KRKA

Živeti zdravo življenje.

AKTUALNA VPRAŠANJA INFORMACIJSKE VARNOSTI

Dušan Dular

Se počutimo preveč varne?

Podjetja in napadalci

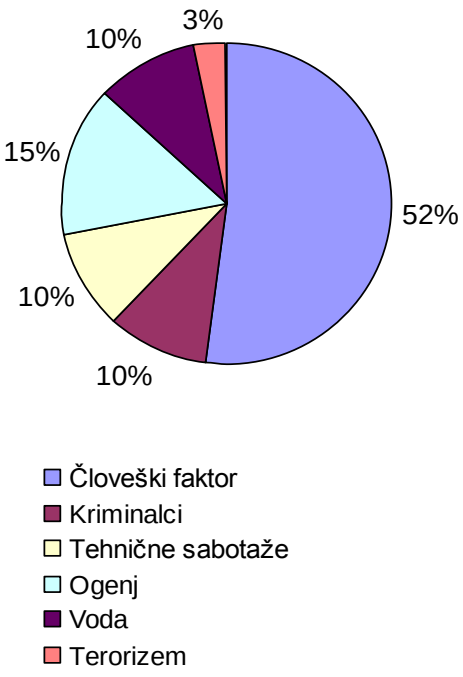
- Črvi, trojanci, virusi
- Hackerji
- Konkurenca
- Teroristi
- Zaposleni

Zakaj je varnost pomembna?

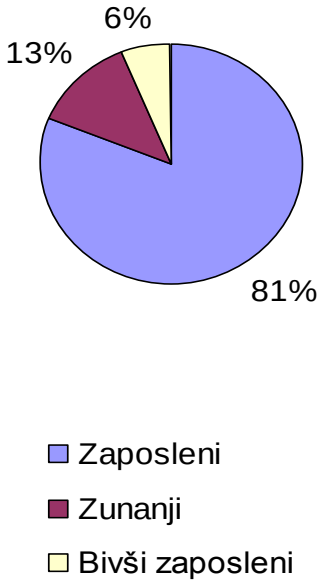
- Izguba informacij
- Zloraba informacij
- Izguba zaupnosti
- Izguba verodostojnosti
- Finančna izguba
- Pravna odgovornost

Informacijska varnostna tveganja

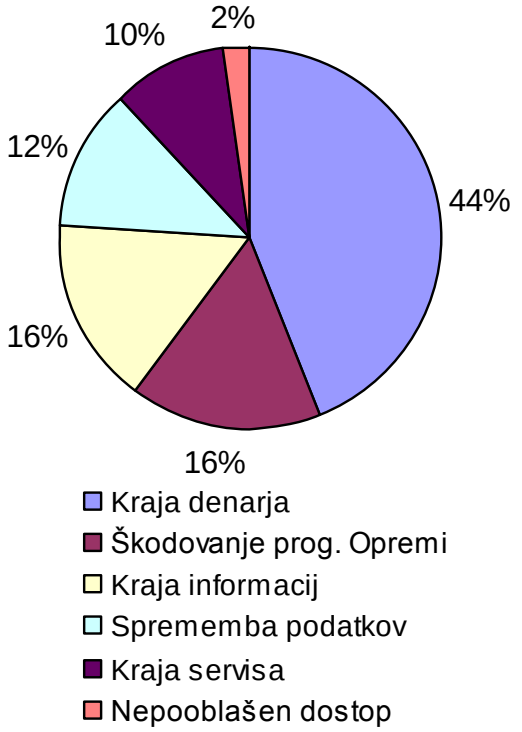
Osnovni razlogi za škodo



Povzročitelji



Vrsta računalniškega kriminala



Informacijska varnost v svetu in pri nas

Nastop informacijske nesreče lahko pomeni za podjetje prenehanje poslovanja. Izguba vseh podatkov pomeni, da ima podjetje le 6-odstotkov možnosti, da preživi informacijsko nesrečo.

Nastop kakršnekoli informacijske nesreče za podjetje brez vzpostavljenega sistema varovanja informacij pa pomeni, da ima le 50-odstotkov možnosti, da preživi.

Le dve tretjini podjetij po svetu se zaveda tveganj, povezanih s sodobno tehnologijo. Od tega jih samo ena tretjina intenzivno dela na učinkovitem izvajanju aktivnosti varovanja informacij.

Razloge za to gre iskati predvsem v:

napačnem razumevanju področja informacijske varnosti s strani vodstva in popolnega ignoriranja posledic, ki bi lahko nastale ob nastopu informacijske nesreče.

