

Standardi sistemov za upravljanje varovanja informacij

Kazalo

Uvod.....	4
Zgodovina »7799«	5
Pregled	5
Iskanje mednarodnega priznanja.....	5
Certifikacijske sheme	6
BS7799 Part 2	6
c:cure – ali ne c:cure	7
Priprava ISO/IEC 17799	7
Part 2 revizija	7
Prvi član družine ISO 27000	8
Prihodnost standardov ISMS	9
Družina standardov ISO 27000.....	9
ISO/IEC 27000: Vocabulary and definitions	9
ISO/IEC 27001: Specification for an Information Security Management System.....	10
ISO/IEC 27002 (ISO/IEC 17799:2005): Code of Practice for Information Security Management	10
ISO/IEC 27003: Implementation guidance.....	11
ISO/IEC 27004: Information Security Management Metrics and Measurement	11
ISO/IEC 27005: Guidelines for information security risk management.....	12
ISO/IEC 27006: Guidelines for information and communications technology disaster recovery services.....	13
Vzpostavitev sistema upravljanja varovanja informacij	14
Integracija sistema vodenja varovanja informacij z drugimi sistemi vodenja.....	15
Pridobitev certifikata ISMS	16
Proces certifikacije.....	16
Dodatek A: Število ISMS certifikatov po državah	17

Uvod

Danes je upravljavcem varovanja informacij na voljo več standardov, dobrih praks, postopkov, politik in metodologij. Nekatere so namenjene vsem organizacijam (na primer standarda ISO/IEC 17799, BS 7799-2, priporočila GASSP, OECD Guidelines - navodila za varnost informacijskih sistemov in mrež), druge metodologije so bolj specializirane, na primer za produkte (Common Criteria/ISO 15408), za informacijsko tehnologijo (GMITS ISO 13335, okvir COBIT) in podobno. Med vsemi referenčnimi sistemi s področja varovanja informacij je najbolj celovit in v svetu najbolj priznan standard ISO 17799/BS 7799-2. Njegova uporaba je neodvisna od pojavne oblike informacije.

Naj si bo informacija v pisni, elektronski ali ustna obliki, takoj ko jo spoznamo kot vredno varovanja, postane predmet sistema upravljanja varovanja informacij. Varovanje informacij pomeni ohranjanje njene: zaupnosti, celovitosti in razpoložljivosti.

Praktiki varovanja informacij so zaradi vpetosti informatike in z njo povezanih tehnologij v naše poslovne procese ponavadi informatiki in prevečkrat se zgodi, da se varovanje informacij dojema preozko. Varovanje informacij dostikrat pojmujejo kot tehnološki problem, problem zgolj informatike in informatikov, v bistvu pa gre pri tem za problem upravljanja.

Zagotavljanje varnosti informacij ni zgolj postavitve požarnega zidu, uvedba nujne uporabe gesel ali izdelave varnostnih kopij, zagotavljanje varnosti informacij je mnogo več. Je že res, da je danes velika večina informacij v elektronski obliki, vendar so te informacije mnogokrat predmet groženj, ki ne bile tuje niti ljudem iz zgodnejših obdobj človekovega razvoja. Poplave, požari, tatvine opreme, vdori v zgradbe in poslovne prostore in na koncu, vendar ne najmanj pomembno, človeški faktor in z njim povezana pozabljivosti ali neprevidnosti tudi ogrožajo »elektronske« informacije.

Poleg tega je se še vedno srečujemo s precejšnjo količino informacij shranjenih in posredovanih v oblikah, ki bi jih težko označili kot elektronske. Pogovor je po mnenju mnogih še vedno najbolj učinkovit način izmenjave informacij. Pisarne brez papirja se nam še vedno zdijo precej oddaljene.

Področje zagotavljanja varnosti informacij je torej izredno široko in zahteva celovit pristop. Problema varovanja informacij se zaradi vseh njenih pojavnih oblik ne da rešiti izključno s tehničnimi ukrepi, ampak jih je vedno potrebno dopolnjevati z drugimi ukrepi, postopki, standardi in politikami.

Zgodovina »7799«

Pregled

Izvor ISO/IEC 17799 lahko iščemo v obdobju UK Department of Trade and Industry's (DTI) Commercial Computer Security Centre (CCSC). CCSC, ki je bil ustanovljen meseca maja 1987, je imel dve glavni nalogi. Prva naloga je bila pomagati ponudnikom izdelkom s področja varnosti IT vzpostaviti nabor mednarodno priznanih kriterijev za vrednotenje varnosti in s temi kriteriji povezano shemo vrednotenja in certificiranja. To je končno privedlo do ITSEC¹ in vzpostavitve UK ITSEC sheme.

Druga naloga je bila pomagati uporabnikom s pripravo kodeksa varovanja informacij ki je izšel leta 1989 kot »Uporabniški kodeks varovanja informacij«. Kodeks se je nadalje razvijal najprej v okviru National Computing Centre (NCC) in kasneje v okviru konzorcija uporabnikov, katerih večina je prihajala iz Britanske industrije. Ti udeleženci pri razvoju so stremeli k temu, da bi bil Kodeks s stališča uporabnikov razumljiv in praktičen. Rezultat teh prizadevanj je bil prvič objavljen kot dokument s smernicami British Standard PD 0003, A code of practice for information security management, in kasneje po javni razpravi kot British Standard BS7799:1995.

