Információ biztonsági „program” kifejlesztése

Információ biztonsági„program” forrásai

A források közé általába a következők tartoznak:

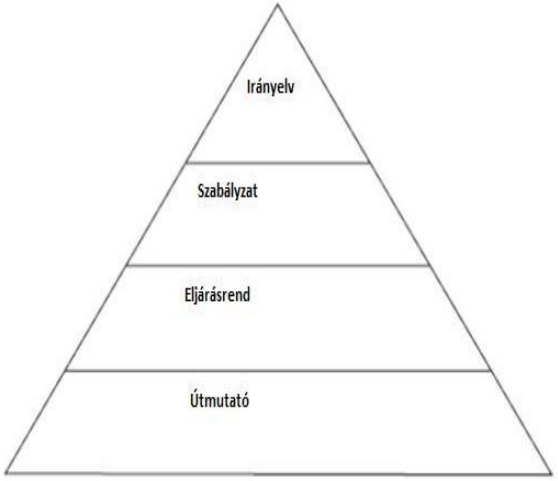
- Dokumentáció
- Architektúra
- Ellenőrzési mechanizmusok, óvintézkedések
- Ellenintézkedések
- Technológia
- Alkalmazottak, szerepkörök/munkakörök/felelősség/hatás és feladat körök, képesség, szakmai képzettség
- Tudatosság terjesztése és oktatás
- Auditok
- Megfelelőség/szabályszerűség kikényszerítése
- Fenyegetések elemzése
- Sebezhetőség elemzése
- Kockázat és gazdasági/üzleti/igazgatási következmények elemzése/értékelése
- Erőforrások kölcsönös függőségének elemzése
- Külső biztonsági szolgáltatást nyújtók
- Egyéb szervezeti támogatások

Dokumentálás

Információ biztonsági program dokumentációja alatt a következő elemeket értjük:

policies, standards, procedures and guidelines.

Biztonsági irányelvek, szabályzat, eljárásrend és útmutatók



Architektúra

- Architecture is the high-level, conceptual configuration of the relationships between
  - Network topologies
  - Operating systems
  - Applications
  - Middleware
  - High-tech widgets
  - Devices
- Architecture specifies the high-level arrangement of technology features and functionality with which required functionality could be designed and configured

- Architektúra magas szintű, az architektúra építő elemek közti kapcsolatok fogalmi szintű leírása
  - Hálózati topológia
  - Operációs rendszerek
  - Alkalmazási rendszerek
  - Köztes rendszerek /szoftverek
  - Csúcstechnológiai kütyük
  - Egyéb berendezések
- Az architektúra a technológiai eszközök sajátosságainak és funkcionális szolgáltatásainak magas szintű leírását tartalmazza, amelynek segítségével a kívánt funkcionális szolgáltatások megtervezhetők és összeépíthetők.

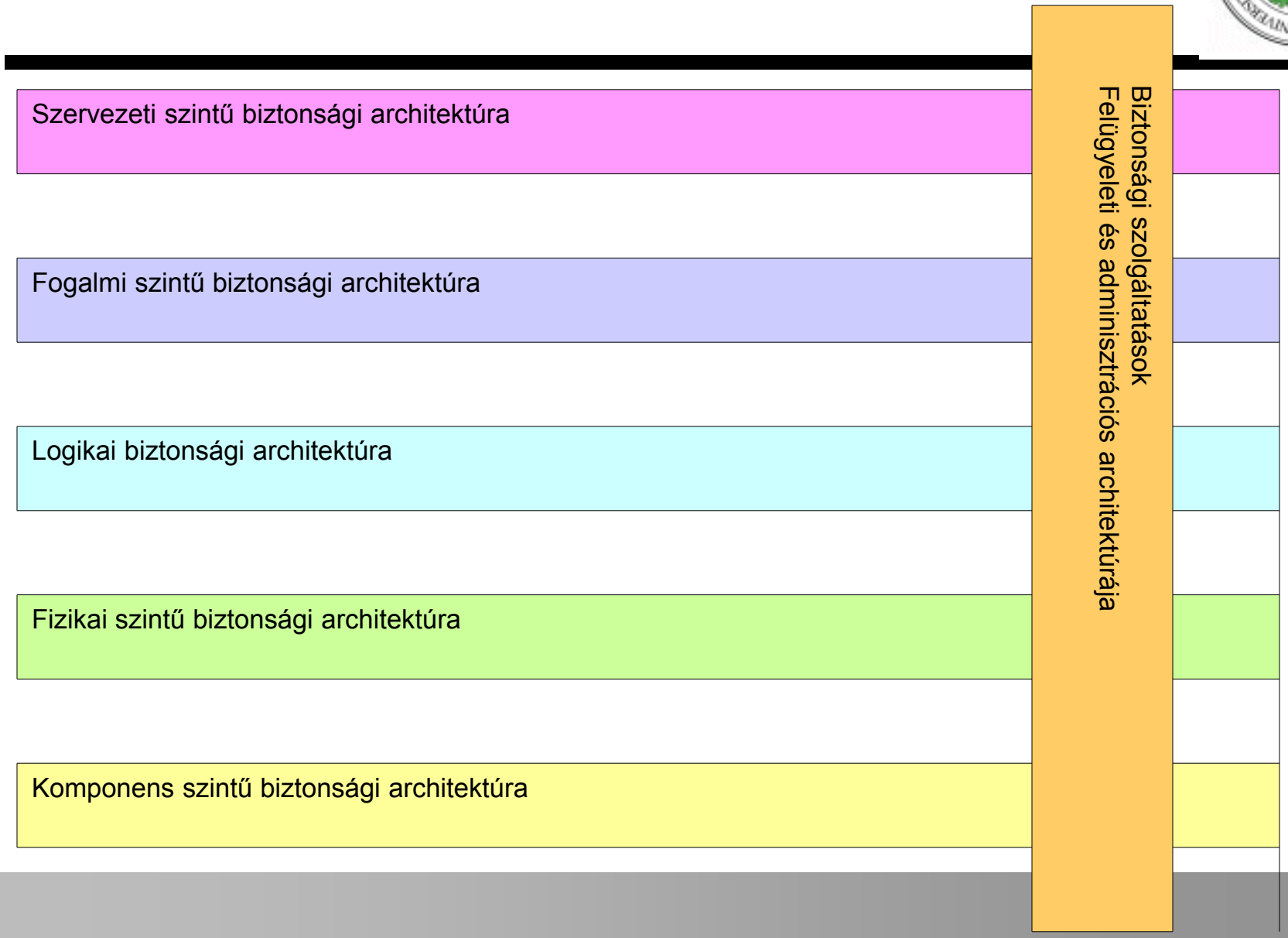
Megvalósítási lehetőségek

Nyilvános keretrendszere	Vezetett megvalósítás
Irányelvek szintje COBIT: ingyenes NIST: ingyenes ISO 27000/…: $...	SABSA
Szabvány szint ISO 15408: $.....	
Eljárásrend szintje	Saját fejlesztés szükséges

Az IT tervezés Zachman féle keretrendszere

J. A. Zachman S. H. Spewak	Entitások = mit? adatot, adat architektúra	Tevékenységek = hogyan? funkciót alkalmazási architektúra	Helyek = hol? hálózatban műszaki architektúra	Személyek = ki?	Idő = mikor?	Motiváció =miért?	
Tervező célkitűzések/ kiterjedés	A szervezeti feladatok listája	A szervezeti folyamtok listája	A szervezet telephelyeinek listája	A szervezet legfontosabb egységeinek listája	A szervezetnek fontos események listája	A szervezeti célok/stratégiák listája	Kiterjedés
Tulajdonos Szervezeti modell	Sematikus modell	Szervezeti folyamatmodell	Szervezeti logisztikai rendszer	Munkafolyamat modell	Központi munkaterv	Üzleti, szervezeti terv	Szervezeti modell
Fejlesztő Információs rendszer modell	Logikai adat modell	Alkalmazási architektúra	A rendszer földrajzi elhelyezkedésé-nek architektúrája	Ember-gép kapcsolati architektúra	Feldolgozási struktúra	Szervezeti szabályok	Rendszer modell
Kivitelező Technológiai modell	Fizikai adatmodell.	Rendszerterv	Rendszerarchi-tektúra /technológiai architektúra	Megjelenítési architektúra	Ellenőrzési struktúra	Szabályzat tervezés	Technoló-giai modell
Végrehajtó (alvállalkozó) Részletes specifikáció	Adat definíció szótár vagy könyvtár	Programok támogató szoftver elemek	Hálózati architektúra	Biztonságtechni-kai architektúra	Időzítés definiálása	Szabályzat meghatározása	Elemek
Működő vállalat/intéz-mény	Adatok	Funkciók	Hálózat	Szervezet	Munkaterv	Stratégia	