EU regulation

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (e-Privacy Directive)
- Basel II Capital Accord
- Human Rights Act 1998
- Electronic Signature Directive
- EDI Directive
- e-Commerce Directive
- MoReq - Model Requirements for the Management of Electronic Records

Industry standards

- EU Directive 91/356 Annex 11 (PIC/S guidance)
- EU Directive 1999/93/EC – Electronic Signatures
- US FDA 21 CFR Part 11

Slovenska zakonodaja in standardi

- Zakon o varstvu osebnih podatkov
- Zakon o elektronskem poslovanju
- Zakon o delovnih razmerjih
- Zakon o gospodarskih družbah
- Zakon o varovanju dokumentarnega in arhivskega gradiva ter arhivih
- Zakon o davčnem postopku
- Slovenski računovodski standardi
- Mednarodni standardi računovodskega poročanja
- Kodeks upravljanja javnih delniških družb Ljubljanske borze

Področja zakonodaje:

Varnost informacij
Zaščita osebnih podatkov
Transparentnost poslovanja

http://www.ipri-zavod.si/

KRKA

O varstvu osebnih podatkov in zasebnosti

Del širšega spektra zasebnosti

Konvencijsko varstvo - Splošna deklaracija o človekovih pravicah, Evropska konvencija o človekovih pravicah

Ustavno varstvo

Zakonsko varstvo Direktiva 95/46/ES - Direktiva o varstvu osebnih podatkov, Direktiva 2002/58/ES - Direktiva o zasebnosti in elektronskih komunikacijah, Zakon o varstvu osebnih podatkov (ZVOP-1)

Neodvisni nadzorni organi - Informacijski pooblaščenec, Article 29 Working Party,European Data Protection Supervisor

Kaj je poslovna skrivnost?

Definicijo poslovne skrivnosti podaja Zakon o gospodarskih družbah.

Za poslovno skrivnost se štejejo podatki, za katere tako določi družba s pisnim sklepom. S tem sklepom morajo biti seznanjeni vsi, ki so dolžni varovati poslovno skrivnost.

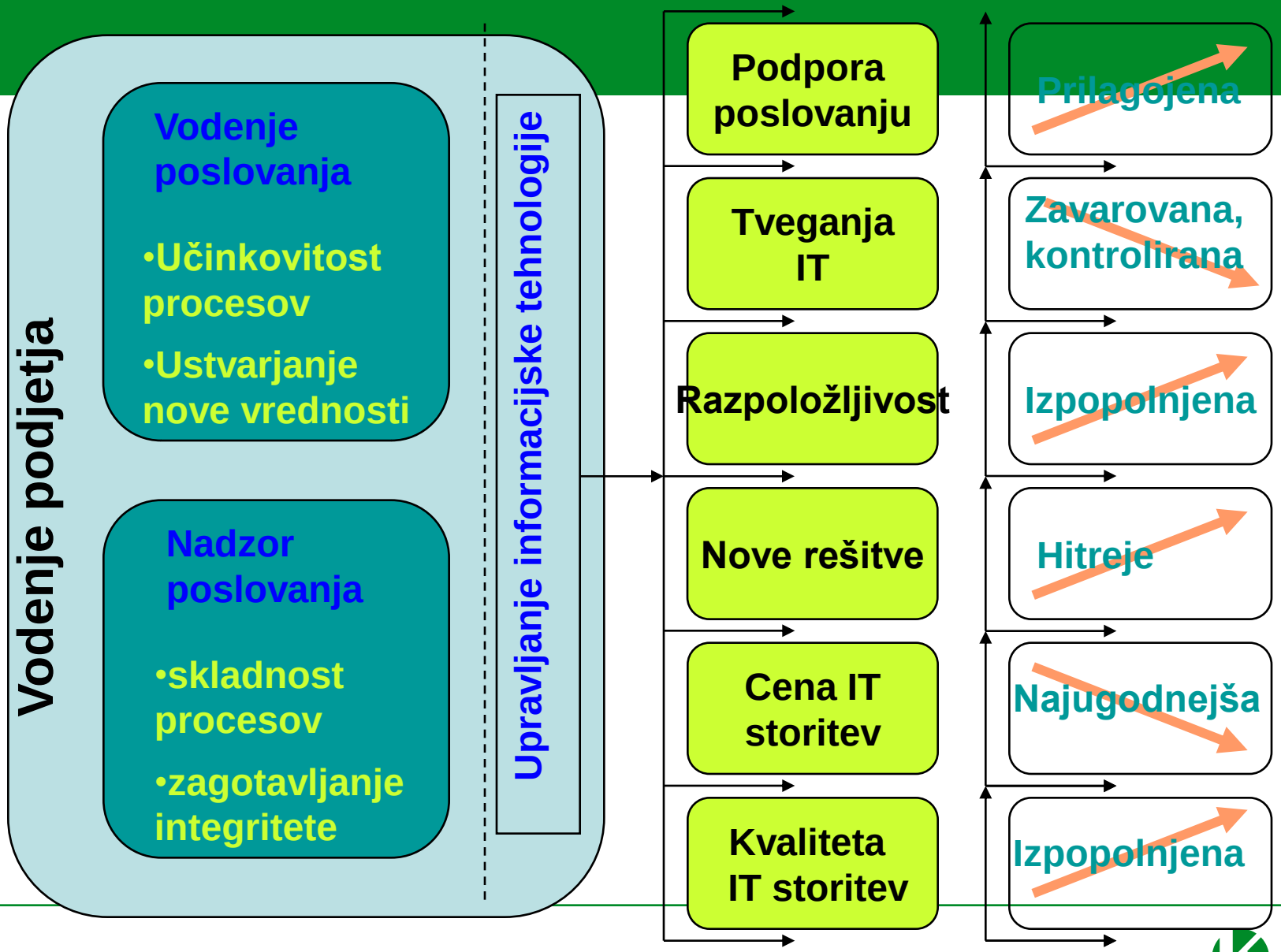
Med poslovno skrivnost družbe se lahko štejejo tudi drugi podatki, če je očitno, da bi njihovo razkritje nepooblaščenim osebam lahko družbi povzročilo občutno škodo.