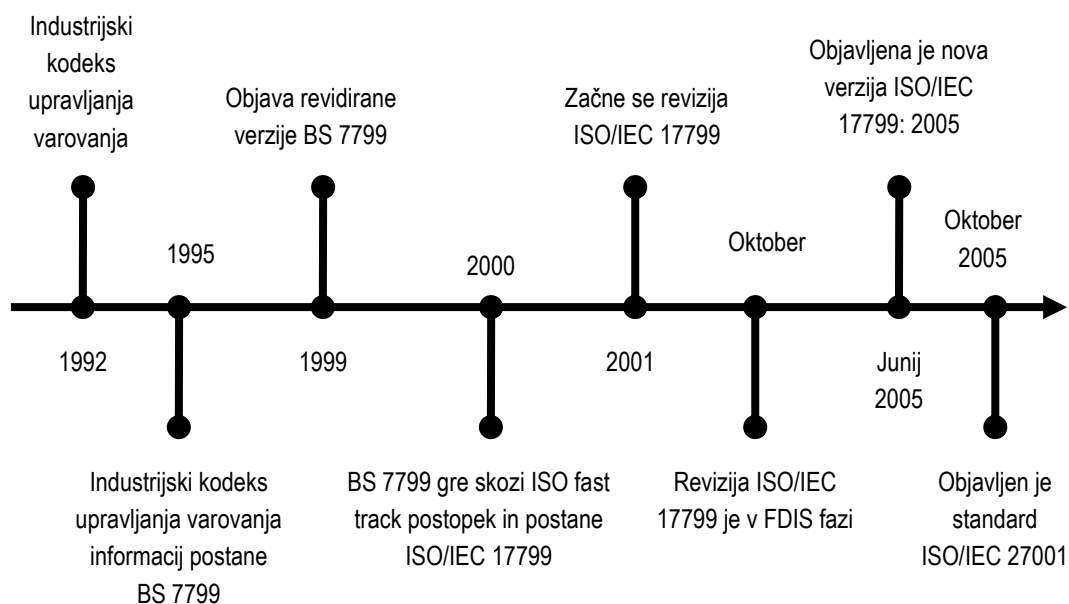
Drugi del BS7799-2:1998 je bil dodan v mesecu februarju leta 1998. Po obširni reviziji in javni razpravi, ki se je začela novembra 1997, je bila prva revizija standarda, standard BS7799:1999, objavljena aprila 1999. Prvi del standarda je bil oktobra 1999 po »Fast Track²« postopku predlagan v sprejem kot ISO standard. Z manjšimi dopolnili je bil 1. decembra 1999 objavljen kot ISO 17799:2000. BS 7799-2:2002 je bil uradno objavljen 5. septembra 2002.

Iskanje mednarodnega priznanja

Oktobra leta 1999 se ni zgodilo prvič, da je bil BS7799 predlagan za ISO standard. Začetna verzija standarda, BS7799:1995, je bila vložena v postopek že poleti 1995 vendar je bila vloga zavrnjena. Državam, ki so se zavzemale za sprejem standarda, to ni vzelo poguma. Avstralija in Nova Zelandija sta standard, z manjšimi predelavami sklicevanj na zakonodajo, sprejeli kot svoj nacionalni standard AS/NZS 4444. Nizozemska je standard sprejela v celoti in vzpostavila certifikacijsko shemo, ki je zaživela leta 1997. Zanimanje mednarodne skupnosti je opogumilo Britance, da so z razvojem standarda nadaljevali.

¹ Maja 1990 so Francija, Nemčija, Nizozemska in Velika Britanija na osnovi raziskav v posameznih deželah izdale Information Technology Security Evaluation Criteria (ITSEC). Po intenzivni mednarodni razpravi je junija 1991 Evropska Komisija izdala verzijo 1.2 za uporabo pri shemah vrednotenja in certificiranja sistemov varovanja informacij. ITSEC je strukturiran nabor kriterijev za vrednotenje računalniške varnosti v okviru izdelkov in sistemov. Od izdaje ITSEC leta 1990 se je precej Evropskih držav dogovorilo o priznavanju veljavnosti ITSEC vrednotenj.

² Standard, ki je bil razvit izven ISO odborov je vložen v t.i. »Fast Track« procesiranje. Standard je predložen neposredno kot ISO/DIS (Draft International Standard) v pet mesečno obdobje potrjevanja. Če DIS glasovanje pozitivno se pripravi končna oblika besedila in se predloži kot FDIS (Final Draft International Standard). FDIS gre skozi isti postopek potrjevanja in je nato ob pozitivnem izidu objavljen kot mednarodni standard.



Certifikacijske sheme

To, da so Nizozemci prvi vzpostavili certifikacijsko shemo, je precej ogorčilo Britance. Certifikacijska shema je vključevala revolucionarne ideje o osnovnem in naprednem nivoju certificiranja in o samocertificiranju in certificiranju s strani neodvisnega certifikacijskega organa. »Napredni nivo« certificiranja je dopuščal možnost, da bi bilo v resničnih razmerah mogoče potrebno poleg varoval iz BS7799 uporabiti še katera druga varovala. British Standards BDD/2 odbor, ki je odgovoren za BS 7799-2:2002 Information Security Management Systems - specification with guidance for use, je pozdravil te ideje in jih združil s svojimi idejami v zvezi s certifikacijo s strani neodvisnega organa. Tako je nastala »c:ure« certifikacijska shema.

