MEHARI 2010

Pregled

Mart 2010.godine

Radna grupa za metodologiju

Molimo da vaše komentare i pitanja ostavite na forumu:
http://mehari.info/

UDRUŽENjE ZA INFORMACIONU BEZBEDNOST FRANCUSKE

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador, 75009 PARIS
Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88 – e-mail: clusif@clusif.fr
Web: http://www.clusif.fr

MEHARI brend registrovan od strane CLUSIF-a..

Zakon od 11. marta 1957. godine, u skladu sa stavkama 2. i 3. člana 41., odobrava samo na jednoj strani "kopiju ili reprodukciju, strogo su rezervisane za ličnu upotrebu korisnika i nisu namenjeni za kolektivno korišćenje", a sa druge strane, analiza i kratkih citata u svrhu primera i ilustracija "bilo kao predstavljanje ili potpuna ili delomično umnožavanje, napravljeno bez odobrenja autora ili prava stranaka ili zakonskih naslednika je nedopuštena" (prvi stav člana 40).
Ova reprezentacija ili umnožavanje, u kakvom god procesu, predstavljaće krivotvorenje i plagijat po članu 425 i povlači odgovorajuću kaznu.

ZAHVALNOST

CLUSIF se specijalno zahvaljuje gospodinu Žan Filipu Žoasu (Jean-Philippe Jouas) za njegov izuzetan doprinos, gospodinu Aleksandru Bratiću (za sve sugestije oko ovog prevoda možete poslati direktno na e-mail acobratic@yahoo.com) za ovaj prevod i gospodinu Zoranu Jasaku za korekciju prevoda, kao i članovima Komisije za metodologiju koji su učestvovali u realizaciji ovog dokumenta:

Jean-Philippe	Jouas	Odgovoran za provođenje Metode Odgovoran za radne principe grupe, mehanizme i bazu znanja za MEHARI
Jean-Louis	Roule	Odgovoran za radnu grupu MEHARI dokumentacija
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost
Martine	Gagné	HydroQuébec
Moïse	Hazzan	Ministarstvo usluga Vlade Kvebeka (Ministère des Services Gouvernementaux du Québec)
Gérard	Molines	Molines Consultants
Chantale	Pineault	AGRM
Luc	Poulin	CRIM
Pierre	Sasseville	Ministarstvo usluga Vlade Kvebeka (Ministère des Services Gouvernementaux du Québec)
Claude	Taillon	Ministarstvo obrazovanja, rekreacije i sporta Kvebeka (Ministère de l'Éducation, du Loisir et du Sport du Québec)
Marc	Touboul	BULL SA

Sadržaj

1. UVOD

MEHARI metodologija je napravljena i neprekidno se aktuelizuje da bi služila kao pomoć šefovima službe informacione bezbednosti (Chief Information Security Officers - CISO) pri obavljanju svakodnevnih zadataka i pri upravljanju informacionom bezbednošću. Ovaj pregled je namenjen šefovima službi informacione bezbednosti (CISO), ali takođe i revizorima, rukovodiocima informacionih sistema (CIO), ili risk menadžerima koji dele uglavnom iste ili slične probleme ili izazove.

Cilj ovog dokumenta je da opiše kako se MEHARI koristi. Detaljniji opisi metodologije i odgovarajućih alata nalaze se u drugim dokumentima dostupnim iz Kluziva (CLUSIF-a.):

- MEHARI: Koncept i funkcionalne specifikacije,
- MEHARI vodič:
    - analiza uloga i klasifikacija,
    - procena servisa sigurnosti i
    - analiza rizika,
- MEHARI Referentni priručnik službe sigurnosti,
- MEHARI baza znanja.

Glavni cilj MEHARI-JA je da obezbedi procenu rizika i metod upravljanja u domenu bezbednosti informacija, u skladu sa zahtevima ISO/IEC 27005:2008 standarda, kao i da obezbedi skup alata i elemenata neophodnih za sprovođenje standarda[1].

Dodatni ciljevi su:

- Obezbeđivanje direktne i individualne analize rizičnih situacija opisanih u scenarijima,
- Obezbeđivanje kompletnog seta alata koji je specifično dizajniran za upravljanje bezbednošću na kratak, srednji i dugi rok, i koji je prilagodljiv različitim akcijama i terminima završetka.