Upravljanje informacijskih storitev

- Sarbanes–Oxley, EU direktive, lokalna zakonodaja, … zahtevajo kontrole, ki narekujejo **upravljanje informacij**
- **Naraščajoče informacijske nevarnosti** v smislu kraje, industrijske špijunaže, potvarjanja… so povečale fokus na **upravljanje informacijske varnosti**
- Mednarodne institucije kot so npr.: ITGI (IT Governance Institute), ISO, razvijajo **ogrodja za uspešno upravljanje informacij.**
- Inšpektorji, revizorji ,… vse bolj **poudarjajo in zahtevajo od vodstev podjetij, da se prilagodijo**

  z uvajanjem ISO standardov ali drugih ogrodij

Obseg upravljanja IT storitev

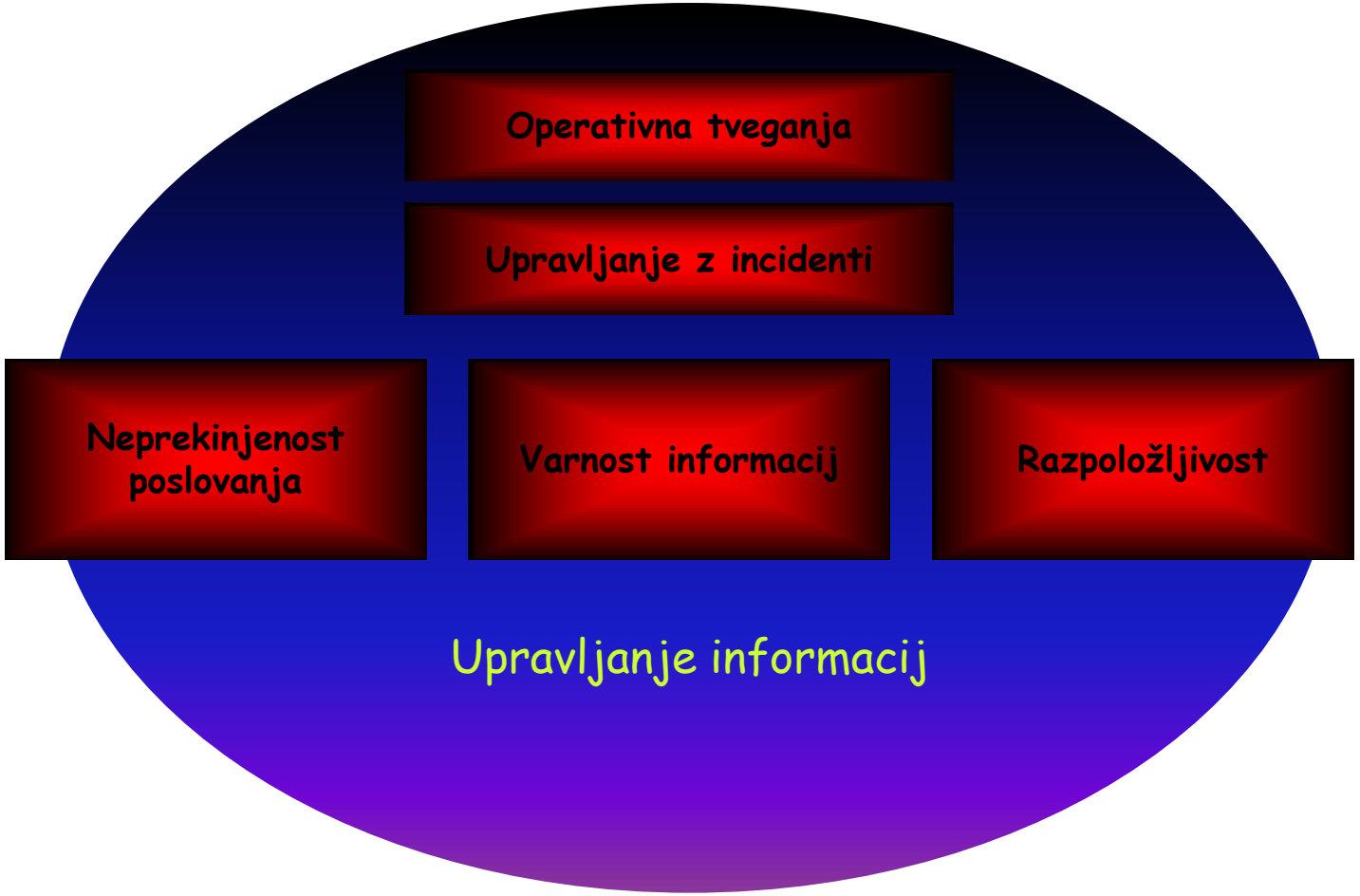


Vloge v upravljanju IT

Vodstvo	Kako definirati poslovne usmeritve za IT in uporabiti pravilne načine vodenja, da zagotovimo najvišjo poslovno vrednost IT storitev in obvladujemo tveganja?
Vodje procesov	Kako zagotoviti, da vlaganja v IT zagotavljajo ustrezno podporo procesom, ki je zanesljiva in varna?
Vodstvo ITT	Kako zagotavljati IT storitve v skladu s potrebami poslovanja in usmeritvami vodstva?
Upravl. kakovosti Not. revizija	Kako zagotoviti, da smo skladni s politikami, predpisi in zakoni in da so prepoznana in zmanjševana nova tveganja?
Presojevalci	Kako dati neodvisno zagotovilo o vrednosti IT storitev in obvladovanju tveganj?