BS7799 Part 2

Pojavila pa se je težava. Ker je bil BS7799:1995 kodeks varovanja informacij, kako bi presojevalec ocenil ali organizacija, ki jo presoja izpolnjuje kriterije. Dejansko, če bi bila vključena nadzorstva, ki niso opisana v BS7799, kako bi presojevalec vedel katera nadzorstva bi morala biti uporabljena in katera ne. Odgovor na to in podobna vprašanja smo dobili z BS7799 Part 2, ki natančno opredeljuje kaj morata organizacija in presojevalec narediti, da bi zagotovila uspeh postopka certifikacije.

Skoraj po naključju je priprava BS7799 Part 2 pripeljala do dramatičnega zaključka da je koncept ISMS³ v osnovi bolj pomemben od koncepta Kodeksa. Z vključitvijo raznih povratnih zank koncept ISMS vodjem omogoča nadzorovanje in kontrolo njihovih varnostnih sistemov in s tem

³ ISMS – Information Security Management Systems

zmanjševanje preostalega poslovnega tveganja in zagotavljanje da varovanje stalno izpolnjuje korporacijske zahteve, zahteve poslovnih partnerjev in pravne zahteve.

c:cure – ali ne c:cure

Manj kot dve leti po nastanku se je UK "c:cure" certifikacijska shema znašla pred izzivom, ki ga je pred njo postavil EA7/03 v obliki dokumenta z naslovom "Guidelines for the Accreditation of Bodies operating Certification/Registration of Information Security Management Systems". Ta dokument je bil dogovorjen in sprejet po celi Evropi in med člani European co-operation for Accreditation. Dokument je postal osnova za mnogo revizij, ki so jih neodvisne organizacije opravljale v ZDA, celinski Evropi, Afriki in Veliki Britaniji, in je bil sprejet tudi v drugi delih sveta. S spoznanjem širšega priznanja EA7/03⁴, je DTI 2. oktobra 2000, prekinil podporo shemi c:cure in na ta način je bila certifikacijska shema c:cure ukinjena. Zamenjala jo je mednarodno priznana in sprejeta norma.

Priprava ISO/IEC 17799

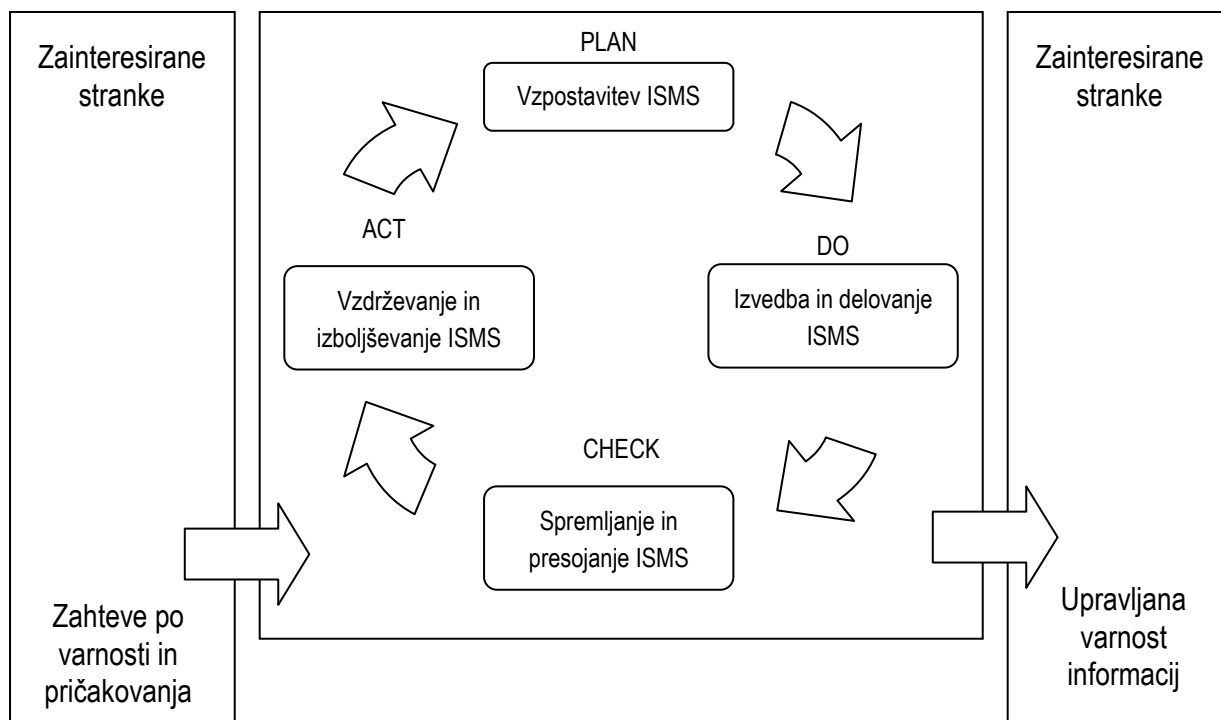
Po objavi BS7799:1999 v mesecu aprilu 1999, je bil Part 1 te nove verzije standarda v oktobru 1999 po »Fast Track« mehanizmu predlagan za ISO standard. Mednarodno glasovanje se je zaključilo avgusta 2000 in standard je bil potrjen z zahtevano večino glasov. Oktobra 2000 je bilo odobrenih osem manjših popravkov besedila BS in standard je bil 1. decembra 2000 objavljen kot ISO/IEC 17799:2000. 15. junija 2005 je bila objavljena zadnja verzija ISO/IEC 17799:2005.