Svakako, MEHARI obezbeđuje konzistentnu metodologiju sa odgovorajućom bazom znanja kako bi bio od pomoći šefovima službi informacione bezbednosti, generalnim menadžerima, menadžerima bezbednosti ili ljudima koji su zaduženi za upravljanje rizicima u njihovim svakodnevnim zadacima i aktivnostima.

Povezanost MEHARI-ja sa ISO/IEC 27000 opisana je na kraju dokumenta.

[1] Alati i prateća sredstva, koje obezbeđuje MEHARI opisani su i nabrojani u dokumentu *MEHARI: koncept i funkcionalna specifikacija*

2. UPOTREBA MEHARI-JA

MEHARI je iznad svega metod za procenu i upravljanje rizikom.

U praksi, ovo znači da su MEHARI i baza znanja koja stoji iza njega dizajnirani za preciznu analizu rizika i rizičnih situacija opisanih kroz scenarija.

U svakodnevnim aktivnostima, upravljanje informacionom bezbednošću je aktivnost koja se menja i evoluira tokom vremena. Korektivne akcije su različite u zavisnosti da li je organizacija uradila nešto u domenu informacione bezbednosti ili da li su postojale značajne investicije u vidu vremena i truda.
U uspostavljanju informacione bezbednosti preporučuje se da se napravi presek stanja postojećih bezbednosnih mera, politika i organizacije i uporedi se sa preporučenom praksom, kako bi se jasno definisala neusaglašenost na kojoj će se raditi.

Nakon ovakve procene i odluke o uvođenju informacione bezbednosti donose se odluke o konkretnim akcijama. Ovakve odluke koje se obično grupišu u planove, korporativna pravila, politike ili radni okvir za informacionu bezbednost trebale bi biti donešene na osnovu strukturiranog pristupa. Ovaj pristup može biti baziran na analizi rizika kako se zahteva u ISO/IEC 27001 kao deo ISMS (Information Security Management System). Ostala stredstva kao što su testiranje performansi informacione bezbednosti, bilo interno, profesionalno ili ukoliko to radi eksterni konsultant.

U ovoj fazi bez speifične analize rizika, pitanje uloga u informacionoj bezbednosti mora biti rešeno. Veoma često, kada je odluka o ulogama doneta, osoba koja donosi konačnu odluku za određivanje budžeta neće biti u nedoumici “da li je ovo zaista potrebno?”. Zbog nepostojanja preliminarne procene i odluke o ulogama uključenih u infomacionu bezbednost, mnogi projekti vezani za informacnionu bezbednost su odloženi ili zatvoreni.

Često kasnije, ali ponekad u samom početku uvođenja informacnione bezbednosti, dovodi se u pitanje stvarni rizik koji je identifikovan u kompaniji. Ovo je često formulisano u pitanjima sličnim sledećim: “Da li su svi rizici kojima kompanija može biti izložena identifikovani i da li postoji garancija da su nivoi identifikovanog rizika prihvatljivi?”

Ovakva pitanja mogu se pojaviti na korporativnom nivou ili u vezi sa određenim projektom. Potrebna je metodologija rada koja uključuje i analizu rizika.

MEHARI se zasniva na principu da alati i informacije koji se zahtevaju u svakoj fazi razvoja informacione bezbednosti moraju biti konzistentni. Treba razumeti da rezultati dobijeni u pojedinoj fazi mogu biti ponovno korišćeni od strane drugih alata ili u okviru drugog procesa u kompaniji.

Različiti alati i moduli MEHARI metodologije dizajnirani su da prate direktne i individualne analize rizika, mogu biti korišćeni odvojeno jedni od drugih u bilo kojoj fazi razvoja informacione bezbednosti, koristeći različite pristupe upravljanja i mogu garantovati konzistentnost rezultata i odluka.

Svi ovi alati i moduli – kratko opisani u nastavku – sačinjavaju konzistentnu metodu procene rizika sa pratećim alatima, modulima za analizu uloga i nadgledanje kvaliteta sigurnosnih mera itd.