KRKA

Širina in obseg…



Načela varovanja informacij

- **Zaupnost**
  - Zaščita občutljivih informacij pred nepooblaščenim razkritjem oz. dostopom
- **Neoporečnost**
  - Varovanje točnosti in popolnosti informacij in računalniških programov
- **Razpoložljivost**
  - Informacije in računalniške storitve morajo biti na voljo uporabnikom, kadar je potrebno

INTERNE KONTROLE

Predpisi ne določajo katero metodologijo ali tehnologijo uporabiti oz. kako zagotoviti skladnost. Za doseganje skladnosti organizacije povzemajo notranje kontrole na osnovi okvirov (frameworks), ki slonijo na “najboljši praksi” za doseganje skladnosti.

Najbolj popularni okvirji so:

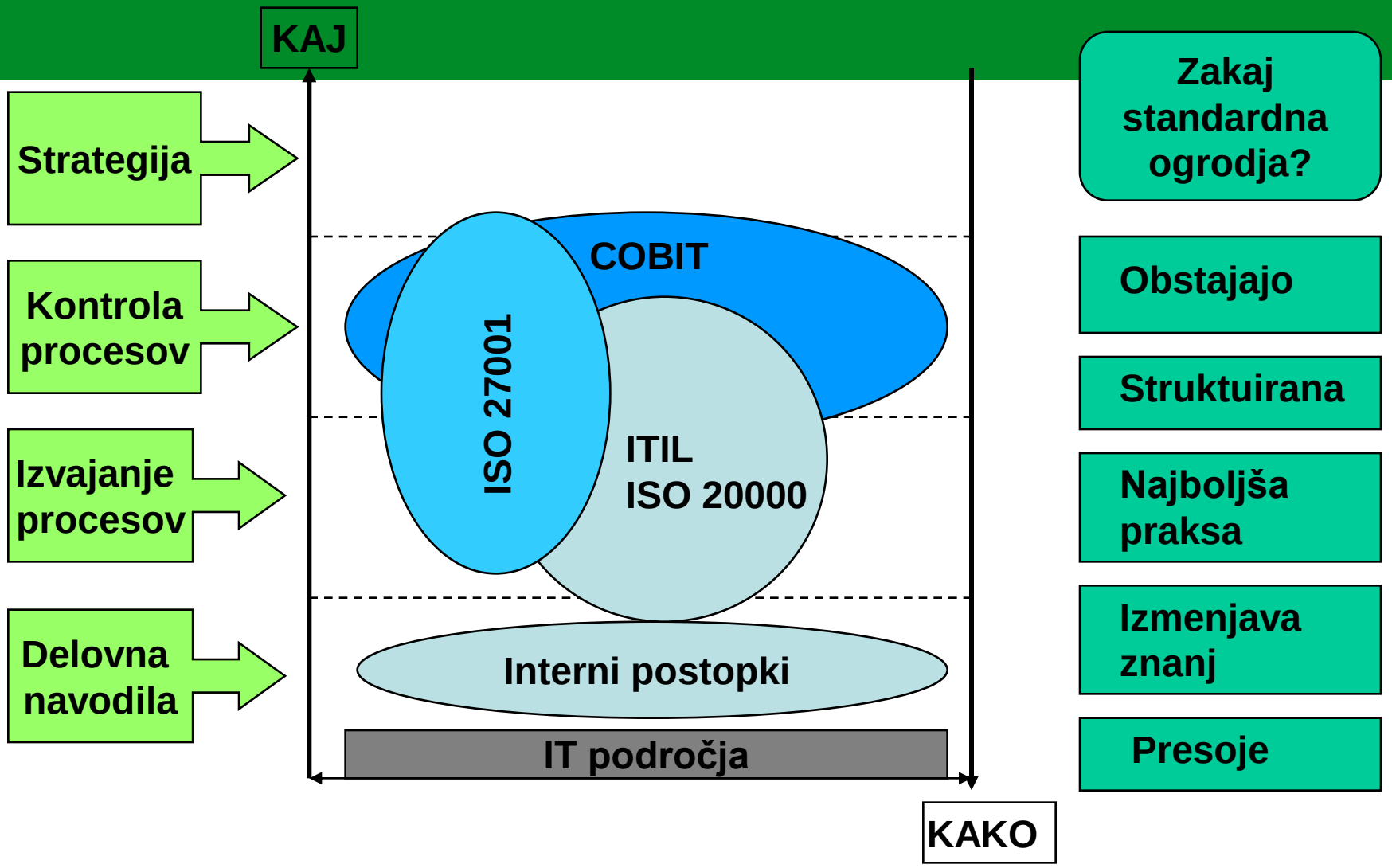
COSO – določa zahteve za učinkovito vodenje podjetja