SABSA


Szervezeti szintű biztonsági architektúra
Fogalmi szintű biztonsági architektúra
Logikai biztonsági architektúra
Fizikai szintű biztonsági architektúra
Komponens szintű biztonsági architektúra
Biztonsági szolgáltatások
Felügyeleti és adminisztrációs architektúrája

A biztonsági szolgáltatások kezelésének architektúrája

Szervezeti szintű réteg	Szervezeti motivációk, hajtóerők kialakítása; szervezeti szintű kockázatok elemzése, értékelése; szolgáltatáskezelés, kapcsolatkezelés, teljesítmény kezelés, beszállítói, ellátási hálózat kezelése.
Fogalmi szintű réteg	A szervezet **sajátosságai profiljának kialakítása**, működési kockázati kezelés célkitűzéseinek kidolgozása a kockázat elemzés segítségével, szolgáltatás nyújtásra tervkészítés, szolgáltatási szerep /feladat /munka /felelősség /hatáskörök, szervezeti kultúra értéktételezéseinek meghatározása, szolgáltatás portfólió kezelés, a szolgáltatási katalógus megtervezése, napra készen tartása, a szolgáltatások teljesítmény kritériumainak és célkitűzéseinek kezelése (szolgáltatási szintek meghatározása).
Logikai réteg	Informatikai vagyon/ tárgyi eszköz kezelés, irányelvek/ házirend kezelése, szolgáltatásnyújtás kezelésem ügyfélszolgálat, szolgáltatás katalógus kezelése, és a szolgáltatás értékelés kezelése.
Fizikai szintű réteg	Informatikai vagyon/ tárgyi eszköz biztonsága és védelme, működési kockázatokra vonatkozó adatok gyűjtése, üzemeltetés, felhasználó támogatás, szolgáltatási erőforrások védelme, szolgáltatás teljesítmény adatok gyűjtése.
Komponens szintű réteg	Eszközök védelme, üzemeltetési / működési kockázatokat kezelő eszközök, eszközök telepítése, alkalmazottak delegálása, biztonsági eszközök, szolgáltatás monitorozó, felügyleti eszközök.

Szakterületek együttműködése

A szervezeti architektúra

Funkcionális/üzleti architektúra

Információs architektúra

Alkalmazási architektúra

A szervezet alapfeladatainak eredményes végrehajtását biztosító architektúrák

Szervezeti biztonsági architektúra

Műszaki architektúra

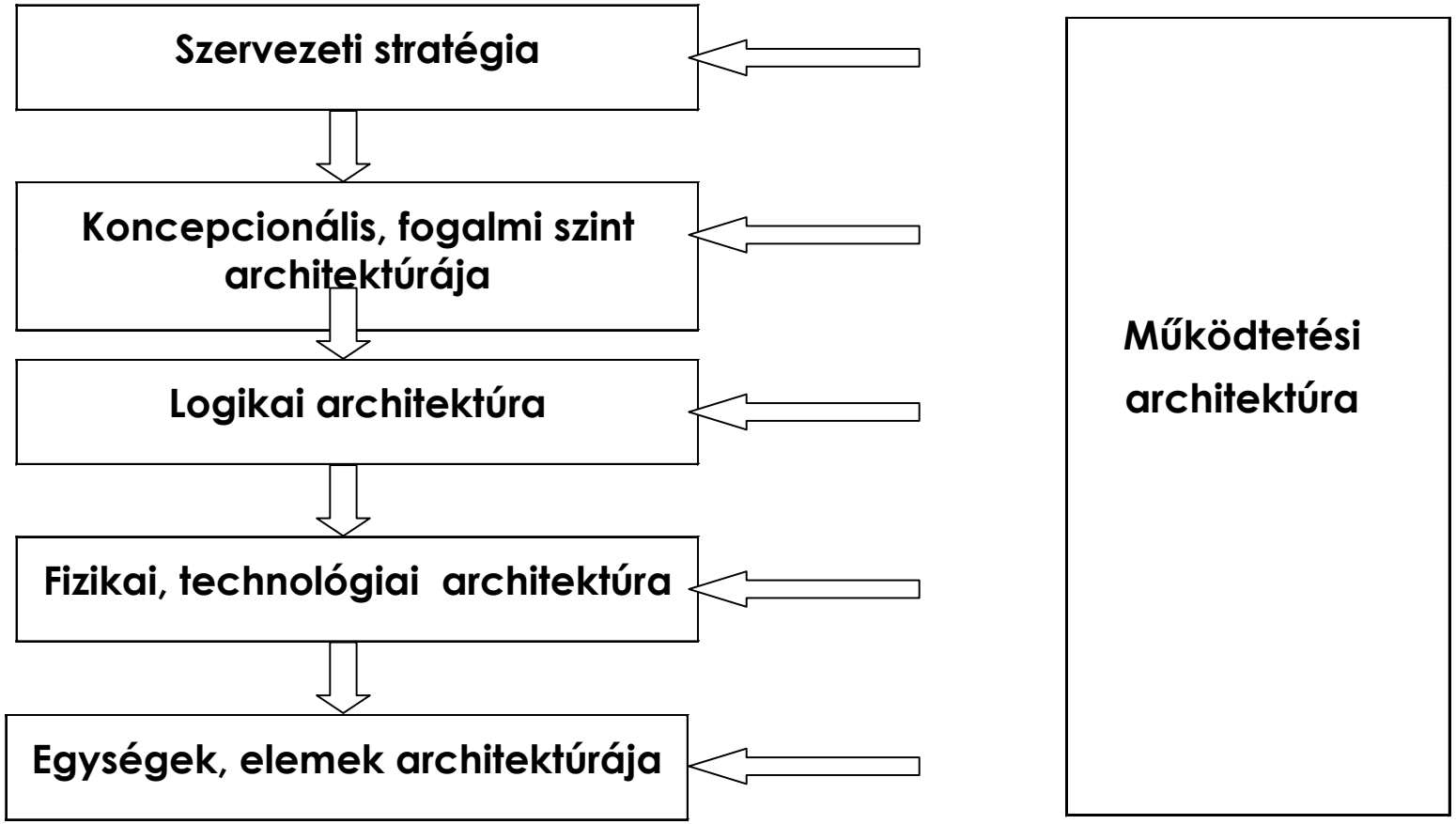
Termék architektúra

Szolgáltató infrastruktúra, a szervezet alapfeladatainak eredményes végrehajtását támogató architektúrák

Miért? Mit? Hogyan? Hol? Ki? Mikor?

