) kao skup preporuka i smjernica izrađen prema najboljoj praksi. ISO 27001 kao krovni dokument sadrži popis zahtjeva obaveznih za certifikaciju i direktno se referencira na ISO 27002 kao skup smjernica i kontrola za realizaciju sigurnosti.

ISO 27001 pripremljen je na način da se odlično integriše sa poslovnim procesima organizacije i već postojećim standardima ISO 9001 i ISO 14001, te kroz prizmu poslovne opravdanosti upravlja procesima informacione sigurnosti u organizaciji. Ovaj standard je vrlo dobro prihvaćen jer osigurava fleksibilnost, definira upravljački okvir, a ne zadire u konkretnu tehničku implementaciju, što ga čini primjenjivim u različitim organizacijama.
ISO 27001 standard je prvi u porodici ISO 27000.

Popis standarda vezanih uz problematiku zaštite i sigurnosti informacionog sistema koji su već doneseni ili su planirani u narednom razdoblju su:

- ISO 27000 – Rječnik termina koji se koriste unutar ISO 27000 serije standarda;
- ISO 27001:2005 – Sistem upravljanja informacionom sigurnošću (ISMS);
- ISO 27002:2007– Kodeks postupaka za upravljanje informacionom sigurnošću;
- ISO 27003 – Vodič za implementaciju ISMS-a;
- ISO 27004 – Mjerenje i metrika efikasnosti sistema informacione sigurnosti;
- ISO 27005 – Upravljanje rizicima informacione sigurnosti (baziran na BS 7799-3);
- ISO 27006:2007 – Zahtjevi za postupkom analize i certificiranja standarda;
- ISO 27007 – Upute za analizu ISMS-a;
- ISO 27011 – Upute za uspostavu ISMS-a u telekomunikacionom sektoru;
- ISO 27031 – Specifikacije za ICT odjel pripremljenosti poslovnog kontinuiteta;
- ISO 27032 – Upute za cyber- sigurnost.

1.1. ISMS – Information Security Management System

Norma ISO/IEC 27001:2005 opisuje proces uvođenja sistema upravljanja informacionom sigurnošću (eng. Information Security Management System – ISMS). Takav proces pruža sistematski pristup upravljanju osjetljivim informacijama s ciljem očuvanja njihove sigurnosti.
Informaciona sigurnost je zaštita bilo kakvih informacija u svrhu očuvanja:

- **povjerljivosti** (eng. confidentiality) – osiguranje da je informacija dostupna samo onima koji imaju ovlašteni pristup istoj;
- **integriteta** (eng. integrity) – zaštita postojanja, tačnosti i kompletnosti informacije, kao i procesnih metoda;
- **raspoloživosti** (eng. availability) – osiguranje da autorizirani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva.

2. UPRAVLJANJE RIZIKOM

Upravljanje rizikom je proces kojim se potvrđuje poslovna opravdanost odabira sigurnosnih rješenja i kontrola koje će osigurati dovoljan nivo sigurnosti. Također, proces upravljanja rizikom omogućuje razvoj strategije i postavljanje ciljeva u području informacione sigurnosti.
Upravljanje rizikom uključuje tri procesa:

- procjenu rizika,
- umanjivanje rizika i
- evaluaciju rizika.

Proces upravljanja rizika omogućuje stvaranje ravnoteže između operativnog i ekonomskog troška zaštitnih mjera, te dobiti koja se ostvaruje zaštitom informacionih sistema i podataka. Dobro strukturirana metodologija upravljanja rizikom jedan je od ključnih faktora pri odabiru odgovarajućih sigurnosnih kontrola koje osiguravaju kontinuirano odvijanje poslovnih procesa.

3. PROCJENA RIZIKA

Procjena rizika je identifikacija i određivanje vrijednosti resursa zasnovanih na poslovnim potrebama organizacije. Odgovarajuća zaštita nužno zahtjeva procjenu vrijednost imovine ovisno o njihovoj važnosti za poslovni proces. U razmatranje treba uzeti u obzir zakonske i poslovne zahtjeve, posljedice (eng. impact), gubitka povjerljivosti, raspoloživosti i integriteta. Vrlo je teško preporučiti određenu metodu ili alat za procjenu rizika bez detaljnog poznavanja organizacije koja uvodi standard. Za razliku od ISO 27001, ISO/IEC 27005:2008 standard nudi propisanu metodu za analizu i procjenu rizika. ISO 27001 je fleksibilan standard i nudi mogućnost da organizacija primjenjuje čak i nekoliko metoda za procjenu rizika.

