МЕХАРИ 2010

Преглед

Април 2010

Работна група за методологија

Ве молам да ги праќате вашите прашања и коментари на форумот:
http://mehari.info/

КЛУБ ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИИ НА ФРАНЦИЈА

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

МЕХАРИ е трговска марка регистрирана од страна на CLUSIF.

Законот од 11. март 1957. година, според ставките 2. и 3. од член 41., одобрува од една страна само "копија или репродукција, стриктно резервирана за лична употреба на корисникот која не е наменета за колективно користење", а од друге страна, анализа и кратки цитати со цел пример и илустрација" било какво претставување или комплетна или делумна репродукција, направена без одобрување на авторот или носителот на правата или нивните законски наследници е противзаконска" (прв став од член 40).
Ваква репрезентација или репродукција, преку било каков процес, ќе претставува плагијат казнив според член 425 и релевантните членови од Кривичниот законик.

Благодарница

CLUSIF сака посебно да им се заблагодари на Jean-Philippe Jouas за неговиот извонреден придонес, Јасмина Трајковски, Ана Мешковска и Теодор Димитров за овој превод (сите сугестии и коментари за овој превод можете да пратите директно на jasmina.trajkovski@tpconsulting.com.mk, ana.meskovska@tpconsulting.com.mk и teodor.dimitrov@makpetrol.com.mk), како и на Комисијата за методологија која учествуваше во реализација на овој документ:

Jean-Philippe	Jouas	Одговорен за Комисијата за методологија Одговорен за работната група Принципи, Механизми и бази на знаења за МЕХАРИ
Jean-Louis	Roule	Одговорен за работната група за МЕХАРИ документација
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost
Martine	Gagné	HydroQuébec
Moïse	Hazzan	Ministère des Services Gouvernementaux du Québec
Gérard	Molines	Molines Consultants
Chantale	Pineault	AGRM
Luc	Poulin	CRIM
Pierre	Sasseville	Ministère des Services Gouvernementaux du Québec
Claude	Taillon	Ministère de l'Éducation, du Loisir et du Sport du Québec
Marc	Touboul	BULL SA

СОДРЖИНА

1. ВОВЕД

МЕХАРИ методологијата оригинално е направена и постојано се надградува со цел да им помогне на Офицер за безбедност на информации (Chief Information Security Officers - CISOs) при воведувањето и управувањето со безбедност на информации.
Овој преглед е насочен примарно кон нив, но исто така е наменет за ревизори, одговорни за информации или информациони системи (Chief Information Officers - CIOs) или Одговорни за управување со ризици кои исто така се изложени на истите или слични предизвици.

Главната цел на овој документ е да објасни како МЕХАРИ може да се користи. Подетален опис на методологијата и на поврзаните алатки е дадена во други документи на Clusif, поконкретно во:

- МЕХАРИ: Концепти и функционални спецификации,
- МЕХАРИ водич: за
    - Анализа на влијанија и класификација,
    - Евалуација на безбедносни мерки и
    - Анализа на ризик,
- МЕХАРИ референтен прирачник за безбедносни мерки,
- МЕХАРИ база на знаење.

Главната цел на МЕХАРИ е да обезбеди метод за оценка и управување со ризик, специфичен за областа на безбедност на информации, усогласен со барањата на ISO/IEC 27005:2008 и да обезбеди множество од алатки и елементи потребни за негова примена[1].Дополнителни цели се:

- Да се обезбеди директна и индивидуална анализа на ризиците опишани во сценаријата,
- Да се обезбеди комплетно множество од алатки посебно дизајнирани за краткорочно, среднорочно и долгорочно управување со безбедност на информации, прилагодливи на различните нивоа на зрелост и типови на акции кои се разгледуваат.

Во секој случај, МЕХАРИ обезбедува конзистентна методологија со соодветна база на знаење, која им помага на офицерите за безбедност на информации (CISOs), генералните директори, и одговорните за информации или информациони системи, или други лица вклучени во намалување на ризик преку нивните специфични задачи и активности.

Врската на МЕХАРИ со ISO/IEC 27000 стандардите е опишана на крај на овој документ.