2.1. Analiza ili procena rizika

Analiza rizika je izraz koji se spominje u skoro svakoj publikaciji koja se bavi informacionom sigurnošću, kao inicijalna metoda za sigurnosne zahteve i standarde propisane od strane ISO/IEC. Međutim u većini slučajeva desi se greška da se ne dogovori podrazumevana metoda rada.

Već više od 15 godina, MEHARI obezbeđuje strukturirani pristup za procenu rizika[2], baziran na nekoliko jednostavnih principa.

Rizična situacija može biti opisana pomoću više faktora:

- Strukturni (organizacioni) faktori, koji ne zavise od sigurnosnih mera, ali zavise od bazičnih aktivnosti organizacije, okruženja i sadržaja.
- Faktori ublažavanja rizika koji su u direktnoj zavisnosti od sigurnosnih mera.

U stvari, analiza uloga u procesu informacione bezbednosti je neophodna kako bi se odredio maksimalni uticaj posledica rizične situacije. Ovo je tipično strukturni faktor, dok će procena bezbednosti biti korišćena za ocenu ublažavanja rizika.

MEHARI uključuje kvalitativnu i kvantitativnu procenu ovih faktora, i pomaže pri proceni nivoa rizika. Kao rezultat toga, MEHARI integriše alate (kao što su kriterijumi za procenu, formule itd.) i bazu znanja (posebno za određivanje sigurnosnih mera) koji su osnovne komponente za minimalni okvir propisan sa ISO/IEC 27005

2.1.1 Sistematična analiza rizičnih situacija

Da bi se pravilno odgovorilo na pitanje "koji su rizici u okviru organizacije i da li je nivo rizika prihvatljiv ili ne" potreban je strukturirani pristup kako bi se identifikovale sve potencijalne rizične situacije, kao i individualna analiza najkritičnijih situacija, i nakon toga identifikacija akcija kako bi se redukovao rizik.

Pristup koji obezbeđuje MEHARI baziran je na osnovi znanja koja se odnosi na rizične situacije i automatizovane procedure za evaluaciju faktora koji odlikuju svaki rizik koji daje mogućnost određivanja njihovog nivoa. Dodatno, metoda pomaže pri selekciji odgovorajućeg plana ublažavanja rizika.

Za ocenu rizika postoje dve opcije:

- Korišćenje skupa funkcija baze znanja (za Microsoft Excell ili Open Office) pruža mogućnost integracije MEHARI modula (klasifikacija sredstava iz analize uloga, analize informacione bezbednosti). Ove funkcije daju mogućnost procene aktuelnog nivoa i mere za smanjenje rizika
- Ili softverska aplikacija (kao što je RISICARE[3]) koja ima raznovrsniji korisnički interfejs i koja omogućuje simulacije i dalju optimizaciju.

[2] Detaljan opis modela rizika se nalazi u dokumentu *MEHARI Fundamentalni principi i funkcionalne specifikacije.*
[3] Od proizvođača softvera BUC S.A.

2.1.2 Spontana analiza rizičnih situacija

Isti set alata može biti korišćen u svakom momentu u različitim pristupima upravljanja informacionom sigurnošću.

U nekim slučajevima upravljanja informacionom bezbednošću gde upravljanje rizicima nije glavni cilj i gde se informacionom bezbednošću upravlja kroz reviziju ili referentnim okvirom za bezbednost, postojaće specifični slučajevi u kojima pravila ne mogu biti primenjena. Spontana analiza rizika može biti korišćena kako bi se donela odluka o daljoj metodologiji rada.

2.1.3 Analiza rizika u novim projektima

Modeli i mehanizmi analize rizika mogu biti korišćeni u upravljanju projektima, kako bi se ocenio nivo rizika i donela odluku koje mere će biti korišćene u ublažavanju rizika.

2.1.4 Procene informacione bezbednosti

MEHARI kroz dijagnostički upitnik o kontrolama sigurnosti omogućuje ocenu nivoa kvaliteta mehanizama i rešenja koja su implementirana kako bi se redukovao rizik[4].

2.1.5 Pregled ranjivosti, element analize rizika

MEHARI omogućava struktuirani model rizika koji uzima u obzir i "faktore smanjenja rizika" u cilju unapređenja sigurnosti servisa.

Rezultat ocene ranjivosti će biti važan izvor informacija za analizi rizika u cilju obezbeđivanja da sigurnosni servisi ispunjavaju njihovu ulogu – suštinska stvar za kredibilitet i pouzdanost analize rizika.

