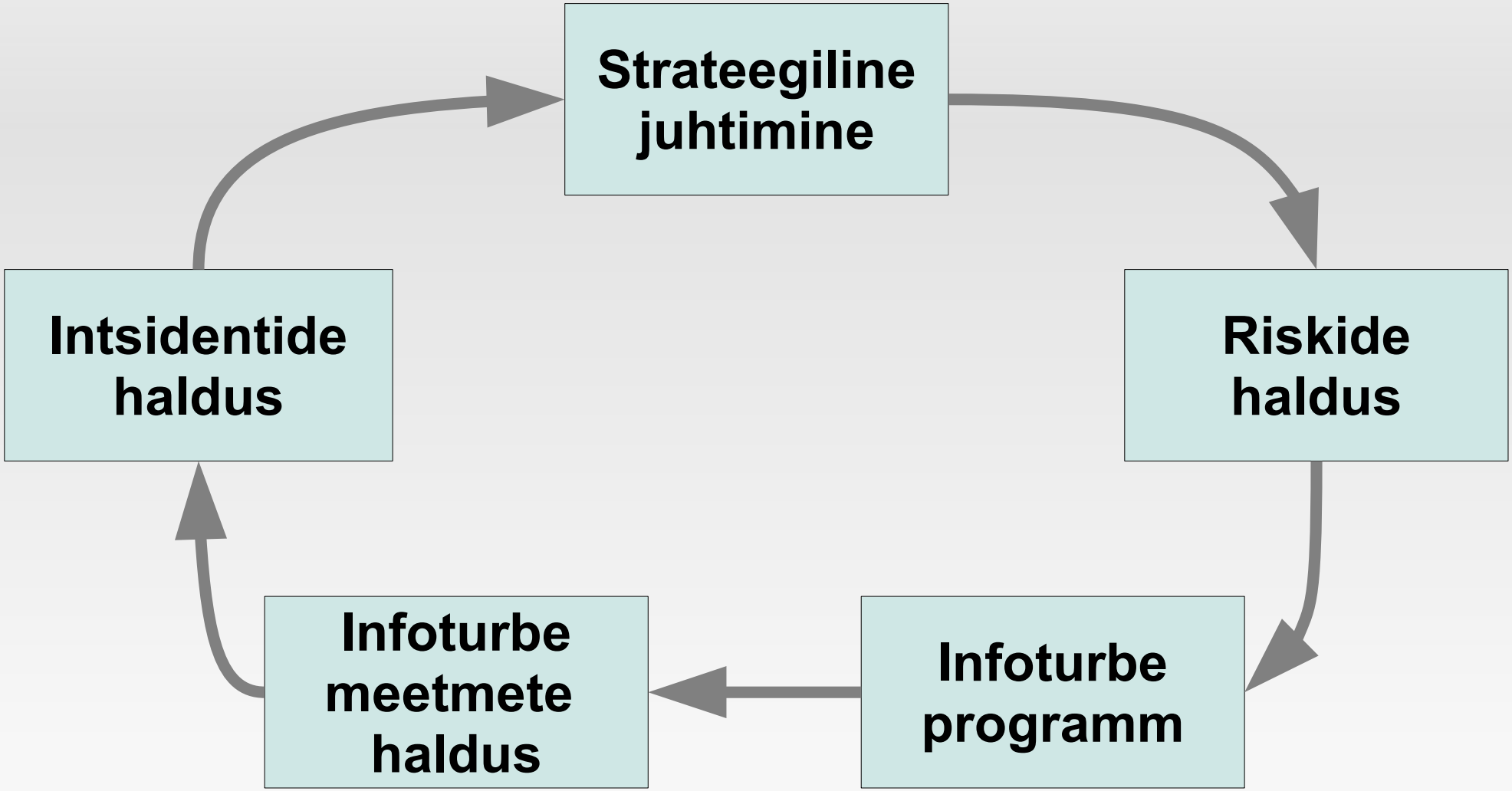
Infoturbe haldus

Hillar Põldmaa

Infoturbe halduse protsess

Klassikaline infoturbe juhtimine



Klassikaline infoturbe juhtimine

Strateegiline juhtimine

- Kehtestada ja juurutada raamistik, mis kindlustaks, et:
  - Infoturbestrateegiad oleksid kooskõlas ärivajadustega
  - Vastaksid kehtivale seadusandlusele
  - Vastaksid standarditele