J. A. Zachman S. H. Spewak keretrendszer	Biztonsági architektúra		
Tervkészítő (szervezeti/üzleti/stratégia) célkitűzések/kiterjedés	Üzleti vetület (összefüggések)	Miért?	Szervezeti biztonsági stratégia
Tulajdonos, vezető Szervezeti modell	Szervezeti vetület (irányelvek)	Mit?	Szervezeti politika, biztonsági, Irányelevek architektúrája
Fejlesztő Információs rendszer modell	Tervezői vetület	Hogyan?	Logikai architektúra
Kivitelező Technológiai modell	Kivitelezői vetület	Hogyan, hol?	Fizikai, technológiai architektúra
Végrehajtó (alvállalkozó) Részletes specifikáció	Integrációs vetület	Mivel?	Egységek, elemek architektúrája
Működő vállalat/intézmény	Üzemeltetési vetület	Ki, mikor?	Működtetési architektúra

Biztonsági architektúra modellje



Az IT tervezés
Zachman féle keretrendszere

.	Eszközök (Mit?)	Folyamatok (Hogyan?)	Helyszínek (Hol?)	Emberek (Ki?)	Idő (Mikor?)	Motiváció (Miért?)
Szervezeti vetület (Összefüggések rétege)	**Mi a rendszer típusa, mi a terméke? A cég védendő értékei: jó hírnév védel-me, a védendő információk**	**Hogyan működik? A védendő üzleti folyamatok (tranzakciók, kommunikáció)**	**Hol működik? Zárt rendszer, több telephely, külső partnerek, nyílt, országos /nemzetközi kapcsolatok**	**Ki használja? Szervezeti és menedzselési kérdések, ellátási lánc, stratégia partnerek, outsourcing**	**Mikor használja? Határidők, ciklusok, azonnali igények, terhelés megoszlás, csúcsok**	**Miért használja? Üzleti célok, sikertényezők, működési kockázatok**
Szervezeti architektúra vetület (Koncepciók rétege)	**Mit kell megvédeni? Üzleti titok, szer-vezeti egységek, kapcsolataik**	**Hogyan mű-ködjön a véde-lem? Felső szintű biztonsági straté-giák: PKI, alkal-mazás védelem**	**Hol vannak a vé-dendő területek? A védelem hely-függősége, biz-tonsági domainek**	**Ki menedzsel? Menedzselés szervezeti modell-je: biztonsági hatóságok, PCA, CA, RA**	**Mikor kell a védelem? Időpont, tartam? Jelszó, tanúsítvány élet-ciklus, CLR idő**	**Miért fontos? Szervezeti kocká-zat elemzés, se-bezhetőség és költség hatékonys**
Tervezői vetület (System engineering, Logikai réteg)	**Védendő adat-entitások és kapcsolatuk, PKI tanúsítvány, CA**	**Biztonsági szol-gáltatások: hite-lesség, teljesség, letagadhatatlan s**	**Védelmi terület definiálása, biz-tonsági domainek logikai, fizikai, stb.**	**A jogosultsági profilok: felhasz-náló, rendszer-gazda, auditor**	**A biztonsági folyamat ciklusa jogosultság, tanú-sítvány kiadáskor**	**Biztonsági politikák köve-telményei, CPS, helyi domain pol.**
Kivitelezői vetület (Fizikai réteg)	**Védendő adatstruktúrák: üzenetek, táblák, elektr. aláírások**	**A biztonsági me-chanizmus: titko-sítás, vírus véde-lem, AC szerverek**	**A biztonságtech-nológiai infra-struktúra elemeinek helye**	**Biztonsági fel-használói interfé-szek képernyő formája**	**Az ellenőrzési rendszer működtetéséne k időrendje**	**Biztonsági szabályok, feltételek és tevékenységek**
Inegrációs vetület (Elemek rétege)	**Adatmezők és címek részletes specifikációja**	**Termék és eszköz: hardver, szoftver és a vonatkozó szabványok**	**Számítógépes fo-lyamatok, cso-mópontok címei és protokollok**	**Felhasználói azonosítók, kivé-telek és ACL-ek**	**Biztonsági tevékenységek időtartama és sorrendje**	**Biztonsági tevékenységek és intézkedések**
Üzemeltetési vetület, réteg	**Üzemeltetési biztonság: bizal-masság, teljesség, authentikusság**	**Felhasználók és rendszerek biztonsági adminisztrációj a, mentések,**	**Hálózatok és plat-formok biztonsá-ga a szabványok alkalmazásával**	**Felhasználók, operátorok és adminisztrátoro k támogatása**	**Biztonsági tevékenységek időbeosztás sze-rinti végzése**	**Az üzemeltetés folyamatosságá -nak és biztonságának fenntartása**

Az ellenőrzési mechanizmusok mint a megvalósítás stratégiájának forrásai

- Controls are policies, procedures, practices, technologies and organizational structures designed to provide reasonable assurance that:
  - Business objectives will be achieved
  - Undesirable events will be prevented or detected and corrected
- Controls should be automated as far as possible

Az ellenőrzési mechanizmusok:

- irányelvek, eljárásrendek, napi gyakorlat/rutin, műszaki megoldások, technológiák, és szervezeti felépítés, amelyet arra terveztek, hogy ésszerű garanciát nyújtson a következő tekintetében:
  - A szervezeti/üzleti/igazgatási célkitűzéseket el fogják érni
  - A nem kívánt eseményeket meg fogják akadályozni, vagy észlelni fogják, és a következményeket pedig korrigálják
- Az ellenőrzési mechanizmusokat és az óvintézkedéseket amennyira az csak lehetséges automatizálni fogják

SABSA mátrix
Biztonsági szervezeti architektúra

	Vagyon/Eszköz (MI)	**Motiváció (Miért)**	**Folyamat (Hogyan)**	**Humán (Ki)**	**Helyszín (Hol)**	**Idő (Mikor)**
Szervezeti szintű architektúra	*Szervezeti/igazgatási döntések*	*Üzleti kockázatok*	*Szervezeti (vállalati, üzleti)* ***folyamatok***	*Szervezet igazgatása*	*Szervezeti (vállalati, üzleti) földrajzi elhelyezkedése*	*A szervezeti (vállalati, üzleti) tevékenységek időtől való függése*
	Az szervezeti (vállalati, üzleti) vagyon, eszközök, beleértve a célokat és célkitűzéseket	Lehetőségek és fenyegetések leltára	A szervezeti (vállalati, üzleti) működtetésére szolgáló folyamatok leltára	Szervezeti (vállalati, üzleti) felépítés, és a „kiterjesztett szervezet".	Az építmények, épületek, telephelyek, tartományok, igazságszolgáltatás, joghatóság kiterjedése, stb.	A szervezeti (vállalati, üzleti) célkitűzések időfüggése
Fogalmi szintű réteg	Szervezeti/vállalati ismeretek, kockázati stratégia	Kockázat kezelési célkitűzések	A folyamatok korrektségének szavatolása	Jogosultságok, felelősség-, feladat-, és hatáskörök	Keretrendszer számítógép-hálózati tartományokra	Az időmenzió kezelésének keretrendszerei
	Szervezeti/vállalati profil attribútumai	Feltételek megteremtése, ellenőrzési célkitűzések, Irányelvek architektúrája	A folyamatok leképezésének keretrendszere: IKT-ra architektúra stratégia	Felelősök „tulajdonosok/gazdák", gondnokok, végfelhasználók; Szolgáltatás nyújtók és ügyfelek/fogyasztók	Biztonsági tartomány fogalmai és átfogó kockázatkezelési keretrendszerek	Az egész életciklust keretrendszer
Logikai réteg	Információvagyon	Kockázat kezelési irányelvek	Folyamatok és szolgáltatások leképezése, leírása	Entitások és a kölcsönös bizalom keretrendszere	Számítógép hálózati tartományok térképe/topológia	Naptár, ütemtervek, menetrend
	Az Információvagyon leltára	Számítógép hálózati tartományokra vonatkozó irányelvek	Információáramlás; Funkcionális transzformációk;	Entitások sémája; Kölcsönös bizalom modelljei;	A tartományok meghatározásai;	Indítási időpontok; Élettartam, határidők

SABSA mátrix
Biztonsági szervezeti architektúra

Komponens szintű réteg	IKT komponensek	Kockázat kezelési eszközök és szabványok	Szolgáltatási folyamat támogató eszközök és szabványok	Humán erőforrás kezelés eszközei és szabályai	Számítógép hálózat lokációs eszközök és szabványok	Lépések ütemezése, sorrend kialakítását támogató eszközök
	IKT termékek, beleértve az adatokat, repozitóriumokat, adat szótárakat és folyamataikat	Kockázat elemzési eszközök Kockázat katalógus Kockázatok monitorozása és jelentés készítő eszközök.	Szolgáltatás nyújtás eszközei és protokolljai	Személyazonosság kezelése, munkaköri leírások, szerepkörök; funkciók; Tevékenységek, Hozzáférési jogosultsági listák	Csomópontok, címek és egyéb címazonosítók	Ütemező; óra időmérő, interrupt kezelő
Szolgáltatás kezelés architektúrája	Szolgáltatás nyújtás kezelése	Üzemeltetési/működési kockázatok menedzsment	Információfeldolgozási folyamatok menedzsmentje	Humán erőforrás menedzsment	Környezet menedzsment Az épületek, telephelyek, platformok és számítógép-hálózat menedzselése	Idő és teljesítménykezelés
	Az üzemeltetés folyamatosságának és kiválóságának szavatolása	Kockázat becslés, értékelés; Kockázat monitorozás és jelentéskészítés Kockázatokkal való foglalkozás	A rendszerek támogatás, menedzselése, alkalmazások és szolgáltatások	Felhasználó bejegyzésekről gondoskodás Végfelhasználók támogatása	Az épületek, telephelyek, platformok és számítógép-hálózat menedzselése	A naptár és menetrend, ütemrend kezelése