[1] Алатките и дополнителните средства обезбедени од МЕХАРИ, како дополнување на стандардот, се опишани и објаснети во МЕХАРИ: Концепти и функционални спецификации

2. УПОТРЕБА НА МЕХАРИ

МЕХАРИ е пред се метод за оценка и управување со ризик.

Во пракса, ова значи дека МЕХАРИ и неговата база на знаење се дизајнирани за прецизна анализа на ризични ситуации опишани преку сценарија.

Во секојдневното работење, управување со безбедноста на информациите е функција или активност која еволуира со тек на време. Корективните мерки се различни во зависност од тоа дали организацијата има веќе нешто направено во тој домен, или не.
При правење на првите чекори во безбедност на информации, нема сомнеж дека се препорачува прво да се направи анализа на постојните безбедносни мерки и политики на организацијата, и да се спореди со најдобрите практики од индустријата, со цел јасно да се види јазот кој треба да се надмине.

Веднаш по оваа проценка и по одлуката да се имплементира организациска безбедност се носат одлуки за конкретни активности. Ваквите одлуки најчесто се групираат во планови, корпоративни правила, политики или референтни рамки за безбедност и при тоа потребно е истите да се донесат користејќи структуриран пристап. Овој пристап може да се базира на анализа на ризици, како што се бара во ISO/IEC 27001 за воспоставување на Систем за управување со безбедност на информации (Information Security Management System - ISMS). Постојат и други типови на мерки кои може да се применат како на пример компаративна споредба (benchmark), која може да биде интерна, професионална или интер-професионална.

Во оваа фаза потребно е, без специфично нагласување на анализата на ризици, да се разгледа прашањето за влијанијата врз информационата безбедност. Многу често, без разлика како се одлучува, личноста која го има крајниот збор во однос на доделување на финансиски средства без сомнеж ќе го постави прашањето „дали е ова навистина неопходно?“. Поради недостаток на претходна проценка на влијанијата, и генерална согласност за истите, многу проекти поврзани со безбедност на информации се одложени или целосно откажани.

Често пати подоцна во текот на проектот, но понекогаш и на самиот почеток на проектот за воведување на информациона безбедност, се поставува прашањето за реалниот ризик со кој се соочува организацијата. Ова често се формулира во прашање слично на следново: „Дали се идентификувани сите ризици на кои може да биде изложена организацијата, и дали постои некаква сигурност дека нивото на идентификуваните ризици е прифатливо?“. Ова прашање може да се постави како за организации, така и за специфични проекти. Поради тоа потребна е методологија која вклучува анализа на ризици.

МЕХАРИ се заснова на принцип дека алатките потребни во различните фази од развојот на системот за безбедност на информации мора да бидат конзистентни. Ова подразбира дека било кој резултат добиен во една фаза може да се искористи повторно подоцна од друга алатка или во друг дел од организацијата.

Различните алатки и модули од множеството на методологијата МЕХАРИ, дизајнирани за директна или индивидуална анализа на ризици, може да се користат посебно еден од друг во било кој чекор од развојот на информационата безбедност, користејќи различни пристапи за раководење, и да гарантираат конзистентност во донесените одлуки.

Сите овие алатки и модули – накратко опишани подолу – сочинуваат конзистентен метод за проценка на ризици со потребните алатки и модули за анализа на влијанијата и ревизија (audit) на квалитетот на безбедносните мерки, итн.

2.1. Анализа или проценка на ризици

Анализа на ризици се споменува скоро во секоја публикација од областа на информацискатa безбедност, како движечка сила за идентификација и прикажување на барањата за воспоставување на безбедност на информациите, истото се споменува и во ISO/IEC стандардите. Меѓутоа, повеќето публикации не споменуваат кои методи треба да се користат.

Има повеќе од 15 години како МЕХАРИ го има пропишано структурираниот пристап за евалуација на ризик[2], кој е базиран на неколку едноставни принципи.

Ризична ситуација може се карактеризира преку различни фактори:

- Структурни (или организациски) фактори, кои не зависат од безбедносните мерки, туку зависат од суштинските активности на организацијата, како и околината во која функционира организацијата и поставеноста на организацијата.
- Фактори кои го намалуваат ризикот, и кои се директно зависни од применетите мерки за безбедност на информации.