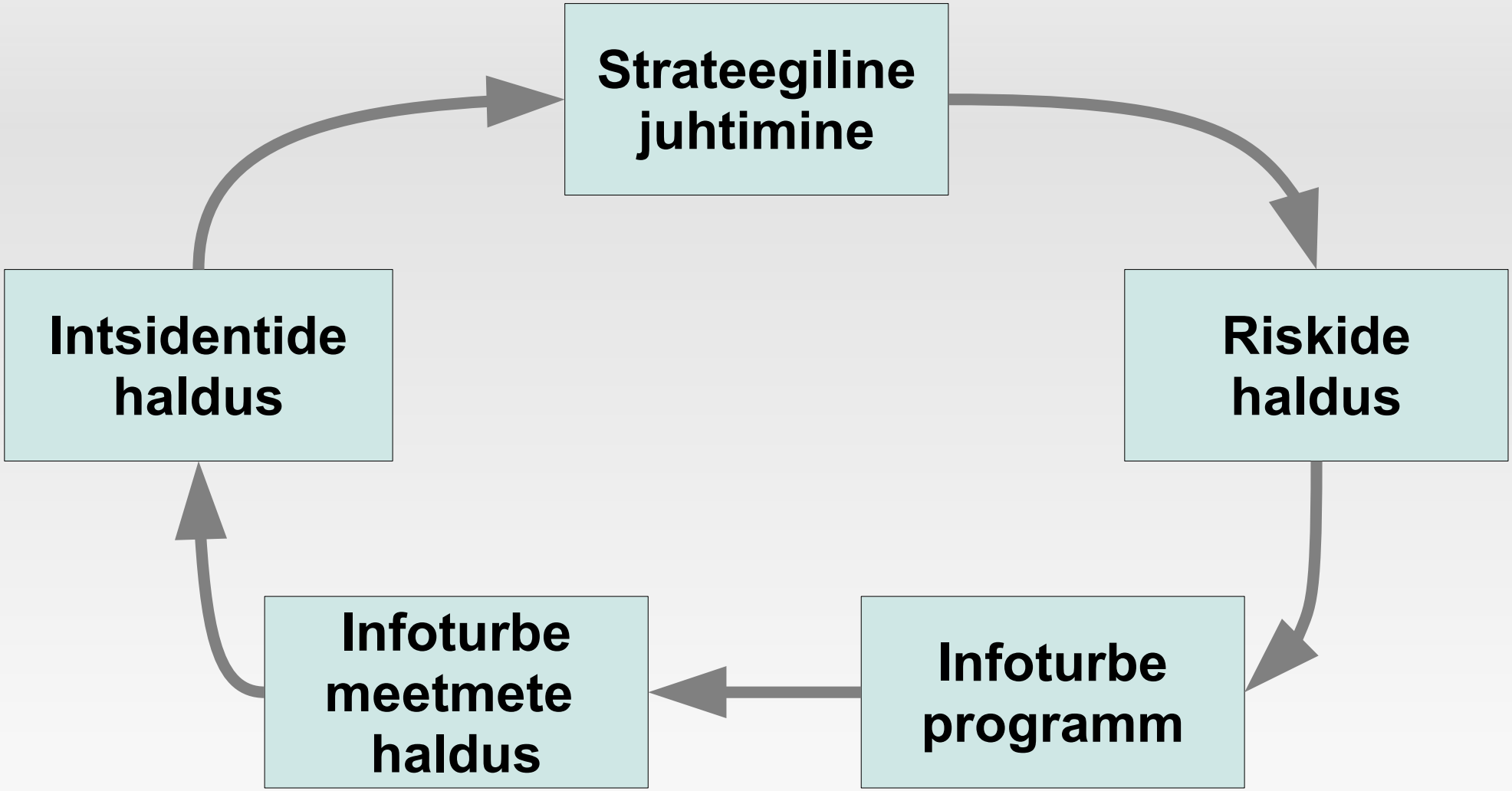
Lisalugemist

- Governance versus management
- http://www.differencebetween.net/business/difference-between-management-and-governance/