Part 2 revizija

BS 7799 Part 2:2002 je bil objavljen 5. septembra v Londonu na konferenci BS 7799 Goes Global Conference. Nova izdaja BS 7799 Part 2 je bila pripravljena zaradi harmonizacije z ostalimi upravljavskimi standardi kot sta ISO 9001:2000 in ISO 14001:1996 z namenom omogočiti konsistentno in integrirano delovanje upravljavskih sistemov. Nova izdaja vpeljuje »Plan-Do-Check-Act« (PDCA)⁵ model kot del upravljavskega pristopa k razvoju, implementaciji in izboljševanju učinkovitosti sistemov upravljanja varovanja informacij v organizacijah. PDCA preprosto pomeni: odloči se kaj želiš, izvedi, preveri če deluje, izboljšaj tisto kar ne deluje in začni vse skupaj znova.

⁴ EA, European Co-operation for Accreditation, je neprofitno združenje, ki je bilo ustanovljeno novembra 1997 in registrirano kot združenje junija 2000 na Nizozemskem. EA je rezultat združevanja EAC, European Accreditation of Certification in EAL, European co-operation for Accreditation of Laboratories. EA je evropsko omrežje nacionalno priznanih certifikacijskih teles na geografskem področju Evrope.

⁵ PDCA (Shewhartov cikel, Demingov krog) strategija nadzora in upravljanja kakovosti s štirimi koraki. PDCA uporabljamo ponavljajoče, v najkrajših možnih ciklih, v navidezni spirali, ki nas pripelje do končnega cilja. V vsakem ciklu smo bližje komičnemu cilju. Ta pristop je zasnovan na spoznanju da so naše znanje in sposobnosti omejene vendar jih stalno izboljšujemo. Pogosto nimamo na voljo vseh informacij, ki bi jih potrebovali. Namesto, da bi se ujeli v smrten objem neskončnih analiz in iskanja takojšnje popolnosti, je bolje, da napredujemo z približno popolnostjo. Čez čas bomo pridobili več znanj, ki nam bodo omogočala boljše definiranje ciljev, in spretnosti, ki nam bodo pri doseganju ciljev pomagale.



Implementacija PDCA modela odseva principe, ki jih je predstavila OECD⁶ v svojih smernicah (OECD Guidelines for the Security of Information Systems and Networks, 2002) za upravljanje varnosti informacijskih sistemov in omrežij. Nova verzija Part 2 ponuja robusten model za implementacijo OECD principov pri ocenjevanju tveganj, načrtovanju in implementaciji varnosti, upravljanju varnosti in ponovnih ocenah varnosti.

Vključitev upoštevanja OECD smernic v BS 7799-2:2002, je izdajo dokumenta zakasnila do 5. septembra 2002. Zakasnitev izdaje je bila izvedena z namenom časovne uskladitve z izdajo smernic OECD. Poleg tega je bilo potrebno zagotoviti da so bila pravočasno pripravljena pravila UKAS⁷ za prehod iz BS 7799-2:1999 na BS 7799-2:2002.

Prvi član družine ISO 27000

Leto 2005 je bilo na področju ISMS pomembno še zaradi enega dogodka. ISO/IEC JTC 1/SC27, odbor, ki je odgovoren za ISO/IEC 17799, je 15. oktobra 2005 izdal prvega izmed standardov družine 27000. Nova shema označevanja ISMS standardov se bo v naslednjih petih do sedmih letih uporabljala za označevanje ISO standardov s področja ISMS. Prvi izmed standardov nove družine je standard ISO/IEC 27001. Novi standard je revizija standarda BS 7799-2:2002

⁶ Organisation for Economic Co-operation and Development

⁷ The United Kingdom Accreditation Service

Prihodnost standardov ISMS

Družina standardov ISO 27000

ISO/IEC JTC 1/SC27 odbor si je za prihodnost naložil delo pri razvoju nove družine standardov za sisteme upravljanja z varnostjo podatkov. Ta nova družina je družina standardov 27000.

- ISO/IEC 27000: Vocabulary and definitions
- ISO/IEC 27001: Specification for an Information Security Management System
- ISO/IEC 27002: Code of Practice for Information Security Management
- ISO/IEC 27003: Implementation guidance
- ISO/IEC 27004: Information Security Management Metrics and Measurement.
- ISO/IEC 27005: Guidelines for information security risk management
- ISO/IEC 27006: Guidelines for information and communications technology disaster recovery services

Pri razvoju standardov je začela tesno sodelovati tudi ITU-T tako, da bodo standardi objavljeni v sodelovanju obeh organizacij. ITU je že razvila ISMS zahteve za telekomunikacijske operaterje (dokument X.1501) ki temelji na BS 17799 Part 2:2002. Nadaljnji razvoj bo usklajen z razvojem ISO/IEC 27001. Pričakuje se, da bo vzpostavljeno sodelovanje tudi pri razvoju ostalih standardov družine 27000.

ISO/IEC 27000: Vocabulary and definitions

Standard ISO/IEC 27000 bo po vzoru ISO 9000 razlagal osnovne principe in bo vseboval besednjak in definicije, ki se bodo uporabljale v vseh ostali članih družine 27000. Varovanje informacij je, kot vsako tehnično področje, povezano s kompleksno terminologijo. Ni veliko avtorjev, ki bi se pri pisanju tehničnih besedil spopadli s problemom podrobne razlage pojmov. Pri standardih je to drugače. Neustrezno definirani pojmi vodijo v zmedo in razvrednotenje formalnih ocen in certifikacije.