CobiT – določa zahteve za učinkovito upravljanje informacij

ISO 2700x – določajo najboljše prakse s področja informacijske varnosti

ISO 20000 (ITIL) – določa najboljše prakse za učinkovite informacijske storitve

IT OGRODJA



ITGI document: **Aligning COBIT,ITIL, and ISO17799 for Business Benifit**

KRKA

Pristop k vodenju varnosti informacij

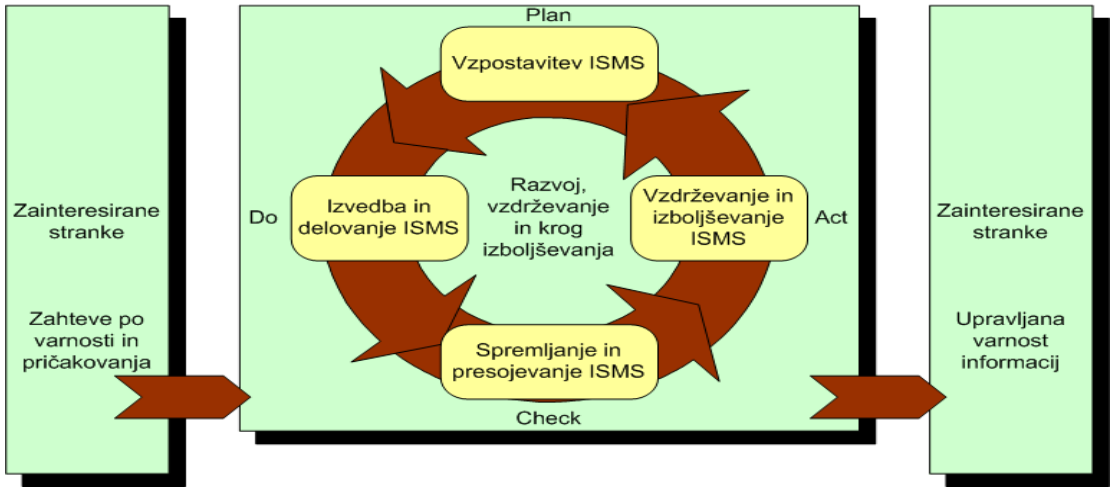
Poslovni cilji, poslanstvo, vizija, strateške usmeritve, ...

Potrebe po varovanju informacij

SVVI- Sistem vodenja varnosti informacij
ISMS – Information Security Management System
varnostna politika, ki “živi” v organizaciji

Integracija v sistem vodenja kakovosti

ISO 27001 – postavlja specifikacijo zahtev za SVVI
(vzpostavljanje, odgovornosti, delovanje, izobraževanje, izboljševanje…



ISO 27002 – podaja priporočila najboljše prakse
(jedro standarda so smernice za imlementacijo nadzorstev)

9001

14001

OHSAS18001

HACCP

GMP

27001

Po standardu ISO 27001 mora organizacija:

- Določiti obseg in meje sistema vodenja informacijske varnosti
- Definirati politike informacijske varnosti
- Definirati pristop k oceni tveganja
- Izvajati analizo in oceno tveganj
- Prepoznati in izvajati ukrepe za zmanjšanje tveganja
- Pripraviti izjavo o uprabljenosti kontrol iz ISO 27002 standarda
- Uvesti izbrane kontrole za dosego kontrolnih ciljev
- Določiti kako meriti in nadzirati efektivnost izbranih kontrol
- Izvajati izobraževanja in programov zavedanja
- Upravljati izvajanje sistema inf. varnosti

ZVDAGA

Zakon jasno opredeljuje, da mora podjetje imeti urejeno informacijsko varnost, če želi imeti pravno veljavno elektronsko arhiviranje (akreditacija NP ni nujna)

Podjetja, ki opravljajo storitev elektronskega arhiviranja morajo imeti s strani Arhiva Slovenije potrjena Notranja pravila, v katerih se 70% zahtev nanaša na informacijsko varnost.

Arhiv Slovenije je jasno povedal, da v primeru certifikacije po standardu ISO 27001, zahteve NP ne bodo predmet globljega preverjanja.

Analiza tveganj

- Ocenjevanje tveganj:
  - kaj moramo varovati (viri)?
  - zaradi česa (ranljivosti)?
  - pred čim (grožnje)?
  - vrednotenje virov, ranljivosti, groženj

OCENJEVANJE KRITIČNOSTI

Kritičnost poslovnih procesov/sistemov določajo:

Zaupnost

Celovitost

Razpoložljivost

GMP kritičnost

Zaupnost

Vsaka informacija/dokument/podatek ima določeno stopnjo zaupnosti
Npr:
5 – strogo zaupno
4 – zaupno
3 – interno zaupno
2 – interno
1 – javno

V skladu s stopnjo zaupnosti izvajamo ukrepe za zaščito zaupnosti.