Kasulik teada

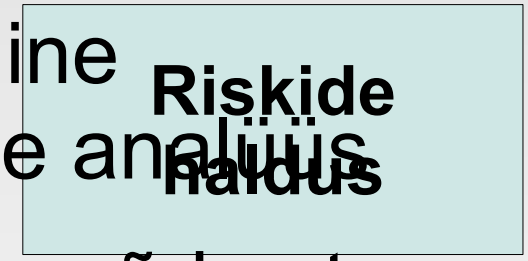
- C-level (C-suite)
- Kõrgem juhtkond
- Ametinimetuses sisaldub „chief“ (C)
- CEO, CFO, CTO, CIO

Klassikaline infoturbe juhtimine

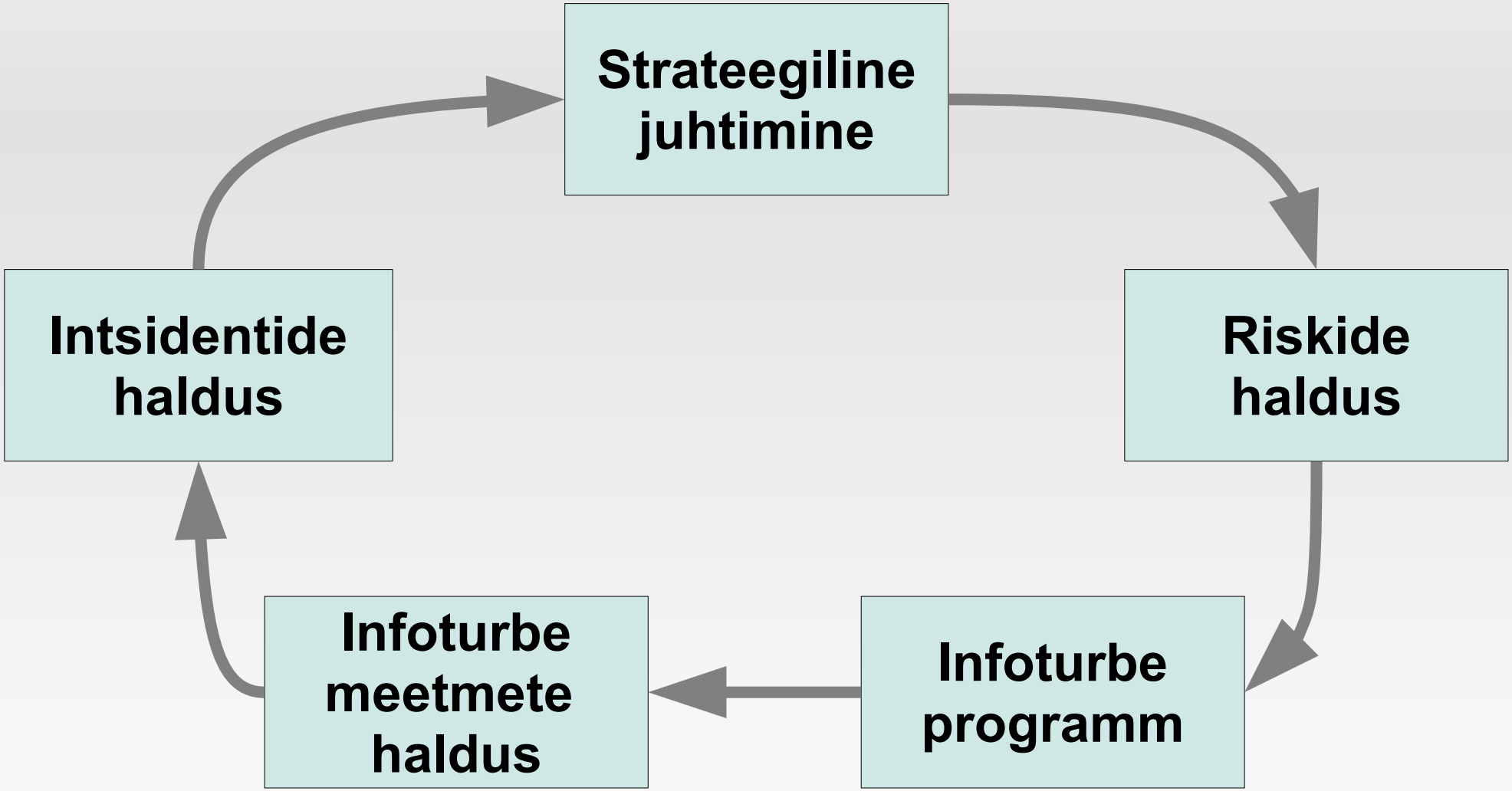


Klassikaline infoturbe juhtimine

- Süstemaatiline infoturbe riskide hindamise protsess
- Perioodiline ärimõjude analüüs
- Ohtude ja nõrkuste hindamine
- Turvameetmete valik