Po predvidevanjih bo ISO/IEC 27000 precej podoben ostalim standardnim besednjakom in definicijam. Upamo, da bo njegova vsebina postala splošno sprejet besednjak strokovnjakov s področja varovanja informacij. Verjetno bo ISO/IEC 27000 vsrkal vase tudi vsebino dveh drugih smernic in sicer ISO/IEC Guide 2:1996 "Standardization and related activities – General vocabulary" in ISO/IEC Guide 73:2002 "Risk management – Vocabulary – Guidelines for use in standards".

ISO/IEC 27001: Specification for an Information Security Management System

Prvi standard družine 27000 je standard ISO/IEC 27001, ki je bil objavljen 15. oktobra 2005. Standard ISO/IEC 27001 izhaja iz standarda BS 7799-2:2002, ki so ga po celem svetu uporabljali za neodvisno revizijo in certifikacijo in je sedaj s prihodom naslednika ukinjen.

Oba stadarda, ISO/IEC 27001 (ISMS) in BS 7799 Part 2:2002 (ISMS), uporabljata »Plan-Do-Check-Act (PDCA)« procesni model kot sta ga privzela ISO 9001 (QMS) in ISO 14001 (EMS). PDCA procesni model definira cikel aktivnosti pri načrtovanju in vzpostavitvi ISMS, izvedbo in operativno uporabo ISMS, redni nadzor in preglede ISMS, in izboljševanje in dopolnjevanje ISMS na osnovi sprememb in novih zahtev okolja. Koncept procesnega cikla PDCA zagotavlja implementacijo učinkovitega varovanja informacij in učinkovitost vzpostavljenega varovanja informacij skozi stalno izboljševanje.

PDCA procesni model v ISO/IEC 27001 zajema nabor procesov upravljanja s tveganji. Namen teh procesov je identifikacija in ocenjevanje tveganj in vplivov tveganj z namenom obvladovanja ugotovljenih tveganj z različnimi upravljavskimi možnostmi. Ena izmed upravljavskih možnosti za obvladovanje tveganj je izbira in implementacija ustreznih nadzorstev. Dodatek A standarda ISO/IEC 27001 vsebuje nabor nadzorstev iz standarda ISO/IEC 17799:2005 izmed katerih lahko, glede na to katera tveganja moramo zmanjšati, izberemo ustrezna nadzorstva.

ISO/IEC 27002 (ISO/IEC 17799:2005): Code of Practice for Information Security Management

Zadnja verzija standarda ISO/IEC 17799 je bila objavljena 15. junija 2005. V zadnji izdaji standarda so mnoge novosti in izboljšave, katerih namen je vzdrževati sodobnost in skladnost priporočenih dobrih praks s trendi na področju varovanja informacij. Nova izdaja vsebuje tudi spremembe, ki se nanašajo na nove trende na področju poslovanja organizacij.

Novosti in izboljšave v ISO/IEC 17799 se nanašajo na:

- Povečano uporabo zunanjih storitev in zunanjega izvajanja in upravljanje varne uporabe teh storitev,
- Razširjena nadzorstva in smernice za upravljanje virov, ki obravnavajo zadeve kot sta 'sprejemljiva uporaba' in 'lastništvo',
- Na uvajanje novih tehnologij, kot sta brezžična omrežja in mobilno računalništvo, in načine uporabe teh tehnologij,
- Problem 'mobilne kode',
- Rast števila novih groženj in z njimi povezanih novih tveganj pri poslovanju organizacij in navezovanje na nadzorstva in smernice za obvladovanje incidentov,
- Celovit pristop k varnostnim vidikom, ki so povezani s človeškimi viri,
- Rastoč problem upravljanja ranljivosti, vključno z upravljanjem popravkov.

Nekaj izboljšav je bilo narejenih tudi na področju »prijaznosti uporabe« standarda. Uporabniki sedaj lažje razlikujejo med nadzorstvi in smernicami za implementacijo nadzorstev.

Revidirana verzija standarda ponuja organizacijam pomembno orodje za upravljanje tveganj na področju varovanja informacij, izboljšanje sposobnosti za obvladovanje incidentov in podporo zagotavljanju neprekinjenega poslovanja in s tem pomaga organizacijam pri izkoriščanju tržnih priložnosti. Ključni namen tega kodeksa je omogočiti podjetjem varovanje zaupnosti, celovitosti in razpoložljivosti občutljivih in kritičnih informacij.

Standard ISO/IEC 17799:2005 Code of practice for information security management je tesno povezan z novo družino ISMS standardov. Kljub tej tesni povezanosti v bližnji prihodnosti še ne bo prišlo do spremembe njegovega imena. Preimenovanje standarda ISO/IEC 17799:2005 v ISO/IEC 27002 naj bi se zgodilo v mesecu aprilu leta 2007. Zakasnitev preimenovanja je povezana z velikim uspehom, vzponom in tržno prisotnostjo ISO/IEC 17799 in bo omogočila bolj postopen prehod na novo shemo poimenovanja.