Всушност, анализата на влијанијата по безбедностана информациите е потребна за да се одредат нивоата на сериозност на последиците од ризичните ситуации. Ова претставува типичен структурен фактор, додека оценката на ризици по безбедност на информациите се користи за евалуација на факторите за намалување на ризикот.

МЕХАРИ овозножува квалитативна и квантитативна евалуација на овие фактори, а резултатот помага во евалуацијата на нивоата на ризик. Во овој процес, МЕХАРИ интегрира алатки (како што се критериуми за оценка, формули итн.) и бази на знаење (особено за дијагностицирање на мерки за безбедност на информации), кои претставуваат основни дополнувања на минималната рамка предложена од ISO/IEC 27005.

2.1.1 Систематска анализа на ризични ситуации

Со цел да се одговори на прашањето «кои се ризиците над организацијата и дали тие се прифатливи или не?», потребен е структурен пристап за идентификација на сите потенцијални ризични ситуации, индивидуално да се анализираатнајкритичните од нив, и да се идентификуваат активности кои ќе го намалат ризикот до прифатливо ниво.

Пристапот на МЕХАРИ се базира на бази на знаење за ризични ситуации и автоматизирани процедури за евелуација на фактори кои го карактеризираат секој ризик и со тоа дозволуваат оценка на неговото ниво. Дополнително, овој метод овозможува помош при селекцијата на соодветни планови за справување со ризиците.

Со цел да се оцени ризикот, предложени се две главни опции:

- Користење на множество на функции од базата на знаење (за Microsoft Excel или

[2] Детален опис на моделот за ризик е прикажан во МЕХАРИ основни принципи и функционални спецификации.

Open Office) со што се овозможува интегрирање на резултатите од модулите на МЕХАРИ (пр. класификација на средства од анализата на влијанија, дијагноза на безбедносни состојби). Со овие функции, можно е да се оценат тековните нивоа на ризиците и да се предложат дополнителни мерки за намалување на ризиците.

- Користење на софтверска апликација (како на пример RISICARE[3]) која обезбедува побогат кориснички интерфејс и која овозможува симулации, визуелизација и дополнителна оптимизација.

2.1.2 Спонтана анализа на ризични ситуации

Истото множество на алатки може да се користи во секој момент и за други пристапи за воспоставување на систем за управување со безбедност на информации.

При некои пристапи за управување со безбедност на информации, каде управувањето со ризици не е главна цел и каде безбедноста се управува преку ревизии / проверки или референтни безбедносни рамки, често ќе постојат одредени случаи каде овие правила нема да можат да се применат. Спонтана анализа на ризици може да се користи за да се одлучи како е најдобро да се продолжи во таквите случаи.

2.1.3 Анализа на ризици во нови проекти

Моделот и механизмите за анализа на ризик може да се користат и за управување со проекти; за планирање на справувањето со ризици и мерките кои треба да се применат.

2.2. Проценка на информационата безбедност

МЕХАРИ обезбедува интегрирање на деталните дијагностички прашалници за имплементираните безбедносни мерки и контроли, дозволувајќи оценка на нивото на квалитет на механизмите и решенијата од аспект на намалување на изложеноста на ризик[4]

2.2.1 Преглед на ранливости, елемент од анализа на ризици

МЕХАРИ обезбедува структуриран модел на ризик кој ги зема во предвид "факторите за намалување на ризик", дефинирани како безбедносни мерки (security services).

Оценката на ранливости која е резултат од спроведениот преглед е клучен влезен податок во анализата на ризици кој обезбедува избраните безбедносни мерки навистина ќе ја вршат својата задача. Ова претставува основен фактор за кредибилитетот и издржаноста на анализата на ризик.

Основната сила на МЕХАРИ е во неговиот капацитет да го оцени тековното ниво на ризик како и идното ниво базирано на експертската база на знаење која ја користи за оценка на нивото на квалитет на безбедносните мерки, независно дали се имплементирани или е само одлучена нивната примена.

2.2.2 Планови за информациона безбедност базирани на прегледот на ранливости

Еден од можните пристапи за дефинирање на акциските планови е како директна последица на оценката на состојбата односно квалитетот на безбедносните мерки.