Klassikaline infoturbe juhtimine

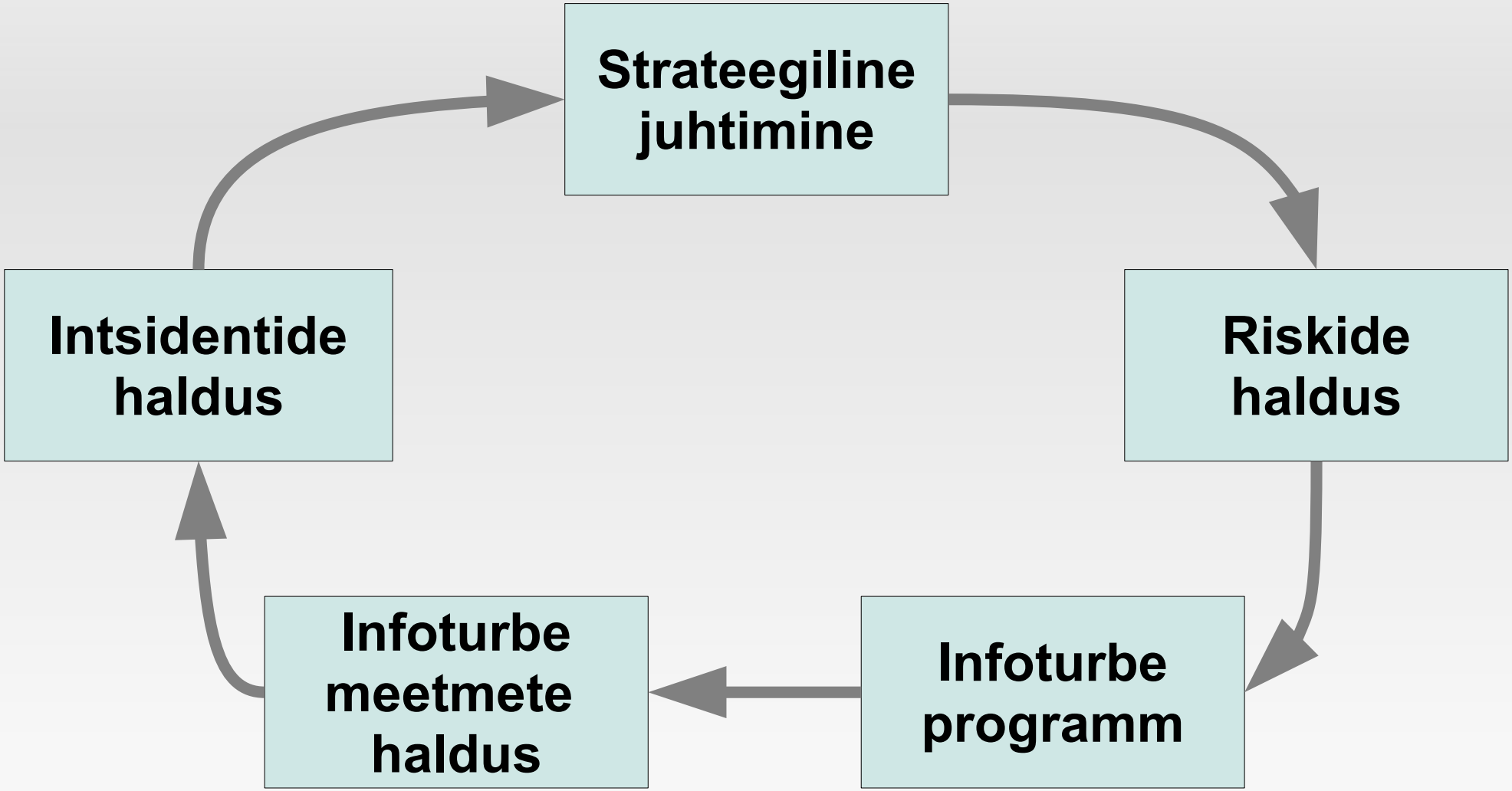


Klassikaline infoturbe juhtimine

- Turvameetmete rakendamise plaan
- Infoturbe teadlikkuse tõstmise programm
- mõõdikud infoturbe programmi tõhususe hindamiseks