Suštinska prednost MEHARI-ja je mogućnost da oceni trenutni nivo rizika, kao i nivo rizika u budućnosti koji je baziran na ekspertskoj bazi znanja, ocenjujući kvalitet mera bezbednosti, bez obzira da li su operativne ili su donete odluke o implementaciji.

2.1.6 Plan bezbednosti baziran na pregledu ranjivosti

Mogući pristup je da se napravi akcioni plan, direktno kao rezultat ocenjivanja statusa sigurnosnih servisa.

Proces unapređenja informacione bezbednosti koji je zasnovan na gore objašnjenom veoma je jednostavan: potrebno je sprovesti ocenjivanje i odlučiti se za unapređenje svih servisa koji su ispod propisanog nivoa sigurnosti.

MEHARI upitnik može biti korišćen u ovakvoj vrsti pristupa.

Preliminarne analize biznis uloga, takođe, treba da budu planirane čime se obezbeđuje veza ka ovom modulu MEHARI-ja. Analiza uloga omogućava određivanje zahtevanog nivoa kvaliteta za relevantne servise bezbednosti, i shodno tome, mogućnost ignorisanja drugih delova procene.

[4] Sigurnosne mere i kontrole su grupisane u podservisima,servisima i konačno u sigurnosnim domenima.

2.1.7 Pomoć baze znanja u kreiranju referentnog okvira za informacionu bezbednost

Baza znanja koju koristi MEHARI može biti korišćena za direktno kreiranje referentnog okvira za informacionu bezbednost (ili sigurnosne politike) koji će sadržati i opisati set sigurnosnih pravila i instrukcije na koji način kompanija može da se drži tih pravila.

Ovaj pristup je često korišćen u organizacijama ili kompanijama sa određenim brojem organizacionih jedinica ili lokacija. U ovakvim slučajevima su u pitanju velike multinacionalne kompanije sa velikim brojem lokacija ili članova grupe. Ali se isto tako lako primenjuje na kompanijama srednje veličine sa velikim brojem filijala i poslovnica. U ovakvim slučajevima teško je efikasno obavljanje procene rizika.

Izrada okvira za informaciou bezbedost

MEHARI upitnici za procenu informacione bezbednosti su dobra baza za menadžere informacione bezbednosti za odlučivanje šta će biti primenjeno u njihovoj kompaniji.

Upravljanj**e izuzecima od pravila**

Kreiranje seta pravila, kroz radni okvir za informacionu bezbednost često nije usaglašen sa izazovima lokalne implementacije, tako da mora postojati svest o odstupanjima i tim razlikama se mora upravljati.

Korišćenje baze znanja sa konzistentnim setom alata i analičkom metodologijom omogućava da se pravilno upravlja lokalnom divergencijom. Razlika zbog koje nastaju odstupanja može biti pokrivena specifičnom analizom rizika koja će se odnositi na direktne razloge odstupanja.

2.1.8 Oblasti pokrivene modulom pregleda ranjivosti

Sa aspekta analize rizika, u smisu identifikovanja rizičnih situacija i želje da se pokriju svi neprihvatljivi nivoi rizika, MEHARI nije ograničen samo na domen informacionih tehnologija (IT).

Modul ocenjivanja pokriva, pored informacionog sistema, sve delove organizacije i zaštitu lokacija, u smislu radnog okruženja, zakonskih i regulatorskih aspekata.

2.1.9 Pregled: Modul ocenjivanja

Treba imati na umu da modul pregleda ranjivosti omogućava širi aspekt i konzistentnost u ocenjivanju informacione bezbednosti. Ova osobina može biti korišćena u različitim pristupima, detaljnim i preciznim analizama i može biti korišćena u svim fazama unapređenja svesti o informacionoj sigurnosti, kao i samoj organizaciji informacione sigurnosti.

2.1.10 Analiza uloga

Osnovna uloga bezbednosti je zaštita sredstava kompanije.

Kakva god da je orijentacija strategije informacione bezbednosti, postoji princip oko koga se slažu svi menadžeri – mora postojati ravnoteža između ulaganja u informacionu bezbednost

na jednoj strani i važnosti odgovarajućih biznis uloga. To znači da je razumevanje biznis uloga osnova i takva analiza uloga u informacionoj bezbednosti zaslužuje visok prioritet i strukturirani metod procene.