SABSA mátrix

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

SABSA mátrix összehangolva az ITIL v3-al

	Vagyon/Eszköz (MI)	**Motiváció (Miért)**	**Folyamat (Hogyan)**	**Humán (Ki)**	**Helyszín (Hol)**	**Idő (Mikor)**
	Szolgáltatás nyújtás kezelése	Üzemeltetési/működési kockázatok menedzsment	Információfeldolgozási folyamatok menedzsmentje	Humán erőforrás menedzsment	Környezet menedzsment Az épületek, telephelyek, platformok és számítógép-hálózat menedzselése	Idő és teljesítménykezelés
	A fentebbi sor a SABSA mátrix 6. sorának megismétlése. Az alábbi öt sor annak a kibontása, hogy a 6. réteg hogyan viszonyul a többi réteghez.					
Szervezeti szintű architektúra	A szervezeti (vállalati, üzleti) motivációk, hajtóerők kialakítása	szervezeti (vállalati, üzleti) kockázatok értékelése	Szolgáltatás menedzsment	Kapcsolattartás	A szolgáltatás nyújtási pont menedzselése	Teljesítmény menedzsment
	szervezeti (vállalati, üzleti) összemérés, összehasonlítás, szervezeti (vállalati, üzleti) motivációk, hajtóerők feltárása	A belső és külső tényezők elemzése	Az ügyfél számára értéket jelentő szolgáltatásnyújtáshoz szükséges szolgáltatási kapacitások menedzselése	A szolgáltatás nyújtók és a szolgáltatást igénybevevők kezelése	Igénykezelés; szolgáltatásnyújtás, telepítés és felhasználás	szervezeti (vállalati, üzleti) szempontú teljesítmény célok meghatározása

SABSA mátrix összehangolva az ITIL v3-al

Fogalmi szintű réteg	„Proxy Asset” kialakítása (Információvagyon helyettesítő)	ORM (Opportunity and Risk Method) Lehetőségek és kockázatok módszere céljainak kialakítása	Szolgáltatás nyújtás tervezése	Szolgáltatás menedzselés szerepkörei Szerepkörök, feladat, felelősség, hatáskörök, meghatározása, pénzbeli kötelezettségek, kulturális értékek	Szolgáltatás portfolió	Szolgáltatási szintek meghatározása (SLA)
	szervezeti (vállalati, üzleti) attribútumok profiljának létrehozása (=Információvagyon helyettesítő), kulcs fontosságú teljesítmény indikátorok (KPI), kulcs fontosságú kockázati mérőszámok (Key Risk Indicator, KRI)	Kockázat elemzés szervezeti (vállalati, üzleti) attribútumok profiljának, a helyettesítő információvagyon (Proxy Asset) alapján	SLA tervkészítés, üzletvitel, ügymenet folyamatosság, pénzügyi tervezés és ROI (Return on Investment), Áttéréstervezés		A szolgáltatási katalógus megtervezés és napra készen tartása	A szolgáltatás teljesítmény szempontrendszerének és célértékeinek meghatározása

SABSA mátrix összehangolva az ITIL v3-al

Logikai réteg	Eszköz, vagyon menedzsment/gazdálkodás	Irányelvek kezelése	Szolgáltatás nyújtás menedzsmentje	Szolgáltatás ügyfelének, fogyasztójának támogatása	Szolgáltatás katalógus menedzsment	Kiértékelés
	Tudásmenedzsment, Termék/szolgáltatás kibocsátás és telepítéskezelés; Teszt és validáció menedzsment	Irányelvek kialakítása Irányelvek megfelelőségének ellenőrzése, auditálása	SLA kezelés, Szállítók menedzselése; Üzlet/ügymenet folyamatosság fenntartása; költségek kezelése/ gazdálkodás; Áttérés menedzsment	Jogosultság kezelés, elhasználói jogosultságok. elhasználói bejegyzések kezelése és létrehozása	Konfigurációkezelés; kapacitástervezés; rendelkezésre állás	Monitorozás, nyomon követés, jelentéskészítés; Teljesítmény kontra KPI és KRI

SABSA mátrix összehangolva az ITIL v3-al

Fizikai szintű réteg	Eszköz/vagyon biztonság védelme	Működési kockázatok adatainak gyűjtése	Üzemeltetés/ működtetés	Végfelhasználók támogatása	Szolgáltatás erőforrásainak védelme	Szolgáltatás teljesítmény adatok gyűjtése
	Változáskezelése; Szoftver és adat épség/sértetlenség védelme	Működési kockázatok kezelésének architektúrája.	„Job” ütemezés; Rendkívüli események és események (incidensek) kezelése; Katasztrófa utáni helyreállítás	Szolgáltatás ügyfél szolgálat; Problémakezelés; Kérelmek kezelése	Fizikai és környezeti biztonság	Rendszer és szolgáltatás monitorozásának architektúrája
Komponens szintű réteg	Eszközök védelme	ORM eszközök	Eszközök telepítése	Humán erőforrás munkába állítása	Biztonsági eszközök	Szolgáltatás monitorozó eszközök
	Termékek és eszközök biztonságának és épségének/sértetlenségének fenntartása	ORM elemzés; Monitorozás és jelentéskészítés, és megjelenítő eszközök.	Termékek és eszközök kiválasztása, beszerzése; Projekt menedzsment	Munkaerő felvétel Fegyelmi eljárások Kiképzés Tudatosság erősítő eszközök	Az üzembe helyezett eszközök és termékek fizikai és logikai biztonságának fenntartása	Szolgáltatások elemzése, monitorozása, jelentéskészítés és megjelenítő rendszerek.

SABSA mátrix a szolgáltatások kezelésére összehangolva az ITIL v3-al

Table 4: SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
CONTEXTUAL ARCHITECURE	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities for Providing Value to Customers	Managing Service Providers & Service Customers; Contract Man'ment	Demand Man'ment; Service Supply, Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing ORM Objectives	Service Delivery Planning	Service Management Roles	Service Portfolio	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Risk Analysis on Business Attributes Proxy Assets	SLA Planning; BCP; Financial Planning & ROI; Transition Planning	Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Service Catalogue	Managing Service Performance Criteria and Targets
LOGICAL ARCHITECTURE	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management; Test & Validation Management	Policy Development; Policy Compliance Auditing	SLA Management; Supplier Management; BCM; Cost Management; Transition Management	Access Management; User Privileges, Account Administration & Provisioning	Configuration Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Asset Security & Protection	Operational Risk Data Collection	Operations Management	User Support	Service Resources Protection	Service Performance Data Collection
	Change Management; Software & Data Integrity Protection	Operational Risk Management Architecture	Job Scheduling; Incident & Event Management; Disaster Recovery	Service Desk; Problem Man'ment; Request Man'ment	Physical & Environmental Security Management	Systems and Service Monitoring Architecture
COMPONENT ARCHITECTURE	Tool Protection	ORM Tools	Tool Deployment	Personnel Deployment	Security Management Tools	Service Monitoring Tools
	Product & Tool Security & Integrity; Product & Tool Maintenance	ORM Analysis, Monitoring and Reporting Tools & Display Systems	Product & Tool Selection and Procurement; Project Management	Recruitment Process Disciplinary Process Training & Awareness Tools	Products & Tools for Managing Physical & Logical Security of Installations	Service Analysis, Monitoring and Reporting Tools & Display Systems

Az ellenőrzési mechanizmusok mint a megvalósítás stratégiájának forrásai

An ISM must recognize the security value of technology product features independently of the label given to a product by the product vendor

Mechanisms that embody the following principles are often used

- Access control (MAC & DAC)
- Secure failure
- Principle of least privilege
- Compartmentalize to minimize damage
- Segregation of duties
- Transparency
- Trust
- Trust no one

Egy informatikai biztonsági felelősnek a műszaki, informatikai termékek biztonsági sajátosságait fel kell tudnia ismerni függetlenül attól, hogy a gyártó/szállító hogyan pozícionálja a termékét

A következő ellenőrzési mechanizmusokat lehet használni

- Hozzáférési jogosultság lista
- Berendezések meghibásodása esetén a biztonság fenntartása az elsődleges
- A minimálisan szükséges jogosultságok engedélyezése
- Károkozás következményeinek szakaszolása
- A feladat és hatáskörök elhatárolása
- Átláthatóság
- Transparency
- Kölcsönös bizalom kialakítása
- De ne bízzunk meg senkibe.