Infoturbe programm

Klassikaline infoturbe juhtimine

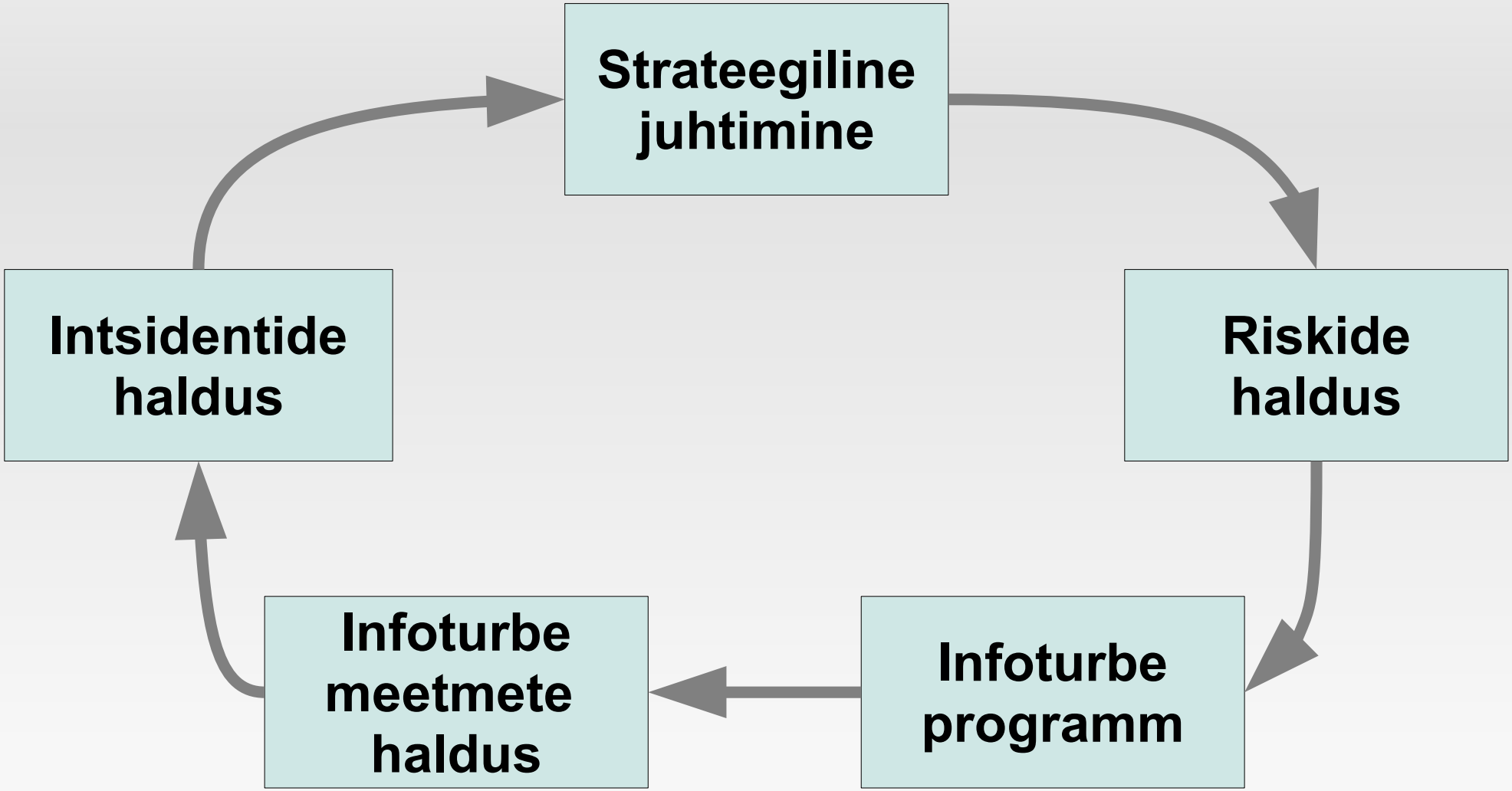


Klassikaline infoturbe juhtimine

- Ressursside haldus
- Jälgimine, et oleks vastavuses poliitikatega
- Mittevastavuste seire ja parandusmeetmed
  - Audit