3.1. Metoda matrice predefinisanih vrijednosti

Jedna od fundamentalnih metoda jeste metoda matrice predefinisanih vrijednosti. Varijacija ove metode eksplicitno je navedena u dodatku standarda ISO/IEC 13335-3. Također varijacija ove metode se koristi i u BS 7799-3:2006. Ova metoda vrijednost fizičkog resursa procjenjuje u odnosu na trošak zamjene ili rekonstrukcije resursa (kvantitativna mjera). Taj trošak se zatim konvertuje u kvalitativnu skalu koja se upotrebljava za podatkovne resurse. Vrijednost programske opreme se procjenjuje isto kao vrijednost fizičkih resursa. Dodatno, ako neki aplikacijski program ima unutrašnje zahtjeve povjerljivosti, integriteta ili raspoloživosti, njegova vrijednost se procjenjuje kao i vrijednost podatkovnih resursa. Vrijednost podatkovnih resursa se određuje intervjuiranjem vlasnika podataka koji najbolje poznaju vrijednost i osjetljivost podataka.

Bitne pretpostavke kod određivanja vrijednosti podataka su:

- sadrži li podatak lične informacije;
- koje su zakonske i ugovorne obveze vezane za podatak;
- koji je ekonomski interes od podatka;
- znači li neraspoloživost podatka prekid neke poslovne aktivnosti;
- koji je financijski gubitak u slučaju kompromitiranja podatka i sl.

Ova metoda za procjenu rizika koristi tri parametra: vrijednost resursa, prijetnje i ranjivosti. Svaki od tih parametara promatra se u odnosu na moguće posljedice, dok se prijetnje promatraju u odnosu na odgovarajuće ranjivosti. Svi parametri se kvantificiraju proizvoljno. Informacije o vrijednosti imovine određuju vlasnici tih resursa.

AV – vrijednost resursa, imovine
V – ranjivost
T – prijetnja

Za određivanje vrijednosti resursa koristi se numerička vrijednosti u rasponu od 0 (mala) do 4 (vrlo velika), dok se za kvantifikaciju ranjivosti i prijetnji koristi raspon od 0 (nizak nivo) do 2 (visok nivo). Nivo rizika se određuje sumom vrijednosti parametara, tj.

$$\mathbf{R = AV + V + T}$$

Minimalna i maksimalna vrijednost procijenjenog rizika iznose:

$$\mathbf{R_{MIN} = AV_{MIN} + V_{MIN} + T_{MIN} = 0}$$

$$\mathbf{R_{MAX} = AV_{MAX} + V_{MAX} + T_{MAX} = 8}$$

Određivanje rizika nekog resursa se na kraju određuje tablicom predefiniranih vrijednosti. Vrijednost imovine se određuje u odnosu na sva tri atributa tzv. trojka (povjerljivost, integritet, dostupnost – PID (eng. CIA)). Rizik se na kraju procesa također klasificira. Naime cilj određivanja rizika je njegovo smanjivanje, prenošenje na „treću osobu“ ili prihvatanje.

Tabela 1. Tablica predefiniranih vrijednosti rizika

NIVO PRIJETNJE		NIZAK			SREDNJI			VELIKI		
NIVO RANJIVOSTI		N	S	V	N	S	V	N	S	V
VRIJEDNOST IMOVINE	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

3.2. Karakteristike ostalih metoda za procjenu rizika

Da bi se mogla osigurati implementacija i efikasan rad ISMS-a potrebno je napraviti optimalan odnos između procjenjene vrijednosti rizika i poslovnih zahtjeva organizacije. Kako je sam ISMS fleksibilan moguće je koristiti različite metode u procjenjivanju. U tabeli 2. prikazane su neke od metoda koje se danas koriste za procjenu rizika:

Tabela 2. Osnovne karakteristike ostalih metoda procjene rizika

Metoda:	Opis:	Ciljane organizacije:
CRAMM	CRAMM je metoda za analizu rizika razvijena od strane britanske vladine organizacije CCTA (Central Communication and Telecommunication Agency). Ovu metodu je teško primjeniti bez CRAMM alata. Danas je ova metoda u upotrebi u vladi Velike Britanije. Primjenjiva je u velikim organizacijama, koje mogu biti vladina tijela i u industriji.	Vladine organizacije Velike kompanije
A&K analiza	Metoda Afhankelijkheids- en Kwetsbaarheidsanalyse (A&K analiza) je razvijena od strane danske kompanije RCC. Dansko ministarstvo unutrašnjih poslova je prvi subjekt koji je koristio metodu 1996. godine. Metoda je od tada ostala nepromijenjena. A&K analiza je preferirana metoda danskih vladinih tijela od 1994. godine i od danskih kompanija.	Vladine organizacije Velike kompanije Mali i srednji privredni subjekti
MAGERIT	Magerit predstavlja otvorenu metodologiju za upravljanje i analizu rizika, razvijenu od strane španskog ministarstva vanjskih poslova. Ova metoda je ponuđena kao framework i vodič za srodne institucije. Magerit ima sljedeće ciljeve: • Stvoriti svijest kod odgovornih za informacione sisteme o postajanju rizika i potrebi da se na ovakve rizike na vrijeme odgovori; • Pruziti sistematsku metodu za analiziranje rizika;	Vladine organizacije Velike kompanije Mali i srednji privredni subjekti

	• Pomoci u definisanju i planiranju odgovarajućih mjera da bi se rizici držali pod kontrolom; • Inidirektno pripremiti organizacije za evaulaciju, kontrolu, certifikaciju ili akreditaciju procesa.	
MARION	Metodu MARION (Methodology of Analysis of Computer Risks Directed by Levels) su razvili CLUSIF (Club de la Sécurité de l'Information Français) i zadnja nadopuna je urađena 1998. godine. Bazirana je na procedurama kontrole, koje omogućavaju da se estimira nivo IT sigunosnih rizika, kroz balansirano intervjuiranje različitih subjekata vezanih za sigurnost organizacije. Nivo sigurnosti se estimira kroz 27 pokazatelja razvrstanih u 6 grupa. Svaki pokazatelj dobiva ocjenu od 0 do 4. Ocjena 3 se smatra nivoom ispravne sigurnosti. Kako CLUSIF ne sponzorira više ovaj projekat MARION je zamijenjena MEHARI metodom, iako je MARION još uvijek u upotrebi u nekim kompanijama.	Velike kompanije
Mehari	• Pruža model upravljanja rizikom, modularne komponente i procese • Uključuje klasifikaciju procjena - otkriva ranjivosti kroz kontrolu • Analizira rizične situacije • Analiza bazirana na matematskom modelu • Omogućava optimalan izbor korektivnih mjera • Postavlja dodatne mjere na ISO 27002	Vladine organizacije Velike kompanije Mali i srednji privredni subjekti
MIGRA	MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale) je kvalitativna metoda upravljanja i procjene rizika koja je pogodna i za informacione i za fizičke resurse. Metoda pruža analitički framework baziran na klasičnoj viziji rizika kao multidimenzionalnog entiteta koji ovisi o tri pitanja: a) Koji resurs može biti kompromitovan? b) Koliko je vjerovatnoća kompromitovanja resursa? c) Koje se poljedice kompromitovanja? MIGRA definiše: • Taksonomiju sigurnosti i rizika za dvije razmatrane domene (fizički i	Vladine organizacije Velike kompanije

	informacioni resursi); • Framework za generisanje modela sigurnosnog opsega koji će se analizirati; • Algoritam (baziran na anketiranju) za procjenjivanje, sa 4 nivovskom skalom (visoko, srednje, nisko, neprimjenjivo); • Šemu za provođenje analiza prijetnji i ranjivosti; • Proceduru za proračunavanje rizika; • Mehanizam za identifikaciju svakog mogućeg scenarija i skupa pripadajućih sigurnosnih mjera; • Proceduru za obavljanje analiza propusta, sa akcentom na korporativne sigurnosne politike, normative, standarde, vodiče i najboljom praksom.	

4. LITERATURA

[1] Technical Department of ENISA Section Risk Management, Mr. George Patsis: ENISA Deliverable: Information Package for SMEs With examples of Risk Assessment / Risk Management for two SMEs, 2007.,

[2] Brian Honan: Implementing ISO27001 in a Windows Environment, 2009.,

[3] Stephen Ryan, Kurt Dillard, Jared Pfost: Microsoft Solutions for Security and Compliance, The Security Risk Management Guide, 2006.