ISO/IEC 27003: Implementation guidance

V tem trenutku so na voljo samo neuradne informacije v zvezi s smernicami ISO/IEC 27003 ISMS implementation guidance. Odbor JTC1/SC27 se ukvarja z razvojem smernic katerih namen je nuditi pomoč pri implementaciji različnih elementov PDCA procesa iz standarda ISO/IEC 27001. Razvoj smernic se naslanja na Dodatek B standarda BS 7799 Part 2:2002. Po nekaterih predvidevanjih naj bi bil objavljen proti koncu leta 2008.

ISO/IEC 27004: Information Security Management Metrics and Measurement

Prav tako kot standard ISO/IEC 27003 je tudi standard ISO/IEC 27004: Information Security Management Metrics and Measurement v začetni fazi razvoja. Namen standarda ISO/IEC 27004 je ponuditi smernice in merila za merjenje učinkovitosti implementacije ISMS, tako procesa kot nadzorstev. Standard bo opredeljeval tehnike, ki jih lahko uporabimo za določanje in opisovanje učinkovitosti sistemov upravljanja varovanja informacij v skladu z ISO/IEC 27001. Standard obravnava sredstva (nadzorstva za varovanje informacij) in aktivnosti (processe in postopke za varovanje informacij).

Metrika se uporablja v glavnem za merjenje izvedbenih komponent⁸ ISMS (Implement and operate the ISMS), rezultati meritev pa služijo kot vhod za komponente faze preverjanja⁹ (Monitor and review). Rezultati meritev so osnova za sprejemanje odločitev in fazo ukrepanja¹⁰ (Maintain and improve), v okviru katere skrbimo za stalno izpopolnjevanje sistema upravljanja varovanja informacij.

⁸ »DO« faza PDCA cikla

⁹ »CHECK« faza PDCA cikla

¹⁰ »ACT« faza PDCA cikla

Standard ISO/IEC 27003 bo ponudil dragoceno orodje za pripravo kazalnikov učinkovitosti za primerjave in postavljanje ciljev.

ISO/IEC 27005: Guidelines for information security risk management

BS 7799 Part 3. "BS 7799-3:2006 - information security management systems - guidelines for information security risk management" je novi BS, ki naj bi bil objavljen v marcu 2006. Novi standard bo vseboval smernice v zvezi z obvladovanjem tveganj v smislu ISO/IEC ISO 27001.

Standard bo pokrival:

- Ocenjevanje in vrednotenje tveganj,
- Implementacijo ustreznih nadzorstev,
- Nadzorovanje in pregledovanje tveganj kot stalen ali periodičen proces;
- Vzdrževanje in stalno izboljševanje sistema nadzorstev.

BS 7799-3 poizkuša umestiti tveganja povezana z varovanjem informacij v širši kontekst poslovnih tveganj. Povezovanje varovanja informacij s poslovnimi cilji je dober način za nasprotovanje tradicionalno negativnemu pogledu na varnostna nadzorstva: nadzorstva zmanjšujejo tveganja in na ta način prispevajo k zmanjšanju potencialne škode, poleg tega pa vodstvu organizacije omogočajo, da bolj samozavestno ubira poti, ki se jih drugače izogibalo.

Glede na informacije, ki jih je objavil British Standards Institute, naj bi bil standard na voljo v marcu 2006. Standard BS 7799-3 podpira uporabo procesnega pristopa k ocenjevanju tveganj, obvladovanju tveganj in stalnemu nadzoru, pregledu in ponovnemu ocenjevanju tveganj. Procesni pristop vzpodbuja uporabnike standarda k poudarjanju pomembnosti:

- Razumevanja poslovnih zahtev varovanja informacij in potrebe vzpostavitve politike in ciljev varovanja informacij,
- Izbire, implementacije in delovanja nadzorstev v kontekstu splošnega obvladovanja poslovnih tveganj,
- Nadzorovanja in preverjanja delovanja in učinkovitosti sistema upravljanja varovanja informacij pri upravljanju tveganj,
- Stalnega izboljševanja na osnovi objektivnega merjenja tveganj

Predvideva se, da bo standard BS 7799-3:2006 v prihodnosti privzet standard ISO/IEC 27005. Trenutno še ni znano niti kdaj naj bi se to zgodilo niti ali bo standard BS 7799-3:2006 pred ali v procesu transformacije v ISO standard doživel še kakšne spremembe. Verjetno je, da bo v procesu

transformacije prišlo do zlitja dveh standardov, standarda ISO/IEC 13335¹¹ in standarda BS 7799-3, v standard ISO/IEC 27005, vendar so to zaenkrat samo še ugibanja.

ISO/IEC 27006: Guidelines for information and communications technology disaster recovery services

ISO je najavil začetek aktivnosti na pripravi standarda ISO/IEC 27006 "Guidelines for information and communications technology disaster recovery services". Standard ISO/IEC 27006 naj bi bil zasnovan na osnovi SS507¹² Singapore Standards for Business Continuity/Disaster Recovery (BC/DR) Service Providers. Objava standarda je predvidena za mesec november 2007. Informacije o standardu ISO/IEC 27006 so šele preliminarne tako, da lahko pride pred dejansko izdajo standarda do večjih ali manjših sprememb v vsebini in poimenovanju standarda.