Celovitost

Nivo	Tipično vprašanje: Kako natančno/zanesljivo moramo zagotoviti/izdelati/izmeriti izdelek/podatek, da zaradi tega ne trpi poslovanje procesa/Krke? Si lahko privoščimo napačno informacijo? Kašna je cena odprave posledic?
5	Napačni podatek/informacija povzroči takojšnje nastajanje škode, ki lahko v kratkem časovnem obdobju preraste v škodo velikih razsežnosti (npr. izpad vseh ključnih funkcij podjetja, slabo kvaliteto ali uničenje proizvodov, veliko nevarnost za ljudi,…). V trenutku uporabe podatka/informacije je preverjanje pravilnosti/ zanesljivosti nemogoče.
4	Napačni podatek/informacija povzroči problem večjih razsežnosti, ki ima za posledico veliko materialno škodo, zastoje v delovanju ključnih procesov podjetja (proizvodnje, skladiščenja, …), izgubo ugleda podjetja. Možnost pravočasnega odkritja in poprave napake je majhna s tem, da posledice skozi čas naraščajo.
3	Napačni podatek/informacija povzroči lahko povzroči veliko škodo podjetju, vendar je napake možno z ukrepi/kontrolami učinkovito odkrivati in odpravljati preden povzročijo škodo.
2	Natančnost/zanesljivost podatkov/informacij je sicer želena, vendar se da skozi daljše časovno obdobje posledice napačnih podatkov/ informacij kontrolirati in brez večjih posledic odpravljati (npr. dolgoročno planiranje)
1	Informacije/podatki so zgolj informativnega značaja in se na njihovi osnovi ne sprejema poslovnih odločitev

KRKA

Zagotavljanje celovitosti podatkov v aplikaciji

Stopnja celovitosti se določi že v zgodnjih fazah razvoja. V skladu z deklarirano stopnjo celovitosti posamezni procesi sprejemajo organizacijske ukrepe, ki pripomorejo k zagotavljanju celovitosti, za IT sisteme/aplikacije pa se sprejmejo ukrepi, ki ta nivo celovitosti zagotavljajo.

Možni ukrepi:

- **Kontrola vnosov (potrjevanje pravilnosti)**
- **Dvojni vnosi podatkov,**
- **»Check sum« kontrole pri prenosu podatkov**
- **Zagotovitev zahtevane natančnosti avtomatskega odčitavanja podatkov**
- **Nabori pričakovanih vrednosti,**
- **Kontrole na obseg/rang pričakovanih vrednosti**
- **Križne kontrole »enakih podatkov« v različnih sistemih**
- **Kontrole na šifrante**
- **Logiranje transakcij**
- **Obvladovanje dostopov**
- **Obvladovanje pravic nad podatki (vloge)**
- **Dodeljevanje pravic za branje, pisanje/spreminjanje, brisanje…**
- **Uporaba tehnik, ki zagotavljajo nespremenljivost podatkov (npr.: e - podpis)**
- **Backup podatkov**

Vsaka stopnja celovitosti ima svojo ceno !!!

KRKA

Razpoložljivost

Nivo	Čas vzpostavitve	Koliko časa smo lahko brez določenega procesa/sistema in zaradi tega ne trpi poslovanje/delovanje procesa/Krke?
5	Najnižji možni čas	Izpad procesa/sistema povzroči takojšnje nastajanje škode, ki lahko v kratkem časovnem obdobju nekaj minut preraste v škodo velikih razsežnosti (npr. izpad vseh ključnih funkcij podjetja, slabo kvaliteto ali uničenje proizvodov, veliko nevarnost za ljudi,…)
4	do 1 ure	Izpad procesa/sistema lahko v časovnem obdobju do 30 minut preraste v problem večjih razsežnosti, ki ima za posledico veliko materialno škodo, zastoje v delovanju ključnih procesov podjetja (proizvodnje, skladiščenja, …).
3	do 4 ure	Izpad procesa/sistema lahko v časovnem obdobju do 4 ure obvladujemo z začasnimi ukrepi, ki omogočajo, da brez večjih posledic vzpostavimo normalno delovanje funkcij podjetja, ko se sistem vzpostavi. Daljši izpad ima lahko preraste v problem večjih razsežnosti
2	1 dan	Proces/sistem je podporne narave in ga lahko brez večjih posledic pogrešimo 1 dan. Izpad se da z minimalnimi posledicami nadomestiti ob vzpostavitvi procesa/sistema.
1	1 teden	Z minimalnimi posledicami lahko proces/sistem občasno pogrešimo, mora pa sistem biti operativen v daljšem obdobju, da lahko služi svojemu namenu.