Cilj analize uloga u informacionoj bezbednosti je da odgovori na dvostruko pitanje:

“Šta se može desiti, i ako se desi koliko će biti ozbiljno?”

Ovo pokazuje da se u oblasti informacione bezbednosti, uloge označavaju kao posledice događaja koje ometaju željene operacije kompanije ili organizacije.

MEHARI obezbeđuje modul analize uloga, opisan u MEHARI-JU: Analiza uloga i klasifikacija, koji daje dve vrste rezultata:

Vrednosna skala kvarova i zastoja

Identifikacija kvarova ili potencijalnih događaja je proces koji počinje sa aktivnostima kompanije i podrazumeva identifikaciju mogućih kvarova i zastoja u operativnim procesima. Rezultati su :

- Opis mogućeg kvara
- Definicija parametara koji utiču na nivo ozbiljnosti svakog kvara
- Procenu kritičnih vrednosti parametara koji menjaju nivo ozbiljnosti kvara

Ovaj set rezultata čini vredosnu skalu kvarova i zastoja.

Klasifkacija informacija i sredstava

Obično se u informacionoj bezbednosti govori o klasifikaciji infomacija i klasifikaciji sredstava.

Ovakva klasifikacija se sastoji u definisanju, za svaki tip informacije i svaki tip sredstava i za svaki kriterijum klasifikacije (dostupnost, integritet i tajnost, mada se mogu koristiti drugi kriterijumi kao što je sledljivost / neporecivost), reprezentativnih pokazatelja ozbiljnosti uticaja gubitka informacija ili sredstva.

Klasifikacija informacija i sredstava za informacione sisteme je vrednosna skala kvarova i zastoja koja je definisana ranije u pokazatelje osetljivosti povezane sa sredstvima informacionih tehnologija (IT).

Izražavanje uloga informacione bezbednosti

Vrednosna skala kvarova i zastoja, klasifikacija informacija i sredstava su dva različita načina opisivanja uloge informacione bezbednosti.

Prva je mnogo detaljnija i daje više informacija za šefove službi informacione sigurnosti CISO (CISO), druga je uopštenija i korisnija za kampanje podizanja svesti o informacionoj bezbednosti i komunikaciju.

2.1.11 Analiza uloga, baza za analizu rizika

Jasno je da je ovaj modul ključni faktor u analizi rizika. Bez usaglašavanja o posledicama

potencijalnih kvarova ne može se pravilno oceniti nivo rizika.

MEHARI je striktan metod za ocenu uloga i klasifikovanje sredstava koji daje objektivne i racionalne rezultate.

2.1.12 Analiza uloga u informacionoj bezbednosti: Temelj strateškog planiranja akcionih planova

Analiza uloga je potrebna za uvođenje bilo koje forme planova informacione bezbednosti.

Koji god pristup da se koristi u jednom momentu sredstva će morati da se dodeljuju kako bi se akcioni planovi implementirali i neizbežno će se pojaviti pitanje investicija.

Sredstva i fondovi koji će biti dodeljeni informacionoj bezbednosti su, kao i polise osiguranja, u direktnoj srazmeri sa rizikom. Ukoliko ne postoji dogovor o potencijalnim problemima i kvarovima, veoma je verovatno da budžet za informacionu bezbednost neće biti dodeljen.

2.1.13 Klasifikacija: osnovni element za informacionu sigurnost

Reference radnog modela, politike informacione bezbednosti i odgovarajući pristup upravljanju informacionm sigurnošću su već pomenuti u ovom dokumentu.

U praksi kompanije koje upravljaju bezbednošću na osnovu skupa pravila u obavezi su da istaknu u svojim pravilima i procedurama akcije koje se obavljaju u funkciji poverljivosti informacija koje se u tim akcijama obrađuju. Najčešće se to radi kroz klasifikaciju informacija i popis aj ti (IT) sredstava. MEHARI-jev modul analiza uloga u informacionoj bezbednosti obezbeđuje gore navedenu klasifikaciju i sistematizaciju.