Infoturbe meetmete haldus

Klassikaline infoturbe juhtimine



Klassikaline infoturbe juhtimine

Intsidentide haldus

- Intsidentide avastamine, identifitseerimine, analüüs ja reageerimine
- Seiresüsteemid
- Forensic

Infoturbe strateegiad

Standardid

Standardid

Kokku umbes sadakond erinevat

- ISKE/BSI
- ISO27000 seeria (umbes kümmekond)
- COBIT
- ITIL
- PCI-DSS (pangandus)
- HIPAA (tervishoid)

Standardid

- On abiks meeles pidamisel
- Aitavad põhjendada
- Rakendamine vajab mõistusega lähenemist
- Lisab jäikust

- Kui midagi läheb sandisti...
- Siis läheb ta sandisti vastavalt standardile

Milleks saab kasutada?

- Organisatsiooni struktuur
- Poliitikad, tegevusplaanid
- Kohustused, tavad
- Protseduurid, protsessid
- Ressursid, tehnoloogia
- Välised teenusepakkujad

Infoturbe mõjufaktorid ehk kuidas ennustada tulevikku

Üldised faktorid

- Absoluutne turvalisus on olukord, kus **kellelgi ega millelgi** ei ole võimalust (turvatavale objektile) kahju tekitada
- 100% turvalisust ei ole
- Kergem on kahjusid ära hoida, kui varasid taastada
- Turvameetmeid on **kõige kergem** juurutada (uue infosüsteemi) planeerimisprotsessi järgus
- **Turvalisus on protsess, mitte olek**

Üldiseid arvutialaseid fakte

- Moore seadus – transistorite arv kasvab kahe aastaga kaks korda
- Tänane arvuti on suures osas sama nagu i386 (1985)
- Tänane nutitelefon pärineb samast ajast (ARM/RISK 1985)
- Enamik interneti põhiprotokollidest pärineb 70...80-ndatest
  - TCP, SMTP 1973; DNS 1983; FTP 1985
- Viimased 25 aastat pole tehnikas põhimõttelisi muudatusi toimunud (skype näide)

Moore seaduse tuletised

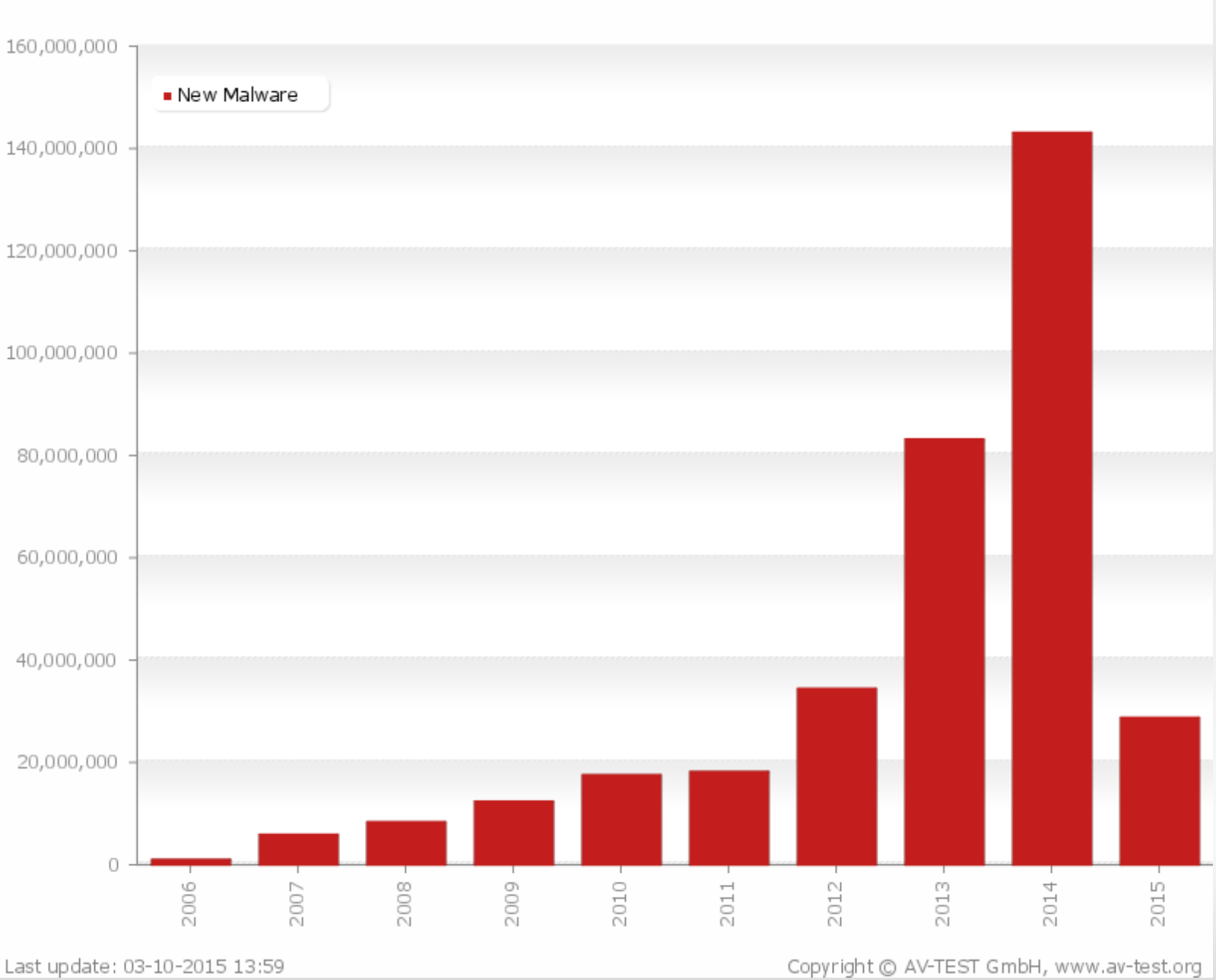
- Infosalvestuse võimekus kasvab
- Infoedastuse võimekus kasvab
- Infotöötlemine kasvab kahe aastaga kaks korda
- Samas tempos kasvab ka pahavara hulk ja kuritegevus