Ellenintézkedések, óvintézkedések

Countermeasures are controls that are put into place in response to a specific threat that is known to exist

They may be:

- Preventive
- Detective
- Corrective

Az ellenintézkedések, óvintézkedések, olyan ellenőrzési mechanizmusok, amelyeket olyan fenyegetésekkel szemben hoznak meg, amelyek előre tudhatók.

Az ellenintézkedések és óvintézkedések a következők lehetnek:

- Megelőző
- Észlelő
- Helyre állító /korrigáló

Technológiák

The choice of technology to reduce information security-related risks is constrained by the legacy architecture of the organization

Through decades of evaluation of alternative preventive, detective and recovery controls, solid tools and techniques to achieve information security goals are now widely available

A szervezet elavult technológiájú architektúrája behatárolja azoknak a technológiáknak a körét, amelyeket fel lehet használni a biztonsággal kapcsolatos kockázatok mérséklésére.

Az elmúlt évtizedekben felhalmozódott tapasztalatok az alternatív technológiák értékelésében, a megelőző, észlelő és helyreállító ellenőrzési mechanizmusok tekintetében, amelyek célja az információ biztonsági célok megvalósítása, ma már széles körben rendelkezésre állnak.

Technológiák

Technologies commonly used include:

Access control lists

System configuration files that allow a system to identify authorized system usage and block system usage that is not specifically authorized

Choke routers

Network devices that form gateways or bridges between two networks, only allowing traffic matching predefined rule sets to pass between the networks

Content filtering

A way to prevent files from moving through a control point by scanning their contents and either letting them pass or blocking them based on a list of predefined rules

Általában használt technológiák:

Hozzáférési jogosultsági lista

Rendszer konfiguráció állományok, amelyek az azonosított és hitelesített rendszer használatot lehetővé teszik, azonban megakadályozzák a jogosulatlan rendszer felhasználást

Lefojtó útvonal irányító

Hálózati eszközök, amelyek két hálózat közötti átjáróként használnak, és csak olyan adatforgalmat engednek át, amely az előre definiált szabályrendszernek megfelel

Tartalom szűrés

Az állományok tartalmának vizsgálata annak érdekében, hogy megakadályozzák azt, hogy az állomány az ellenőrzési ponton túljutva károkat okozhasson. A szabályrendszer szerint vagy továbbengedik, vagy megakadályozzák a belépését a rendszerbe.

Technológiák

Database management systems:

- Technology used to efficiently store and retrieve data by making use of predefined indexes that define data records
- Relied upon by most access control models

Encryption (public key, symmetric or secret key encryption):

- An algorithm used to obscure information so that only those
- Intended can restore it to its original form
- Used to preserve confidentiality of data but may also be used for data integrity checking and non-repudiation

Adatbázis-kezelő rendszerek:

- Az adatok tárolásának és visszakeresésének hatékony technológiája, amely előredefiniált indexelési eljárást alkalmaz, amely meghatározza, hogy melyek az egyes adatrekordok

Sifrírozás, rejtjelezés, kriptográfiai, algoritmikus információ védelem (nyilvános kulcs, szimmetrikus vagy titkos kulcsú sifrírozás):

- Olyan algoritmus, amely az információ elrejtésére szolgál olyan módon, hogy csak azok ismerhessék meg, akik erre illetékesek, és az eredeti formát vissza tudják állítani.
- Az információ titkosságának, bizalmasságának megőrzésére szolgál, továbbá az adatok épségének sértetlenségének és letagadthatatlanságának ellenőrzésére.

Technológiák

Hashing

An algorithm that takes any input and produces a standard length output that obscures the original message and that cannot be used to recreate it, but can be used again on the same message to result in the same output

Open Systems Interconnection (OSI) model

A standard for network communications that defines a framework for implementing protocols in seven layers

Zagyválás

Olyan algoritmus, amely tetszőleges adatbemenetre egy szabványosított hosszúságú kimenetet hoz létre, amely elfedi az eredeti üzenetet, és ezt az algoritmust nem lehet felhasználni az eredeti üzenet rekonstruálására, de ugyanarra az üzenetre ugyanazt az eredményt adja

Open Systems Interconnection (OSI) modell

A hálózati kommunikáció egyik szabványa, amely leír egy keretrendszert a hét rétegen belül megvalósítandó protokollok számára

Technológiák

Layers in the ISO/OSI model are:

- **Application layer** - interface to applications
- **Presentation layer** - a layer at which information is “repackaged” to move up or down the OSI stack
- **Session layer** - reliable end-to-end communications
- **Transport layer** - end-to-end communications
- **Network layer** - packets, global routing
- **Data link layer** - datagrams, switching
- **Physical layer** - cables, electrical signals

Az ISO/OSI modell rétegei:

1. **Applikációs (alkalmazási) réteg:** Az applikációk (fájlátvitel, e-mail stb.) működéséhez nélkülözhetetlen szolgáltatásokat biztosítja.
2. **Megjelenítési (prezentációs) réteg:** Feladata a különböző csomópontokon használt különböző adatstruktúrákból eredő információ-értelmezési problémák feloldása.
3. **Viszony réteg:** Ez a réteg építi ki, kezeli és fejezi be az applikációk közötti dialógusokat (session, dialógus kontroll).
4. **Szállítási réteg:** Megbízható hálózati összeköttetést létesít két csomópont között. Feladatkörébe tartozik pl. a virtuális áramkörök kezelése, átviteli hibák felismerése/javítása és az áramlásszabályozás.
5. **Hálózati réteg**: Összeköttetést és útvonalválasztást biztosít két hálózati csomópont között. Ehhez a réteghez tartozik a hálózati címzés és az útvonalválasztás (routing).
6. **Adatkapcsolati réteg:** Megbízható adatátvitelt biztosít egy fizikai összeköttetésen keresztül. E réteg probléma köréhez tartozik a fizikai címzés, hálózati topológia, közeghozzáférés, fizikai átvitel hibajelzése és a keretek sorrendhelyes kézbesítése. Az IEEE két alrétegre (MAC, LLC) bontotta az adatkapcsolati réteget.
7. **Fizikai réteg:** Elektromos és mechanikai jellemzők procedurális és funkcionális specifikációja két (közvetlen fizikai összeköttetésű)eszköz közötti jeltovábbítás céljából.

Technológiák

Operating systems

Programs that directly interface with computer hardware to allow users to run software

Some security features include verbose and reliable logging mechanisms, and file recovery mechanisms

Public key encryption

Public key encryption is a type of encryption algorithm that utilizes two keys, the public key and the private key

One is used to encrypt; the other is used to decrypt

Operációs rendszer

Egy olyan progam, amely közvetlenül kapcsolódik a hardverhez, és lehetővé teszi a szoftverek futtatását.

Néhány biztonsági szolgáltatás: részletes és megbízható naplózási mechanizmus, állomány (file) rendszer.

Nyilvános kulcsú sifrírozás

A Nyilvános kulcsú sifrírozás egy olyan kriptográfiai algoritmus, amely két kulcsot használ, a nyilvános és magánkulcsot. Az egyiket használja a sifrírozásra, a másikat a visszafejtésre.