¹¹ ISO TR 13335 Parts 1 to 5 (GMITS – Guidelines for the Management of IT Security). GMITS Part 3 – Risk Assessment

¹² Standard for Business Continuity / Disaster Recovery Service Providers (SS507) – Singapur je prva država, ki je vpeljala standard in program certificiranja za ponudnike storitev na področju zagotavljanja neprekinjenosti poslovanja in okrevanja po katastrofah (BC/DR). Standard je bil razvit v sodelovanju Infocomm Development Authority of Singapore (IDA) in IT Standards Committee (ITSC). Standard določa stroge zahteve za BC/DR ponudnike.

Vzpostavitev sistema upravljanja varovanja informacij

Vsaka organizacija bi morala razviti, implementirati, vzdrževati in stalno izpopolnjevati dokumentiran sistem upravljanja varovanja informacij v kontekstu njenih poslovnih aktivnosti in z njimi povezanih tveganj. V skladu s privzetim PDCA principom postopek vzpostavitve sistema upravljanja varovanja informacij razdelimo v štiri faze:

1. Vzpostavitev sistema
2. Implementacija in delovanje
3. Nadzor in pregled
4. Vzdrževanje in izboljševanje

Vzpostavitev sistema

V okviru faze vzpostavitve definiramo obseg sistema varovanja informacij v kontekstu poslovanja in organizacijske sheme organizacije, lokacije, sredstev in tehnologije. Po določitvi obsega moramo definirati varnostno politiko organizacije. Varnostna politika opredeljuje splošno usmeritev glede varovanja informacij, razne zahteve v zvezi z varovanjem informacij, strateški organizacijski kontekst in kontekst upravljanja s tveganji, kriterije za vrednotenje tveganj. Varnostno politiko mora potrditi vodstvo organizacije.

Po določitvi varnostne politike moramo definirati sistematični pristop k obvladovanju tveganj. Pri definiciji pristop k obvladovanju tveganj določimo metodo ocenjevanja tveganj, politiko zmanjševanja tveganj na sprejemljivo raven, kriterije za sprejem tveganj in nivoje sprejemljivega tveganja.

Določitvi sistematičnega pristopa k obvladovanju tveganj sledi identifikacija tveganj v okviru katere identificiramo vire in sredstva, grožnje, ki so jim izpostavljeni, ranljivosti, ki bi jih grožnje lahko izkoristile in vpliv, groženj in ranljivosti, na sredstva in vire.

Identifikaciji tveganj sledi ocena tveganj pri kateri ocenimo potencialno poslovno škodo, verjetnost dogodka, ki bi povzročil škodo, nivo tveganja in sprejemljivost tveganja.

Na osnovi pridobljenih informacij identificiramo in ovrednotimo možnosti za obvladovanje tveganj. Izberemo ustrezna nadzorstva, zavestno sprejmemo tveganja, se tveganjem izognemo ali pa jih prenesemo na nekoga drugega.

Ko smo za posamezna tveganja izbrali način obvladovanja in implementirali vsa izbrana nadzorstva pripravimo izjavo o uporabi nadzorstev in v njej dokumentiramo vsa implementirana nadzorstva in razloge zakaj smo jih implementirali, ravno tako za nadzorstva, ki jih nismo implementirali, navedemo razloge, ki so nas na to navedli.

Vodstvo mora potrditi sprejem ostanka tveganj in dati soglasje k implementaciji in delovanju sistema upravljanja varovanja informacij.

Implementacija in delovanje

V prvih korakih implementacije moramo poskrbeti za formulacijo načrta obvladovanja tveganj, ki vsebuje aktivnosti vodstva, odgovornosti in prioritete pri upravljanju tveganj. Formulaciji načrta obvladovanja tveganj sledi implementacija načrta, ki ima za cilj identifikacijo ciljev nadzorstev z opredelitvijo sredstev in odgovornosti za njihovo izvedbo. Sledi implementacija izbranih nadzorstev, usposabljanja in izobraževanja za dvig zavesti. Nato nastopi upravljanje sistema in virov in implementacija postopkov in drugih nadzorstev za ustrezen odziv na varnostne incidente.

Nadzor in pregled

V tej fazi skrbimo za pravočasno odkrivanje napak pri procesiranju informacij, identifikacijo neuspešnih in uspešnih vdorov v sistem in določamo aktivnosti za obvladovanje incidentov. Vodstvo organizacije spremlja ali se aktivnosti v okviru sistema varovanja informacij odvijajo po pričakovanjih.

Izvajamo tudi redne preglede učinkovitosti delovanja sistema upravljanja varovanja informacij. Pri tem se poslužujemo rezultatov presoj, incidentov, predlogov in povratnih informacij vseh zainteresiranih strank.

Preverjamo stopnjo ostanka tveganj in sprejemljivega tveganja. Pri tem upoštevamo spremembe v organizaciji, tehnologiji, poslovnih ciljih in procesih, identificiranih grožnjah in zunanjih dogodkih. Izvajamo načrtovane interne presoje in vodstvene preglede. Beležimo aktivnosti in dogodke, ki bi lahko imeli vpliv na učinkovitost sistema upravljanja varovanja informacij.

Vzdrževanje in izboljševanje

Organizacija, ki je vzpostavila sistem upravljanja varovanja informacij bi morala redno razvijati in implementirati izboljšave sistema in zagotavljati, da izboljšave dosežejo predvidene cilje, izvajati korekcijske in preventivne ukrepe, sporočati informacije o stanju sistema vsem zainteresiranim strankam.