[3] Од BUC S.A. software editor

[4] Безбедносните контроли, или мерки, се групирани во под-услуги, услуги и на крај безбедносни домени.

Процесот на управување со безбедноста на информациите кој го следи овој пристап е доста едноставен: спроведи ја оценката и одлучи да ги подобриш сите оние безбедносни мерки кои не се на соодветното ниво на квалитет.

МЕХАРИ дијагностичките прашалници може да се користат за спроведување на овој пристап.

Исто така треба да се планира и прелиминарна анализа на деловните влијанија, што претставува врска со тој модул од МЕХАРИ. Анализата на влијанијата овозможува дефинирање на потребните нивоа на квалитет на релевантните безбедносни мерки и последователно, игнорирање на оние кои не се релевантни при спроведување на оценката.

2.2.3 Подршка од страна на базите на знаење во креирање на референтна рамка за информациона безбедност

МЕХАРИ содржи специфични бази на знаење кои може да се користат директно за креирање на референтна безбедносна рамка (security reference framework) или поединечни безбедносни политики кои ќе содржат и ќе опишуваат множество на безбедносни правила и насоки кои организацијата ќе треба да ги следи и спроведе.

Овој пристап често се користи во организации кои имаат повеќе независни локации или организациски единици. Ова е типичен случај со големи меѓународни компании со бројни поврзани организации. Но овој метод може да се примени и на средни компании со голем број на регионални филијали или претставништва. Во такви случаи, подеднакво е комплексно спроведувањето на бројните анализи на ризици.

Дефинирање на референтна безбедносна рамка

МЕХАРИ и неговите прашалници за оценка претставуваат добра основа за одговорните за безбедност да можат да одлучат што треба да се примени во нивната организација.

Управување со исклучоците од правилата

Креирањето на единствено множество на правила преку воспоставување на референтна безбедносна рамка, често се соочува со проблеми при локалнното спроведување, што предизвикува потреба од дефинирање на локализирани исклучоци со кои треба да се управува.

Користење на кохерентна база на знаење, со конзистентно множество на алатки и методологија, овозможува управување со локализираните дивергенции од правилата. Барањата за исклучоци може да се покријат со посебна анализа на ризик која ќе се фокусира на идентификуваниот проблем кој претставува основа за барањето за исклучок.

2.2.4 Домени покриени со модулите за оценка на ранливостите

Од гледна точка на анализа на ризик, а со цел да се идентификуваат сите ризични ситуации и да се покријат сите неприфатиливи ризици, МЕХАРИ не се ограничува само на ИТ доменот.

Модулот за оценка, покрај ИТ системот, ги покрива и целосната организација, заштитата на локациите, како и работната околина и правните и регулаторните аспекти.

2.2.5 Преглед на модулите за проценка

Главната особина на модулот за проценка на ранливости е дека тој обезбедува широк и конзистентен поглед врз безбедноста. Поради тоа истиот може да се користи како дел од различни пристапи, со еволутивно ниво на деталност и длабина на анализата, како и при различити степени на зрелост на свесноста и имплементираните мерки за безбедност во организацијата.

2.3. Анализа на влијанија

Безбедноста е фокусирана на заштита на средствата. Каква и да е ориентацијата на политиката за безбедност, постои еден принцип за кој се согласуваат сите раководители – а тоа е дека мора да постои соодветен баланс помеѓу инвестициите во безбедноста и значајноста на релевантните деловни влијанија.

Ова наведува дека соодветно разбирање на деловните влијанија е фундаментално, и дека анализата на безбедносните влијанија заслужува соодветно висок приоритет и примена на структуриран метод за нивна евалуација.

Целта на анализата на безбедносните влијанија е изнаоѓањето одговор на следново двојно прашање:

“Што може да се случи, и ако се случи, дали ќе е критично?”

Ова покажува дека, во областа на информационата безбедност, влијанијата се гледаат како последици на настаните кои го нарушуваат планираниот тек на активностите и операциите на организацијата.

МЕХАРИ содржи модул за анализа на влијанијата опишан во *МЕХАРИ: Анализа на влијанија и класификација,* кој дава два типа на резултати:

- Вредносна скала за дисфункција (malfunction),
- Класификација на информации и ИТ средства.