Technológiák

Route filtering

A way to program network devices so that they only route network traffic to or from defined sets of network addresses. If there is no route to or from a device, no data can travel to it

Symmetric key encryption

An encryption algorithm in which the key that is used to encrypt a set of data is also the key required to decrypt that data

Útvonal szűrés

A hálózati eszközök olyan programozása, amely egy előre meghatározott hálózati cím halmazból engedi meg vagy hálózati forgalom befogadását vagy oda a továbbítását. Ha egy adott eszköz számára nem létezik ilyen előre definiált útvonal, akkor semmilyen adat nem kerülhet továbbításra abba az irányban.

Szimmetrikus kulcsú sifrírozás

Olyan kriptográfiai algoritmus, amelyben a kulcsot mind sifrírozásra mind visszafejtésre használjuk.

Technológiák

Transmission Control Protocol/Internet Protocol (TCP/IP) and IPSec key encryption

Network communications protocols that follow the OSI model in which the data sent are divided into headers and data, where the header allows network devices to route packets between source and destination while the data are read as streams by the application layer

TCP/IP és IPSec sifrírozás

Számítógép hálózati protokollok halmaza, amelyek az OSI modellre alapulnak. A továbbított adatokat szétbontják fejlécre és az adatokra.A fejléc alapján tudják a hálózati eszközök az egyes csomagok esetében az útvonal irányítást végrehajtani a forrás és a célállomás között miközben az adatokat az alkalmazási réteg mint adatfolyamot folyamatosan olvassa be.

Munkatársak, szerepkörök, jogosultságok, felelősség-, feladat-, és hatáskörök, képzettség és képességek

Roles

Allow responsibilities and/or access rights to be assigned based on the fact that an individual performs a function rather than having to assign them to individual people

Responsibility

A responsibility is a description of some procedure or function that someone is accountable to perform.

Place responsibility where it may be expected that the skills necessary to perform the job will be core competencies of personnel assigned to the role, despite staff turnover

Skills

Training, expertise and experience held by the personnel in the given job function

Szerepkörök

E fogalom lehetővé teszi azt, hogy a hozzáférési **jogosultságokat** annak alapján lehessen megadni, hogy egy munkatárs vajon melyik *funkció* végrehajtására jogosult, és nem az egyes munkatársak személyéhez kell kötni

Jogosultságok, felelősség-, feladat-, és hatáskörök

A felelősség valamilyen funkció vagy eljárás leírását jelenti, amelynek végrehajtásáért valaki felelősségre vonható.

E felelősség-, feladat-, és hatásköröket ahhoz a szerepkörhöz kell helyezni, ahol a szükséges képzettség, képesség, szakmai gyakorlat fellelhető, a munkatársak fluktuációja ellenére

Képzettség, képesség, szakmai gyakorlat

Elvégzett tanfolyamok, kiképzés, szakértelem és szakmai tapasztalatok, amellyel az adott munkakörben dolgozó alkalmazott rendelkezik

Biztonsági tudatosság

Background and training is necessary for execution of tasks

Training classes should be tailored for those with security job responsibilities

An information security awareness program must also include end-user training

Biztonsági ellenőrzés és kiképzés szükséges ahhoz, hogy a munkafeladatok elvégezéséhez felhatalmazást kapjanak

Biztonsági munkakörökben foglalkoztatandók kiképzésére testre szabott tanfolyamok kialakítása

A biztonsági tudatosság emelése érdekében a végfelhasználók számára képzés

3.11.7 Security Awareness (continued)

End users cannot be expected to seek information on security and should be exposed to information on organizational standards relating to:

- Backing up work-related files
- Choosing passwords wisely and protecting them from exposure
- Avoiding e-mail and web-based viruses
- Recognizing social engineers
- Reporting security incidents
- Securing electronic and paper media against theft and exposure
- Spotting malware that could lead to identity theft and desktop spying

3.11.8 Audits

- Security audits have objectives, scope, constraints, approach and results
- Effectiveness is judged on the basis of whether or not controls in place meet a given set of control objectives
- An information security program should have established policies and standards

3.11.8 Audits (continued)

- An audit is extremely useful in identifying whether those policies and standards have been fully implemented
- Where an information security program is under development, the ISM may
  - Select externally published standards
  - Engage an audit team to determine the extent to which his/her own organization is in compliance

3.11.8 Audits (continued)

Different standards publications focus on one or more of these types of items:

- COBIT lists control objectives
- The Standard of Good Practice for Information Security
- SANS Institute
- International Organization for Standardization *Code of Practice for Information Security Management*, ISO/IEC 17799:2005, and corresponding *Information Security Management Systems Requirements*, ISO/IEC 27001:2005
- The Center for Internet Security (CIS)

3.11.9 Compliance Enforcement

- Compliance enforcement has two connotations
  - Compliance with respect to a regulatory environment
  - Compliance with respect to internal policies, standards and procedures

3.11.9 Compliance Enforcement (continued)

- Enforcement activities are management oversight functions by which the control activities designed to achieve an objective of compliance are supervised
- Compliance enforcement is any activity within the information security program designed to ensure compliance with the organization's control objectives

3.11.10 Threat Analysis

Numerous threats exist that may impact security program efforts and objectives. Threats must be evaluated to determine:

- If they are viable
- The likelihood that they will materialize
- Their potential magnitude
- The potential impact

3.11.10 Threat Analysis (continued)

Possible threats may include:

- Unclear objectives
- Carelessness
- Mistakes
- Deficient strategy
- Poor planning
- Inadequate resources
- Incorrect specifications
- Faulty execution

3.11.11 Vulnerability Analysis

- A vulnerability is a characteristic that allows a threat to occur
- Vulnerabilities can be characterized by whether:
  - They were intentionally maliciously created or not
  - Whether they exist in system development or operations
- A vulnerability analysis is designed to identify vulnerabilities in a given information system or environment
- ISMs need to be able to perform a vulnerability analysis in order to ascertain whether controls are adequate

3.11.12 Risk and Business Impact Assessment

BIA

- Determines the impact of losing the support of any resource to an organization
- Establishes the escalation of that loss over time
- Identifies the minimum resources needed to recover
- Prioritizes the recovery of processes and supporting systems

BIAs are based on risk

3.11.12 Risk and Business Impact Assessment (continued)

An information security program should have a process by which:

- Business impact of damage to any information resource is reassessed periodically
- Assessment is used to determine requirements for security measures with respect to that resource

3.11.13 Resource Dependency Analysis

Resource dependency analysis can, to a large extent, replace a BIA for the purposes of developing business continuity plans.

It is based on determining the applications used by a business operation in conducting its primary activities and the resources (networks, databases) needed to perform required functions

3.11.14 External Security Service Providers

- Two types of security services can be obtained from external providers
  - Outsourcing
  - Service contracting*
- Any outsourced activity must be consistent with the goals and objectives of the overall information security program
- Security program elements that monitor outsourced security functions must not themselves be outsourced

*The distinction between outsourcing security and contracting for security services is that when services are contracted for, the ISM retains ownership of and responsibility for the performance of the security service

3.11.15 Other Organizational Support

Subscription services can be integrated into an information security program to leverage external expertise without actually assigning them responsibility for executing any part of the security program.

Types include:

- Best practice organizations
- Security networking roundtables
- Security training organizations
- Vulnerability alerting services

3.12 Implementing an Information Security Program

Assumptions:

- Objectives for the security program have been defined and agreed upon by stakeholders
- Information security program resources required to form the building blocks of the program are in place
- IT controls have been defined and are operational, although not necessarily optimized
- Security reviews and audits are available to indicate where weakness and program gaps exist
- Management supports information security program activities

3.12.1 Policy Compliance

- Policy forms the basis for all accountability with respect to security responsibilities throughout the organization
- In most large organizations the ISM designates formal security roles that hold the department head responsible for getting processes that maintain security policy compliance for a given set of information systems in place

3.12.1 Policy Compliance (continued)

The ISM must:

- Ensure that, in the assignment process, there are no "orphan" systems or systems without policy-compliance owners
- Further provide oversight to ensure that policy compliance processes are properly designed

Where a policy document is deemed to have such little benefit that it may be bypassed, an ISM should use that feedback to effect change being termed the Policy Exception Process

3.12.2 Standards Compliance

- Standards must be designed to ensure that all systems of the same type are configured and operated in the same way.
- As far as possible, compliance with standards should be automated to ensure that system configurations do not, through intentional or unintentional activity, deviate from policy compliance.
- Executive management signs off on policy, while standards simply provide a standard method for complying with policy.
  - If there are deviations, there should be no dispute among executive management that the security program is intact.