2.1.14 Analiza uloga u informacionoj bezbednosti: baza planiranja informacione bezbednosti

Sam proces analize uloga inforamacione bezbednosti zahteva doprinos operativnih menadžera, vrlo često dolazi do potrebe za hitnu akciju. Iskustvo pokazuje da, kada se radi intervju sa top menadžmentom, bez obzira na veličinu preduzeća, i kada oni objasne njihov stav i mišljenje o ozbiljnim zastojima, dovodi do saznanja da postoje problemi koji ranije nisu identifikovani i čije rešavanje zahteva hitne akcije.
Akcioni planovi mogu biti odmah napravljeni, koristeći direktan pristup koji se bazira na dva seta ekspertize: sprovedeno od osoblja koje se bavi poslovnim procesom koji izvršavaju operativni menadžeri i analiza sigurnosnih rešenja, izvršena od strane eksperata za informacionu bezbednost.

2.1.15 Generalni pregled korišćenja MEHARI-JA

Jasno je da je glavna orijentacija MEHARI-ja analiza i ublažavanje rizika. Njegova baza znanja, mehanizmi i alati kreirani su za tu svrhu.

Takođe, kreatori metodologije su imali na umu potrebu za strukturiranim metodoma za analizu i ublažavanje rizika i u zavisnosti od veličine kompanije postoje:

- Stalna metodologija rada – uputstvo za posebne grupe
- Metodologija rada koja se koristi paralelno sa drugim metodama upravljanja
- Metoda rada koja se povremeno koristi kako bi se dopunile redovne prakse

MEHARI obezbeđuje različite pristupe i alate za analizu rizika kada je to potrebno.

MEHARI metodologija čiju bazu znanja čine uputstva i procedure koje opisuju različite module (uloge, rizike, ranjivosti) postoji kako bi bila od pomoći ljudima koji su uključeni u proces informacione bezbednosti na bilo koji način (CISO, risk menadžeri, revizori, CIO), u njihovim različitim akcijama i zadacima.

3. MEHARI I ISO/IEC 27000 STANDARD

Često postavljano pitanje je: kako MEHARI odgovara internacionalnim standardima posebno ISO/IEC 27000 seriji.

Namera je da se objasni kako MEHARI odgovara ISO (ISO) 27001, 27002 i 27005 standardima u smislu kompatibilnosti i ciljeva.

3.1. Odgovarajući ciljevi ISO/IEC 27001, 27002, 27005 i MEHARI

3.1.1 Ciljevi ISO/IEC 27002:2005 standarda

Standard propisuje da organizacija treba da identifikuje zahteve za informacionu bezbednost kroz tri glavna izvora :

- Analizu rizika,
- Zakonskim, statutarnim, regulatornim ili ugovornim zahtevima
- Skupom principa, ciljeva i zahteva koje važe za informacije koje nastaju da bi podržale operativne zadatke

Koristeći ovo kao bazu, kontrolne tačke mogu biti izabrane i implementirane koristeći listu u sekciji "kodeks prakse za upravljanje informacionom sigurnošću", u standardu ili iz nekog drugog konrolnog seta tačka (§4.2).

NB: U okviru 27002: 2005 predviđeno je da standard pruža "uputstva i opšte principe za iniciranje, implementaciju, održavanje i unapređenje upravljanja informacionom bezbednošću" što znači da se ISO standard može posmatrati kao polazna tačka. Međutim, ISO/IEC 27001 propisuje da svako odstupanje mora biti opravdano i prihvatljivo kada se dodaju kontrolne tačke (Dodatak A - A.1).

ISO 27002 standard obezbeđuje skup uputstava koje organizacija može koristiti. Međutim, spisak nije konačan i dodatne mere mogu biti zahtevane. Međutim, ne preporučuje se metodologija za stvaranje kompletnog sistema upravljanja informacionom bezbednošću.

Na drugoj strani, svaki deo objašnjenja najbolje prakse sadrži uvod i komentare o nameri ciljeva, što može biti velika pomoć.

NB: ISO standard, takođe, predviđa u svom okviru koji se može koristiti da "pomogne izgradnji poverenja u inter-organizacione aktivnosti". Ovo nije uključeno slučajno i donosi bitan aspekat koje bi pristalice standarda trebalo da promovišu, što je to evaluacija (čak i sertifikacija) za perspektive informacione bezbednosti, partnera i dobavljača.