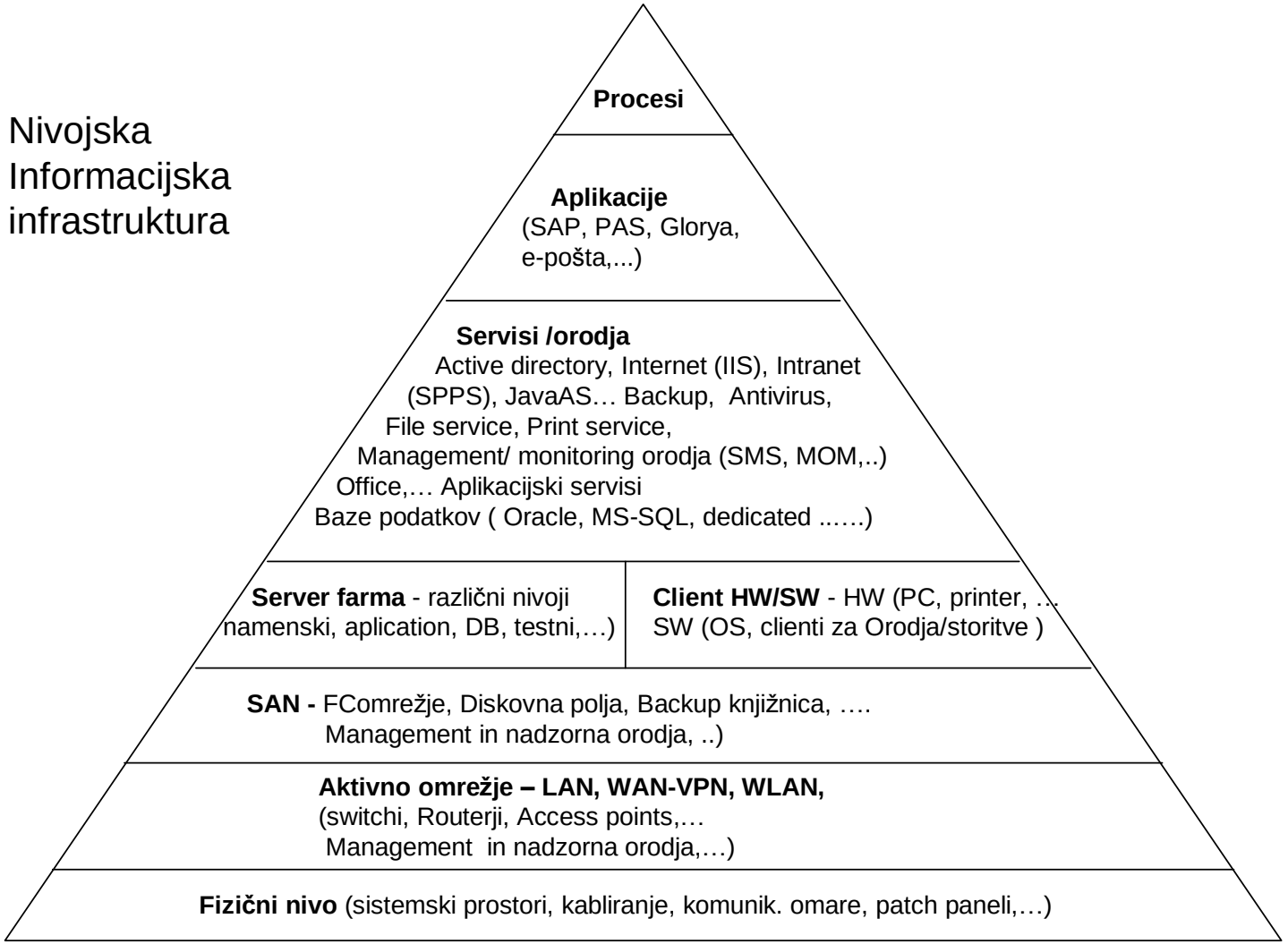
KRKA

Tabela zaupnih dokumentov/podatkov

	lastnik	Dostop DL, pravice	Zaupnost SZ,Z,IZ,I,J	pojavnost (P,ED,BP,..)
Rangiranje izdelkov (letno)				
Plan kadrov (letno)				
Plan stroškov promocije (letno) in poročila				
Planiranje in poročanje dela sodelavcev na terenu (v aplikaciji Sales vision)				
Baza poslovnih partnerjev (v aplikaciji Sales vision)				

Analiza tveganj informacijskih virov

Nivojska Informacijska infrastruktura



Slika št. 1

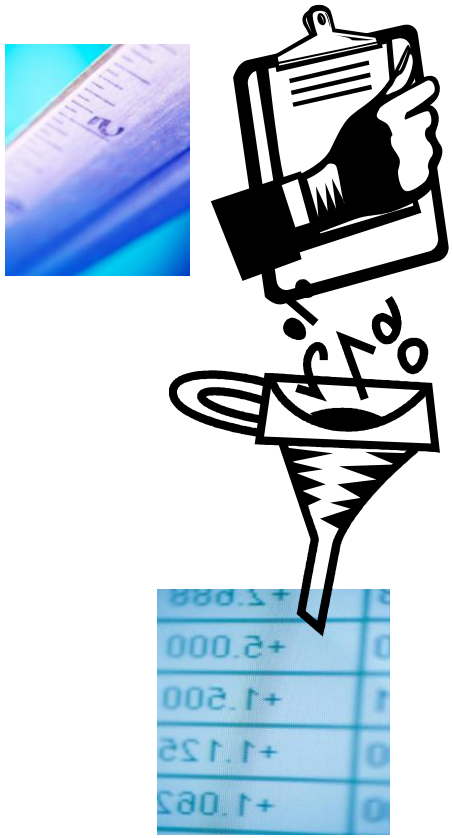
ISO 27002 priporočena nadzorstva

Priporočenih je 133 nadzorstev (Controls), ki so združena v

36 ciljev (Main Security Kategories) ta pa v

11 poglavij (Clauses)

1. Definiranje varnostne politike
2. Organiziranje informacijske varnosti
3. Upravljanje sredstev
4. Varnost v zvezi s človeškimi viri
5. Fizična varnost in okolna varnost
6. Upravljanje komunikacij in operacij
7. Nadzorovanje dostopa
8. Pridobivanje, razvoj in vzdrževanje sistema
9. Upravljanje informacijsko varnostnih incidentov
10. Upravljanje neprekinjenega poslovanja
11. Usklajenost z zakonodajo in predpisi



Z uvedbo posameznih nadzorstev zagotovimo višji nivo informacijske varnosti

KRKA

IZJAVA O PRIMERNOSTI UPORABE KONTROL (primer - izsek)