3.12.3 Training and Education

- Information security programs are almost always dependent on people following instructions - training is thus critical
- Awareness and educational materials should be readily available to those with responsibility for policy enforcement
- Where this type of communication occurs, a user will become accountable for activity that attempts to deviate or bypass any control
- Users will subsequently
  - Understand why policy is enforced in a certain way
  - Be more accepting of activities designed to enforce policy compliance

3.12.4 Controls

The ITGI identifies 11 control objectives in *COBIT 4.1* as the minimum controls needed to be in place to ensure systems security:

- Management of IT security
- IT security plan
- identity management
- User account management
- Security testing, surveillance and monitoring
- Security incident definition
- Protection of security technology
- Cryptographic key management
- Malicious software prevention, detection and correction
- Network security
- Exchange sensitive data

3.12.4 Controls (continued)

Each of the 11 control objectives must be supported with policy, standards, technology and control activities as well as enforcement of control points

The ISM should develop general controls that cover all control objectives listed, and implement application controls only if general controls are not suitable for a given business application or process

3.12.5 Countermeasures

- An information security program must be flexible enough to be able to implement a control or countermeasure with very little advance warning
  - At the same time, an ISM should discourage anyone from making any changes to production systems outside of an authorized change control
- Countermeasures are not always technical in nature

3.12.6 Third-party Service Providers

- Issues concerning sharing data with a service provider should be specifically addressed by senior management
- An information security program may have a policy that includes requirements for protecting data that must be shared with third-party service providers
- If use of third-party services is widespread, standards and procedures for system security are appropriate if systems interfaces are accessible to the service providers

3.12.6 Third-party Service Providers (continued)

When using a 3rd party, ISM's should:

Describe how data are stored & secured in the service provider environment in a way that maintains CIA

Allocate resources to maintain a secure environment

Take responsibility for the security of the service

Maintain accountability in the service provider organization for policy enforcement

Maintain security processes so they are transparent to customers

Maintain well defined procedures

3.12.6 Third-party Service Providers (continued)

- A third-party service must commit to specific company security practices before data are shared with this service
- Requirements should to the maximum extent be
  - Contractual
  - Verified by external auditors or other independent parties acting on behalf of the contracting organization
- If an ISM works for the contracted service, he/she should implement processes to ensure that contractual requirements for information security are met

3.12.7 Integration into Life Cycle Processes

- A key to policy compliance is having a policy-compliance owner for each deployed information system
- To maintain accountability for policy compliance through frequent change, a security program must identify where IT changes are initiated, funded, and deployed
- The ISM must create hooks into processes so that those in job functions that specify, purchase and deploy new systems have policy compliance as part of their job functions
- Gives the ISM time to identify vulnerabilities in new systems, identify new threats presented by systems & assist the implementation team to develop policy-compliant pre-approved standards for production deployment

3.12.8 Monitoring and Communication

Performance monitoring enables senior management to tell if the program is working.

- The ISM must:
  - Identify metrics
  - Specify how they are to be gathered
  - Justify how they are used
  - Use the same metrics as those used to manage the program
- If security incidents presenting risk to the organization are identified, the ISM must:
  - Communicate this risk to senior management
  - Facilitate immediately acting on senior management's decisions

3.12.9 Documentation

- In the context of the information security program development, all documents described in the resource section are resources with which to execute the program
- The program itself creates a plethora of documents
- While standards policies, standards, role and responsibility descriptions, announcements, memos, etc. are needed to run/execute the program, they are resources for the program to use, not documentation of the program itself
- An umbrella document should serve as a guidebook to help independent parties

3.12.10 Detailed Plan of Action For Information Security Program Development

- A gap analysis should have led to identifying a series of projects that will result in improvements to the information security program
  - Each project should have time, budget and measurable result
  - Each must make the environment more secure without otherwise causing control weaknesses in other areas
- An ISM should prioritize the portfolio of projects in such a way that those that overlap are not delayed by each other, resources are appropriately allocated, and the results are smoothly integrated into or transitioned from existing operations

3.12.10 Detailed Plan of Action For Information Security Program Development (continued)

The ISM should employ generally accepted project management techniques

Once the project is done, the control activity should be an integral part of the unified information security program

3.13 Information Infrastructure and Architecture

- Infrastructure refers to the underlying base or foundation upon which information systems are deployed
- Security infrastructure refers to the foundation that enables security resources to be deployed
- When infrastructure is designed and implemented consistent with policies and standards, the infrastructure is said to be secure
- Information security architecture should be used to achieve information security control objectives

3.13.1 Managing Complexity

- Providing a Framework and Road Map
  - Architecture acts as a road map for projects and services that must be integrated
- Simplicity and Clarity through Layering and Modularization
  - Information Systems architecture must take account of
    - The goals that are to be achieved through the systems
    - The environment in which the systems will be built and used

3.13.2 Objectives of Information Security Architectures

The underlying notion for all architecture is that the objectives of complex systems must be comprehensively defined, precise specifications developed, their structures engineered and tested for form, fit and function, and their performance monitored and measured in terms of the original design objectives and specifications.

3.13.2 Objectives of Information Security Architectures (continued)

SABSA

- Developed to address the need for overall comprehensive model for information systems.
- Can utilize COBIT, ITIL and ISO/IEC 27001

3.13.2 Objectives of Information Security Architectures (continued)

- SABSA
  - Six layers
    - Contextual Security Architecture
    - Conceptual Security Architecture
    - Logical Security Architecture
    - Physical Security Architecture
    - Component Security Architecture
    - Operational Security Architecture

3.13.2 Objectives of Information Security Architectures (continued)

- Given that input is the major source of damage to most systems, all systems should have security mechanisms to validate input
- Preventing harm due to unauthorized access is fundamental to the security program
  - Most system configurations have some type of access control lists
  - Information systems should be monitorable and recoverable
  - They should have logs that produce alerts
- Security mechanisms must result in ”defense in depth”

3.13.2 Objectives of Information Security Architectures (continued)

When gathering information used to make architecture decisions, the ISM must constantly shift focus between:

- Business requirements
- The infrastructure engineer's perspective
- Operations support
- End users
- Financial planner
- Engineer
- Operations support manager

3.13.2 Objectives of Information Security Architectures (continued)

- Must also maintain a sharp focus on
  - Security requirements
  - How security features of platforms can be used to provide layered security
- Security architecture requires
  - Balancing requirements
  - Finding a way to meet requirements with available

3.13.3 Information Security Technologies and Architecture

- Biometrics
- Certificate authorities (CAs)
- Digital signatures
- DMZ
- Entitlements
- Firewalls
- Handheld devices
- Single sign-on
- Intrusion detection
- Intrusion prevention
- Masking
- Policy-compliance systems
- Proxy servers
- Secure Socket Layer (SSL)
- Secure Shell (SSH)
- Secure Multipurpose Internet Mail Extensions (S/MIME)
- Security Information Management (SIM)
- Identity management systems
- Virtual private networks (VPNs)

3.13.3 Information Security Technologies and Architecture (continued)

- Biometrics
- Physical or psychological trait
- Trait is recorded via an enrollment process
- Identification and authentication technology recreates a live template
- Compared to the recorded one
- Process by which templates are recorded for storage is usually different than that used to create a live template

3.13.3 Information Security Technologies and Architecture (continued)

Certificate authority

A certificate authority (CA) is a server used to register entities and issue digital certificates in electronic format

Entities may be any user or technology component that requires a certificate

The authority also issues a root certificate

The mechanism to validate a digital certificate is algorithmic

A certificate authority also maintains a certificate revocation list (CRL)

The list is used to allow a program to query the CA to check if a certificate for checking validity