3.1.2 Ciljevi ISO/IEC 27001:2005

Jasan cilj ISO/IEC 27001 je da "obezbedi model za kreiranje i administraciju korporativnog sistema upravljanja infromacionom bezbednošću **ISMS"** i kako bi ga koristili "interno, treća strana, uljučujući sertifikaciona tela".

Cilj evaluacije i sertifikacije stavlja fokus na formalne aspekte (dokumentaciju i registraciju odluka, deklaraciju o primenjivosti, registar i dr.) i kontrole (analize, revizije. itd.).

Jasno je da kod ovog pristupa informacionoj bezbednosti analiza rizika mora biti urađena kako bi se ispitali rizici kojima bi organizacija mogla biti izložena i odabrane odgovarajuće mere za redukovanje rizika na prihvatljiv nivo (paragraf 4.2.1)

ISO/IEC 27001 propisuje da bi analiza rizika trebala biti urađena ali da nije deo standarda, takođe, nije ponuđena odgovarajuća metoda ako se ne uzima u obzir PDCA (PDCA-Plan, Do, Check, Act) rekurzivni proces modela kao što je definisano u uspostavljanju ISMS.

Svakako, preporuka "najbolje prakse" koja može biti korišćena u redukovanju nivoa rizika su "usaglašene sa onim iz ISO/IEC 27002:2005", dok dodatna lista kontrola postoji u dodacima.

Prema ISO/IEC 27001 osnova procene upravljanja informacionom bezbednošću nije toliko stvar znanja ili to da li su odluke koje su donesene odgovoarajuće i prilagođene potrebama kompanije, već da revizor ili sertifikovani revizor može proceniti da li su odluke zaista implementirane.

3.1.3 Ciljevi ISO/IEC 27005:2008

Cilj ovog standarda nije da konstituiše metod za risk menadžment već da odredi minimalni radni okvir i opiše zahteve za proces analize rizika, za identifikaciju pretnji i identifikovanje ranjivosti kako bi se odredio nivo rizika i onda biti u poziciji da se odabere model remedijacije i pratećih planova usmerenih na evaluaciju i poboljšanje situacije.

Standard propisuje da analiza rizika mora biti selektovana u skladu sa ovim zahtevima kako bi se izbeglo korišćenje nedosledne ili pojednostavljene metode, u poređenju sa onim što je bila ideja autora standarda.

3.1.4 Ciljevi MEHARI-JA

MEHARI je konzistentan set alata i metodologije za upravljanje informacionom bezbednošću i odgovarajućih mera baziran na tačnoj analizi rizika. Fundamentalni principi MEHARI-JA:

- Predstavljanje risk modela modela rizika (kvalitativni, kvantitativni)
- Razmatranje efikasnosti mera informacione bezbednosti koje su primenjene ili planirane
- Mogućnost da proceni preostali nivo rizika koji ostaju posle primenjenih mera

Ovi principi su obavezne komponente koji se dopunjuje sa zahtevima ISO/IEC 27000 standarda i posebno ISO/IEC 27005.

3.1.5 Poređenje ciljeva MEHARI-JA SA ISO/IEC 27001 i 27002 standardima

Ciljevi MEHARI-JA i pomenutih ISO standarda su veoma različiti..

- MEHARI ima za cilj da obezbedi sredstva i metode koje se mogu koristiti da se izaberu najpogodnije mere bezbednosti za datu organizaciju i da proceni preostale rizike kada te mere postanu operativne. Ovo nije primarni cilj ISO standarda.
- ISO standardi obezbeđuju skup najboljih praksi koje se svakako veoma korisne ali ne i nužno odgovarajuće za pitanja informacione bezbednosti u okviru organizacije, one su korisne da pokriju sve aspekte informacione bezbednosti, planiranje i reviziju, eksternu ili internu.

MEHARI Referentni priručnik službe sigurnosti daje elemente koji mogu biti korišćeni za izradu radnog okvira za informacionu bezbednost i može se porediti sa ISO/IEC 27002. Jasno je da MEHARI pokriva širi okvir od ISO standarda i da pokriva osnovne aspekte informacione bezbednosti kako u, tako i van informacionih sistema.