Вредносна скала на дисфункција

Идентификацијата на дисфункции или потенцијални настани е процес кој започнува со активностите во организацијата и се фокусира на идентификација на можните дисфункции во оперативните процеси. Тој резултира со:

- Опис на можните типови на дисфункции,
- Дефинирање на параметрите кои влијаат на критичноста на секоја дисфункција,
- Оценка на прагот на тие параметри кога дисфункцијата преминува во критична.

Ова множество на резултати ја формира вредносната скала на дисфункции.

Класификација на информации и ИТ средства

Вообичаено е, во доменот на безбедност на ИТ системите, да се зборува за класификација на информации и класификација на ИТ средства.

Таква класификација се состои во дефинирање на репрезентативни индикатори за критичноста на критериумот на кој се влијае, или за губење на информацијата или средството. Вакви индикатори се дефинираат за секој тип на информации и за секое ИТ

средство, и за секој критериум за класификација (вообичаени: Достапност, Интегритет и Доверливост, но и други критериуми може да се користат како на пример Следливост).

Класификацијата на информациите и средствата, за информационите системи, е всушност претставување на претходно дефинираната вредносна скала на дисфункции пресликана во показатели за чувствителност поврзани со информациите и ИТ средствата.

Изразување на безбедносни влијанија

Вредносната скала на дисфункции и класификацијата на информации и средства се два различни начина за изразување на безбедносните влијанија.

Првиот е подетален и обезбедува повеќе информации за офицерот за безбедност на информациите. Вториот е поглобален и корисен за зголемување на свесноста кај корисниците, но е со помала грануларност односно ниво на деталност.

2.3.1 Анализа на влијанија, основа за оценка на ризици

Јасно е дека овој модул е основата на анализата на ризици. Без јасна и прифатена основа за последиците од потенцијалните дисфункции не е возможно да се донесе одлука за нивото на ризик.

МЕХАРИ претставува строг метод за оценка на влијанијата и класификацијата на средствата, кој обезбедува објективни и рационални резултати.

2.3.2 Анализа на влијанијата по безбедноста на информациите: основа за секое стратешко планирање

Јасно е дека анализа на влијанијата е неопходна за имплементирање на било каков безбедносен план. Следствено, кој пристап и да е користен, доаѓа до моментот кога ќе е потребно да се алоцираат средства за спроведување на акциските планови, и неодложно, аргументирање на целисходноста на таквите инвестиции.

Ресурсите и средствата кои ќе бидат алоцирани за безбедност се, сродно како и за полисите за осигурување, пропорционални со изложеноста на ризик. Доколку не постои прифатено разбирање се потенцијалните дисфункции, тогаш е слабо веројатно дека финансиски средства ќе бидат доделени за безбедност.

2.3.3 Класификација: суштински елемент на политиката за безбедност на информации

Референтни безбедносни рамки, безбедносни политики, и поврзаниот пристап за управување со безбедноста на информациите веќе беа споменати во овој документ.

Во практика, компаниите кои управуваат со безбедноста на информациите преку можество на правила се обврзани во тие правила да вградат модалитет за примена на дефинираните активности пропорционално со чувствителноста на информациите кои се процесираат. При тоа, вообичаено е да се базираат на класификација на информации и на ИТ средства.

МЕХАРИ модулот за анализа на безбедносните влијанија овозможува таква класификација.

2.3.4 Анализа на влијанијата врз безбедноста на информациите: основа за планирање за информациона безбедност

Самиот процес на анализа на безбедносните влијанија, неопходно бара вклучување на оперативните раководители и често води кон потреба од директна акција во најкраток можен рок.

Искуството покажува дека, независно од големината на организацијата, при интервјуирање на оперативниот раководен кадар за нивното гледиште и оценка на критичноста на дисфункциите, се идентификуваат безбедносни потребни за кои тие првенствено не биле свесни, а кои бараат итна реакција. Акциските планови тогаш можат да се направат користејќи лесен и директен пристап базиран на комбинација од два типа на експертиза: таа од самата професија која ја даваат оперативните раководители и онаа за безбедносните решенија која ја даваат експертите за безбедност.