ISO 17799:2005					
Organization of Information security	6,1	Internal Organization			
	6.1.1	Management Commitment to information security	PK - umeščena politika varovanja informacij SOP QM xxxxx SVVI – krovna varnostna politika.	YES	
	6.1.2	Information security Co-ordiantion	Pravila organiziranosti družbe SOP QM xxxxx SVVI – krovna varnostna politika.	YES	
	6.1.3	Allocation of information security Responsibilities	Pravila organiziranosti družbe SOP QM xxxxx SVVI – krovna varnostna politika.	YES	
	6.1.4	Authorization process for Information Processing facilities	Pravila organiziranosti družbe, Poslovnik komisije za investicije	YES	
	6.1.5	Confidentiality agreements	Pravilnik o določanju in varovanju poslovnih skrivnosti Pravilnik o primerni rabi IT	YES	
	6.1.6	Contact with authorities	SOP SM - komuniciranje v kriznih dogodkih + Požarni red + Hišni red	YES	
	6.1.7	Contact with special interest groups	Načela upravljanja informacijskega sistema	YES	
	6.1.8	Independent review of information security	PK + SOP QM izvajanje presoj + Pravilnik o izvajanju notranjih revizij + pogodba z SIQ + zunanji varnostni pregledi	YES	

KRKA

STALNE IZBOLJŠAVE

SKUPNI CILJ

INTEGRIRAN SISTEM VODENJA

ODGOVORNO RAVNANJE

Celovito obvladovanje kakovosti

VARNOST | ZDRAVJE | OKOLJE

KAKOVOST

OHSAS 18001 | ISO 14001 | GMP | ISO 9001 | HACCP

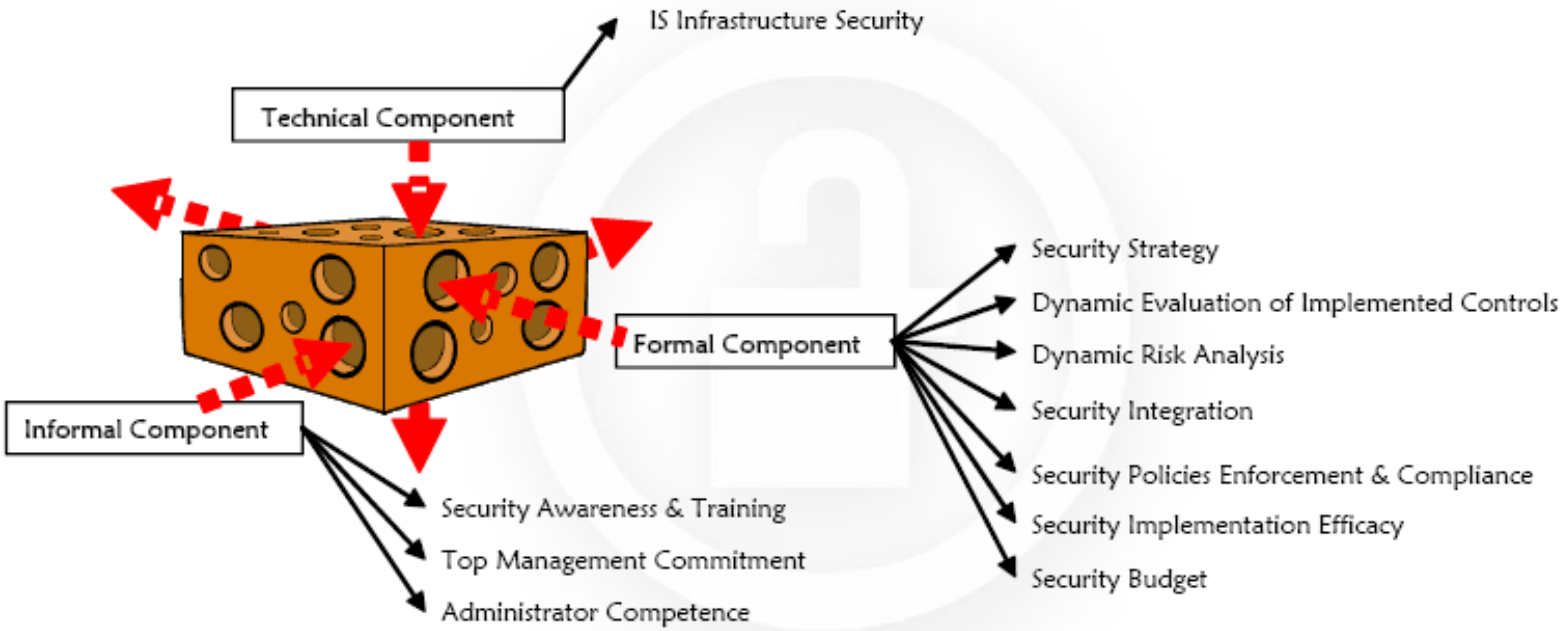
SISTEM VODENJA VAROVANJA INFORMACIJ
ISO 27001

Računalniška varnost je izziv

- Z varnostjo je enako kot pri zavorah v vašem avtomobilu.
  - Njihova **funkcija** je, da vas zaustavijo.
  - Ampak njihov **namen** je, da vam omogočijo da greste hitro.

Bill Malick, Gartner

Critical Success Factors



VPRAŠANJA ????

VPRAŠANJA ????