3.2. Kompatibilnost između ova dva pristupa

MEHARI pristup je potpuno podudaran sa ISO 27002 zato što, bez obzira što nemaju iste ciljeve, relativno je lako prezentovati rezultate MEHARI analize u pogledu na ISO 27002 indikatore.

MEHARI odgovara potrebama koje su izražene u oba standarda ISO 27001 i 27002 za analizu rizika i definisanje mera koje se trebaju implementirati.

3.2.1 Kompatibilnost sa ISO/IEC 27002:2005 standardima

Standardne kontrolne tačke ili najbolja praksa ISO standarda su najčešće generalne mere ponašanja ili organizacione, dok MEHARI pored njih naglašava potrebu za merama čija će efikasnost biti garantovana.

Uprkos ovim razlikama, MEHARI-jev pregled ranjivosti pruža dodatne tabele za prikazivanje indikatora usklađenosti sa krahom koji se koriste u ISO 27002:2005 standardima, takođe, korisne za one koji treba da pokažu usklađenost sa navedenim standardom. Treba pomenuti da su MEHARI upitnici za reviziju dizajnirani i napravljeni tako da omoguće operativnim menadžerima efektivni pregled ranjivosti i utvrde kapacitete svakog servisa sigurnosti kako bi umanjili rizik.

3.2.2 Kompatibilnost sa ISO/IEC 27001 standardom

MEHARI može lako biti integrisan u PDCA (PDCA: Plan – Do – Check – Act) proces kao što je propisano u ISO/IEC 27001, posebno faza ‘PLAN’ (§4.2.1). MEHARI kompletno pokriva opis zadataka koji omogućavaju stvaranje ISMS baze.

Za ‘DU’ (DO) (fazu (§4.2.2), koja ima za cilj da implementira i upravlja ISMS, MEHARI pruža korisne početne elemente kao što su izrada planova za upravljanje rizicima uz davanje prioriteta direktno povezanim za klasifikaciju rizika i uspešnost mera u toku njihovog korišćenja.

Za ‘ČEK’ (CHECK) fazu (§4.2.3), MEHARI predviđa elemente koje omogućavaju procenu preostalog rizika i poboljšanja u merama sigurnosti. Pored toga sve promene u okruženju (uloge, pretnje, rešenja i organizacija) mogu se lako ponovo oceniti ciljanim revizijama koje koriste incijalne MEHARI revizije, tako da planovi sigurnosti mogu biti revidirani i razvijeni tokom vremena.

Za ‘AKT’ (ACT) fazu (§4.2.4), MEHARI implicitno poziva na kontrole i kontinuirano unapređenje informacione sigurnosti; time obezbeđuje da su ispunjeni ciljevi bezbednosti. U ove tri faze, kada MEHARI nije u fokusu, bitno doprinosi njihovom izvršenju i obezbeđuje njihovu efikasnost.

3.2.3 Kompatibilnost sa ISO/IEC 27005:2008 standardima

Radni okvir uspostavljen od strane ovog novog standarda je potpuno primenjiv na način na koji MEHARI omogućava upravljanje rizicima, na primer:

- Proces analize rizika, ocene, i tretman rizika (uzet iz ISO 13335)
- Identifikacija primarnih sredstava i klasifikacija nivoa vezanih za njih, nakon analize uloga
- Identifikacija pretnji, uključujući njihov nivo (prirodne izloženosti), za koji MEHARI ima precizniji opis scenarija rizika.
- Identifikacija i kvantifikacija efikasnosti sigurnosnih mera (ili kontrola) u redukciji ranjivosti
- Kombinacija ovih elemenata za procenu nivoa rizika na skali sa 4 nivoa
- Sposobnost da direktno izaberete mere bezbednosti potrebne za smanjenje rizika

Odatle MEHARI nije lako integrisati u ISMS proces, koji je promovisan od strane ISO 27001 ali je potpuno u skladu sa ISO 27005 zahtevima za metodu upravljanja rizicima.

L'ESPRIT DE L'ÉCHANGE

UDRUŽENjE ZA INFORMACIONU BEZBEDNOST FRANCUSKE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

Rue de Mogador 11
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.fr

Download CLUSIF productions at:

www.clusif.fr