2.4. Генерален преглед за користењето на МЕХАРИ

Јасно, главниот фокус на МЕХАРИ е оценка и намалување а ризикот. Базите на знаење, механизмите и алатките кои се вградени во МЕХАРИ се направени за да ја исполнат таа цел.

Исто така, според мислењето на дизајнерите на оваа методологија, потреба од структуриран метод за анализа на ризици и нивно намалување е различна кај организациите и може да биде: Постојана постапка за работа – водичи за специјализирани групи,

- Постапка која се користи паралелно со други практики за управување со безбедноста, или
- Постапка која повремено се користи како надополнување на редовните практики.

Имајќи го ова во предвид, може да се каже дека МЕХАРИ обезбедува множество од методи и алатки кои овозможуваат спроведување на анализа на ризик тогаш кога тоа и е потребно на организацијата.

МЕХАРИ методологијата, која се состои од бази на знаење, упатства и водичи кои ги појаснуваат различните модули (влијанија, ризици, ранливости), постои со цел да им помогне на лицата кои се вклучени во управувањето со безбедноста (како офицерите за безбедност на информации, одговорните лица за управување со ризици, ревизорите, раководителите на информации или информационите ситеми) при реализација на нивните задачи и активности.

3. МЕХАРИ И ISO/IEC 27000 СТАНДАРДИТЕ

Често се поставува прашањето: како МЕХАРИ соодветствува со интернационалните стандарди, поточно со ISO/IEC 27000 серијата.

Намерата е да се објасни како МЕХАРИ се вклопува во ISO 27001, 27002 и 27005 стандардите, во однос на компатибилноста и целите.

3.1. Соодветните цели на ISO/IEC 27001, 27002, 27005 и МЕХАРИМЕХАРИ

3.1.1 Целите на ISO/IEC 27002:2005 стандардот

Овој стандард пропишува дека организацијата треба да ги идентификува нејзините безбедносни барања користејќи три главни извори:

- Анализата на ризиците,
- Законските, статутарните, регулаторните или договорните барања,
- Множество на принципи, цели и барања поврзани со обработка на информации кои што организацијата ги поставила за поддршка на нејзиното работење.

Користејќи ги овие како основа, контролните точки може да бидат одбрани и поставени користејќи листа која што е содржана во делот „Зборник на практики за управување со информацискатa безбедност“ од стандардот или кои што произлегуваат од било кое друго множество на контролни точки (§4.2).

NB: во рамки на 27002:2005, наведено е дека стандардот обезбедува „насоки и општи приниципи за започнување, воспоставување, одржување и подобрување на управувањето со информацискатa безбедност“, што значи дека на ISO стандардот треба да се гледа како на почетна точка. Сепак, ISO/IEC 27001 наведува (§1.2) дека било какво отстапување (исклучок) мора да биде оправдано и дека е прифатливо да се додадат други контролни точки (Додаток A-A.1).

ISO 27002 стандардот обезбедува збирка на основни напатствија, кои што организацијата може да ги користи. Тој наведува, покрај тоа, дека листата не е конечна и дека може да бидат потребни и дополнителни мерки. Меѓутоа, не е препорачана методологија за изработка на целосен систем за управување со информациона безбедност.

Од друга страна, секој дел од водилките за добрите практики содржат вовед и коментари за посакуваните цели, што може да биде од голема помош.

NB: ISO стандардот исто така наведува дека во неговите рамки може да биде искористен за „помош при градење на доверба при интер-организациите активности“. Ова не е случајно вметнато, туку ги прикажува суштествените аспекти кои што поддржувачите на стандардот ги промовираат, а тоа е евалуација (па и сертификација) на партнерите и добавувачите од аспект на безбедноста на информациите.

3.1.2 Целите на ISO/IEC 27001:2005

Јасната цел на ISO/IEC 27001 е да „обезбеди модел за изработка и раководење со **систем за управување со безбедност на информации (анг. Information security management system-ISMS)“** и да биде „користен како внатрешно така и од страна на трети страни, вклучувајќи ги и сертификационите тела“.

Евалуацијата и стремежот кон сертификација ставаат силен фокус на формалните аспекти (документирање и регистрирање на одлуки, изјави за применливост, регистри и т.н.) и на контролите (преиспитувања, ревизии и т.н.) .