Integracija sistema vodenja varovanja informacij z drugimi sistemi vodenja

Vključitev bistvenih elementov standarda ISO/IEC 27001 v druge sisteme vodenja (npr. vodenja kakovosti po zahtevah standarda ISO 9001, ravnanja z okoljem po zahtevah standarda ISO 14001 ali varnosti in zdravja pri delu po zahtevah standarda OHSAS 18001) lahko omenjene sisteme vsebinsko dopolnjuje in izboljšuje ter povečuje njihovo učinkovitost in uspešnost.

Pri odločitvi za izpopolnitev vzpostavljenega sistema vodenja varovanja informacij z elementi ISO/IEC 27001 mora organizacija slediti predvsem svojim potrebam.

Pridobitev certifikata ISMS

Na tem mestu lahko omenimo, da je standard ISO/IEC 17799:2005 kodeks varovanja informacij in da certifikacija po tem standardu ni mogoča. Standard ISO/IEC 17799:2005 ni bil nikoli načrtovan s tem namenom in ni primeren za ta namen. Nasprotno je bil standard ISO/IEC 27001 Information Security Management System pripravljen prav z namenom za certifikacijo.

ISO/IEC 27001 je revidirana verzija standarda BS 7799 Part 2: 2002, standarda, ki se že sedem let uporablja za akreditirano certifikacijo. Postopek certifikacije po standardu ISO/IEC 27001 je identičen postopku certifikacije po standardu ISO 9001 Quality management system (QMS) in standardu ISO 14001 Environmental management system (EMS). Sedaj ko je standard ISO/IEC 27001 objavljen je bil standard BS 7799 Part 2:2002 ukinjen in nadaljnje certifikacije se bodo izvajale po standardu ISO.

Mednarodni register ISMS akreditiranih certifikacijskih organov je na voljo na spletišču XISEC.

Proces certifikacije

Proces certifikacije v grobem sestoji iz treh faz. V prvi fazi se podjetje pripravlja na certifikacijo. V tej pripravljalni fazi podjetje razvije in implementira svoj sistem upravljanja varovanja informacij, vzpostavljen sistem integrira v svoje vsakodnevne poslovne procese in aktivnosti, usposobi svoje zaposlene in izvaja proces vzdrževanja sistema upravljanja varovanja informacij.

V drugi fazi podjetje najame akreditiran certifikacijski organ, ki izvede presojo sistema upravljanja varovanja informacij. V prvem delu presoje se presojevalec osredotoči na vzpostavljenost in dokumentiranost sistema upravljanja varovanja informacij. Lahko se ga deloma izvede izven organizacije in zajema:

- pregled varnostne politike in ciljev,
- pregled obsega sistema, podpornih postopkov in kontrol,
- poročilo o oceni tveganja, vpeljane programe in ukrepe za zniževanje tveganj,
- izjavo o primernosti, itd.

Drugi del certifikacijske presoje izvedemo v organizaciji. Poudarek je na izvajanju in učinkovitosti sistema vodenja varovanja informacij, izpolnjevanju zahtev standarda ISO/IEC 27001, zakonskih zahtev in zahtev zainteresiranih strank.

V primeru, da je presoja uspešna podjetje pridobi certifikat. Certifikat se podeljuje za obdobje treh let, po triletnem obdobju je potrebna ponovna certifikacija. Tretja faza, če lahko tako poimenujemo, je faza vzdrževanja in izboljševanja sistema upravljanja varovanja informacij v kateri certifikacijski organ v rednih časovnih intervalih (na 6 do 9 mesecev) obiskuje organizacijo in preverja ali organizacija še izpolnjuje predpisane zahteve.

Dodatek A: Število ISMS certifikatov po državah

Japonska	1338	Švedska	7	Ruska Federacija	2
Velika Britanija	229	Španija	6	Slovaška	2
Indija	157	Turčija	6	Južna Afrika	2
Tajvan	77	Brazilija	5	Armenija	1
Nemčija	56	Grčija	5	Bahrajn	1
Italija	42	Islandija	5	Čile	1
Koreja	37	Kuwait	4	Egipt	1
ZDA	34	Mehika	4	Libanon	1
Nizozemska	27	Filipini	4	Litva	1
Kitajska	26	Saudska Arabija	4	Luksemburg	1
Madžarska	26	Argentina	3	Makedonija	1
Hong Kong	21	Kanada	3	Maroko	1
Avstralija	18	Otok Man	3	Nova Zelandija	1
Finska	15	Združeni arabski emirati	3	Katar	1
Norveška	13	Belgija	2	Romunija	1
Švica	13	Kolumbija	2	Srbija in Črna gora	1
Češka	12	Hrvaška	2	Slovenija	1
Irska	11	Danska	2	Tajska	1
Singapur	11	France	2		
Avstrija	9	Makao	2	Skupaj	2292
Poljska	8	Malezija	2		

Vir: ISMS International User Group 2001-2005.

Viri

1. ISMS International User Group, <http://www.xisec.com>
2. International Organization for Standardization (ISO), 1, rue de Varembé, Case postale 56, CH-1211 Geneva 20, Switzerland, <http://www.iso.org>
3. Jože Knez, SIQ in Albin Nedižavec, Termo, Varovanje informacij s standardom ISO/IEC 27001 v obstoječih sistemih vodenja
4. Gamma Secure Systems Limited, Diamond House, 149 Frimley Road, Camberley, Surrey GU15 2PS, United Kingdom, <http://www.gammassl.co.uk>
5. ISO 27001 Security, <http://www.iso27001security.com>