3.13.3 Information Security Technologies and Architecture (continued)

- Digital signatures
- Based on public/private key encryption
- Electronic equivalent of a handwritten signature
- Validates that a given message came from a specific user
- Nonrepudiation - the sender cannot later claim that the message was created by anyone else without admitting to losing his/her private key

3.13.3 Information Security Technologies and Architecture (continued)

Digital signatures

A hashing algorithm hashes the entire message by generating a message digest

The message digest is encrypted using the sender's private key

The result is sent to the receiver as an addendum to the original message

The receiver uses the sender's public key to decrypt the addendum

Applies the hash algorithm to the original message and compares the two message digests

3.13.3 Information Security Technologies and Architecture (continued)

- DMZ
- Based on the military term “demilitarized zone”
- Buffer zone established between neighboring hostile countries
- Refers to the network in which all packets coming in or out are subject to traffic filters and sometimes route filters
- Usually placed between an organization’s private network and the Internet
- Ensure that all Internet connectivity is subject to control points within the DMZ

3.13.3 Information Security Technologies and Architecture (continued)

Entitlements

- Records used to validate the type of data a user is allowed to access
- Commonly indexed by user ID or role
- A user is assigned a role that will be entitled to data to which the role is authorized to access
- User- and role-based entitlements are similar, as access is stipulated upon an attribute in a user record
- The user is authorized to access information by virtue of being authorized to belong to a group
- Rule-based entitlements fields in a user record and perform calculations or execute business logic before releasing specific entitlement-controlled set of data

3.13.3 Information Security Technologies and Architecture (continued)

Firewalls

Definition: devices that filters any type of traffic by inspecting session or application-level activity and comparing it to a given rule set

Usually placed in the network at the point where traffic would be routed to an external site or a DMZ

Similar to how a choke router is placed in the network

Provisioned with rule sets that limit the type of traffic that does and does not get through

3.13.3 Information Security Technologies and Architecture (continued)

- Handheld tokens
- Physical devices used to authenticate users
- Token identifiers such as serial numbers are registered on a server
- User uses the token to generate a one-time password
- Passed to the server for validation
- Cryptographic algorithms and keys on both token and server allow the server to validate the token

3.13.3 Information Security Technologies and Architecture (continued)

Identity Management Systems (IMS)

- Database of user information for identifying enterprise users
- Records in IMS are used to map system logins belonging to a given user to the unique record
- The mapping may be done by copying user lists from downstream systems into the IMS or by storing system login names in the user identity record
- IMS are supplemented with analytics and audit trails for providing a history of a user's relationship with the organization

3.13.3 Information Security Technologies and Architecture (continued)

- Intrusion detection and intrusion prevention
- Process of identifying and responding to malicious activity
- Intrusions are identified via rule-based pattern matching or anomaly detection
- Records a definition of “normal” system behavior and alerts when behavior is abnormal
- Intrusion prevention is a network-based intrusion detection system configured to automatically block network traffic from a source at which it identifies an intrusion

3.13.3 Information Security Technologies and Architecture (continued)

- Masking
  - Changing data so that its original content is rendered unrecognizable
  - Often done to generate test data that looks like production data
  - Confidential data can be masked so that it can be used for testing purposes
- Policy-compliance systems
  - Enforce standards configuration
  - Provide preventive and detective controls to allow a system security configuration to be centrally administered and monitored

3.13.3 Information Security Technologies and Architecture (continued)

Proxy server

Server placed in a network to provide a gateway for a set of destination hosts or networks

Software intercepts individual network sessions from many sources and presents them to the destination on behalf of the original source

The server may also be configured to block it entirely according to a given rule

Users required to authenticate for traffic to be passed to the designated destination

3.13.3 Information Security Technologies and Architecture (continued)

- Secure Socket Layer (SSL)
- Session- or connection-layer protocol used on the Internet for communication with web services
- Uses a hybrid of hashed, private and public key cryptography
- Compute a one-time session key
- Encrypt all subsequent communications with the session
- In conjunction with a CA, it is used by the client to authenticate the server and by the server to authenticate the client

3.13.3 Information Security Technologies and Architecture (continued)

- Secure Shell (SSH)
- Client-server program used to create a secure, encrypted session between two hosts
- Clients store public keys provided by hosts to authenticate the server and encrypt messages
- Host public keys can be provided that the server can use to authenticate the client
- SSH provides terminal session and a secure copy and may be used to tunnel other applications between client and server
- Commonly used to replace the less-secure telnet and ftp and to secure X-Windows

3.13.3 Information Security Technologies and Architecture (continued)

- Secure Multipurpose Internet Mail Extensions (S/MIME)
  - Standard secure e-mail protocol that authenticates the identity of the sender and receiver
  - Verifies message integrity and ensures the privacy of a message's contents, including attachments
- Security Information Management (SIM)
  - Correlates security-related activity across multiple platforms
  - Configured to recognize and alert on patterns in real time or to store for later reporting

3.13.3 Information Security Technologies and Architecture (continued)

- Single Sign-on (SSO)
- System used to authenticate users on diverse platforms
- Each platform must be configured with an “agent”
- Either replaces the platform sign-on mechanisms or
- Forwards user authentication data
- The agent uses the data to authenticate the user to a SSO server

3.13.3 Information Security Technologies and Architecture (continued)

- Virtual Private Network (VPN)
- Secure private network
- Uses the public telecommunications infrastructure
- Transmits data
- Using encryption and authentication
- Encrypts all data that pass between two Internet points
- Maintains privacy and security

3.14 Physical and Environmental Controls

- Are a specialized set of general controls upon which all computing facilities as well as personnel depend.
- The ISM should:
  - Validate technology choices in support of physical security
  - Ensure that formal roles and responsibilities and accountabilities with respect to physical access controls exist
  - Use the roles and responsibilities for interfacing with various local physical security organizations if they are geographically dispersed

3.14 Physical and Environmental Controls (continued)

- Physical controls
- Intended to restrict access to facilities
- Methods for keeping unauthorized individuals from gaining access to tangible information resources include
  - Smart cards or access controls based on biometrics
  - Security cameras
  - Security guards
  - Fences
  - Lighting
  - Locks
  - Sensors

3.14 Physical and Environmental Controls (continued)

- Environmental controls
- Designed to ensure that the facilities in which systems are stored are designed to compensate for physical limitations of computer system operations
- Without environment controls to prevent, detect and recover from physical damage to information systems, control activities would be subject to physical damage from a variety of sources (e.g., theft and weather)

3.15 Information Security Program Integration

- Because organizational departments also have a responsibility for information security process deployment, the ISM is not able to enforce all policy requirements.
  - Personnel outside can be assigned security job responsibilities, thus allowing the ISM to close gaps out of his/her control
  - The ISM may also need to assist business application owners in establishing procedures
  - An ISM must integrate security touchpoints into the life cycle to ensure that the business is not surprised by last-minute introduction of security requirements

3.16 Information Security Program Development Metrics

- Information security program metrics corresponding to control objectives provide senior management with information needed to ascertain whether the information security program is on track
- Control objective metrics should correspond to information security governance goals (covered in chapter 1)

3.16 Information Security Program Development Metrics (continued)

- Strategic alignment examples:
  - Extent to which business areas are represented in the information security program
  - Percentage of those that include data stewardship or information protection in their charter
- Risk management examples:
  - Level at which risks are formally addressed in various business areas
  - Identifiable risk management function in steering committee
  - Periodic testing of the communication lines to escalate risks

3.16 Information Security Program Development Metrics (continued)

Value delivery examples:

Budgeted cost of work scheduled verses budgeted cost compared to the actual cost of the project for that period

Demonstrated effectiveness—low cost and schedule variances

Positive returns on investment through reusable security tools and techniques within the infrastructure and security review processes

3.16 Information Security Program Development Metrics (continued)

- Resource management examples:
  - Resource deficiencies are detected and corrected before impact
  - Identify changing security resource requirements
  - All personnel in lead roles in critical security functions have a backup
- Performance management examples:
  - Verification that control activities are achieving desired results
  - Performance measurement with respect to security activity designed to achieve technical objectives
- Security baselines:
  - To what extent do existing processes conform to security baselines?