Јасно е дека основата на безбедносниот пристап подразбира дека треба да се направи анализа на ризиците, со цел да се испитаат ризиците на кои што организацијтата би можела да биде изложена и да се одберат соодветни мерки за намалување на ризикот на прифатливо ниво (параграф 4.2.1).

ISO/IEC 27001 наведува дека треба да се користи метод за анализа на ризиците, но тоа не е дел од стандардот и не е предложен одреден метод, освен интегрирањето на повторливиот PDCA процес (анг. Plan, Do, Check, Act - планирање, спроведување, проверка, дејствување) при изработка на ISMS.

Исто така, препораките или *добрите практики* кои што можат да бидат искористени за намалување на ризикот се „усогласени со контролните цели наведени во ISO/IEC 27002:2005“, додека соодветната листа на контолни точки е наведена во прилозите.

Според ISO/IEC 27001, основата на **евалуација на системот за управување со безбедност** не претставува, во голема мера, знаење или потврда дека одлуките кои што биле направени се соодветни и прилагодени кон потребите на организацијата, туку повеќе да проверат дека, кога веќе еднаш одлуките се направени, системот на управување навистина е имплементиран така да овозможува ревизорот или сертификационото тело да се сигурни дека одлуките навистина ќе бидат применети.

3.1.3 Целите на ISO/IEC 27005:2008

Целите на овој стандард не се да воспостави метод за управување со ризици, туку, да обезбеди минимална рамка и да ги опише барањата, за самиот процес за проценка на ризиците, за идентификација на заканите и ранливостите кој ќе овозможи проценка на ризикот, нивото на ризикот, а потоа и да се дојде состојба при која ќе може да се одбере соодветен начин на справување со ризиците како и соодветни планови и мерки кои се насочени кон евалуација и подобрување на ситуацијата.

Стандардот дефинира дека треба да се одбере методот за проценка на ризици кој што соодветствува со овие барања со цел избегнување на неконзистентни или симплистички методи кои што не се соодветни со намерата на уредниците на стандадот.

3.1.4 Целите на МЕХАРИ

МЕХАРИ е конзистентно множество на алатки и методолошки специфики за управување со безбедноста на информациите и соодветните мерења, базирани за прецизна анализа на ризик. Основните аспекти на МЕХАРИ:

- неговиот модел на ризик (квалитативен и квантитативен),

- утврдување на ефикасноста на безбедносните мерки кои што се воспоставени или планирани,
- способност да се процени и симулира преостанатото ниво на ризик кое што е последица на применетите дополнителните мерки,

се комплементарни со задолжителните барањата на ISO/IEC 27000 стандардите, а посебно со ISO/IEC 27005.

3.1.5 Споредба на целите на МЕХАРИ и ISO/IEC 27001 и 27002 стандардите

Целите на МЕХАРИ и на предходно споменатите ISO стандарди се коренито различни.

- МЕХАРИ тежи кон обезбедување на алатки и методи кои што може да се искористат за избор на најсоодветните безбедносни мерки за дадена организација, како и за проценка на преостанатиот ризик кога мерките ќе бидат имплементирани. Сето ова не е примарна цел на двата ISO стандарда.
- ISO стандардите обезбедуваат множество на најдобри практики, кои што секако се многу корисни, но не значи дека се соодветни за поставеноста во организацијата. Тие се корисни за покривање на аспектите во однос на зрелоста од гледна страна на безбедноста, планирањето на безбедноста на информациите, независните внатрешни делови во самата организација и партнерите.

Прирачникот за безбеднонсни мерки од МЕХАРИ ефективно обезбедува детални елементи кои што можат да бидат искористени за изработка на безбедносна рамка, при што може да се спореди со ISO/IEC 27002. Од оваа гледна точка, јасно е дека МЕХАРИ покрива пошироко поле од ISO и ги покрива основните аспекти на безбедноста многу пошироко од покривањето само на информацискиот систем.

3.2. Компатибилност помеѓу двата пристапа

Пристапот на МЕХАРИ е целосно сообразен со ISO 27002 затоа што, иако наведените цели не им се исти, релативно е лесно да се претстават резултатите од МЕХАРИ анализата во облик на ISO 27002 индикатори и очекувани резултати.

МЕХАРИ одговара на потребата, изразена во ISO 27001 и 27002 стандардите, за анализа на ризиците со цел дефинирање на мерките што треба се применат.

3.2.1 Компатибилност со ISO/IEC 27002:2005 стандардот

Стандардните контролни точки или *најдобрите практики* од ISO главно се општи, културолошки или организациски мерки, додека МЕХАРИ, дополнително на нив, ја нагласува потребата од мерки чија ефикасност може да се гарантира.

И покрај овие разлики, прегледот на ранливости на МЕХАРИ обезбедува споредбени табели за приказ на индикаторите во линија на елементите кои се користат во ISO 27002:2005 стандардот. Овие споредбени табели се корисни за они кои што треба да обезбедат усогласеност со овој стандард.

Корисно е тука да се спомене дека прашалниците за ревизија (audit) на МЕХАРИ се изработени и пропишани на тој начин да се овозможи оперативните раководители

ефикасно да спроведат проверка на ранливостите и според нив да дојдат до заклучок за капацитетот на безбедносните мерки за намалување на тие ризици.

3.2.2 Компатибилност со ISO/IEC 27001 стандардот

МЕХАРИ може лесно да се интегрира во PDCA процесот (анг. Plan-Do-Check-Act--планирање-спроведување-проверка-дејствување) како што е наведено во ISO/IEC 27001, особено во фазата на „Планирање“ (§4.2.1). МЕХАРИ целосно ги опфаќа активностите кои што овозможуваат изработка на основите на ISMS (анг. Information Security Management System- системот за управување со безбедност на информации).

За фазата на „Спроведување“ (§4.2.2), која има за цел воведување и одржување на ISMS, МЕХАРИ обезбедува корисни почетни елементи како што е дефинирање на планови за управуавње со ризици, со приоретизација директно поврзана со класификација на ризикот и мерење на напредокот при употреба на системот.

За фазата „Проверка“ (§4.2.3), МЕХАРИ обезбедува елементи кои што овозможуваат проверка на преостанатиот ризик, како и подобрувања во однос на безбедносните мерки. Дополнително, сите промени на околината (влијанијата, заканите, системите и организацијата) може лесно повторно да се проценат преку фокусирани ревизии кои ги користат резултатите од првичната МЕХАРИ ревизија. На тој начин безбедносните планови може да се ревидираат и да се развиваат со текот на времето.

За фазата „Делување“ (§4.2.4), МЕХАРИ индиректно се повикува на контоли и на континуирано подобрување на безбедноста и на тој начин обезбедува остварување на целите за намалување на ризикот. Во овие три фази МЕХАРИ не е во центарот на процесот, но во голема мерка придонесува за нивно спроведување и ја обезбедува нивната ефикасност.

3.2.3 Компатибилност со ISO/IEC 27005:2008 стандардите

Рамките воспоставени од страна на овој нов стандард се целосно применливи преку начинот на кој што МЕХАРИ овозможува да се управува со ризиците, на пример:

- Процесот на анализа, проценката и третирањето на ризиците (превземени од ISO 13335),
- Идентификацијата на основните и споредните средства со додаток на нивоа на класификација поврзани со нив, која што произлегува од анализа на влијанијата,
- Идентификација на заканите вклучувајќи ги нивните нивоа (вообичаена изложеност), за која што МЕХАРИ е многу попрецизен при описот на ризичните сценарија,
- Идентификацијата и кванитфикација на ефикасноста на безбедносните мерки (или контроли) при намалување на ранливости,
- Комбинација на овие елементи за оценка на нивото на критичност за активирање на ризичните сценарија, користејќи скала од четири нивоа,
- Можноста за директен избор на безбедносни мерки потребни за спроведување на плановите за намалување на ризиците.

Поради тоа, МЕХАРИ не само што лесно се интегрира во процесот на ISMS, за што се залага ISO 27001, туку и целосно одговара на барањата поставени од страна на ISO 27005 како метод за управување со ризици.

КЛУБ ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИИ НА ФРАНЦИЈА

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

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

Download CLUSIF productions at:
www.clusif.fr