Mõisted

- **Trend** - Statistika mõiste, näitab aegrea pikaajalist arengusuunda.

Fakte küberkuritegevuse kohta

Pahavara kasv (2006-2015)



Küberkuritegevuse areng

- 20 sajand
  - Ülekaalus huvi ja „tahan teada“
- 21 sajand
  - Küberkuritegevus on muutunud äriks

Ründajate motivaatorid

- Huvi
- „Ma suudan“
- Huligaansus (seinte sodimine, bussipeatuste lõhkumine)
- Poliitika (hactivism)
- Raha
  - Varastamisväärtus (päriselus ja internetis)

    Kasum = tulu - kulu

Küberkuritegevuse ökonoomika

- Eesmärk on teenida raha
- Tulud (Krebs näide)
  - Turvanõrkuste müük (börs)
  - Reklaam (spämm, veeb)
  - Isikuandmete vargus (krediitkaardid, panga andmed)
- Kulud
  - riistvara, teadmised, aeg
  - Võimalikud karistused

Küberkuritegevuse ökonoomika (jätk)

- Sisenemiskulud on pea olematud
- Saadavad tulud... (Tšatsin ja Rove Digital)
  - Ainuüksi raha arvetel arestis prokuratuur miljoni euro ulatuses, ent prokuratuur on kasutamispiirangud peale pannud ka kokku 149le ühikule kinnisvarale.
  - isa Viktor on Äripäeva andmetel 6,7 miljoni euro suuruse varandusega Eesti rikaste edetabelis 283. kohal.
    - Delfi 10.11.2011

Tunnetus vs reaalsus

- Me märkame ja tunneme **turvatunnet**, kuid
  - turvatunne ei tähenda veel tegelikku turvalisust,
- turvatunde üks põhjustest võib olla lihtsalt teadmatus.

Turvatunne sõltub

- silmaringi avarusest ning võimest aru saada seoste ja sõltuvuste süsteemist
- teadmisest, mis on võimalik ning mis on ohtlik
- arusaamast enda ümber toimuvate protsessidest ja nende põhjustest
- ettenägemisvõimest (täpsus ja ulatus)
- iseseisva mõtlemise - analüüsi ja sünteesi, süstematiseerimise klassifitseerimise ja modelleerimise võimest
- inimese enese-, grupi-, ühiskonna- ja kultuuritunnetuse adekvaatsusest

Turvameetmete klassifikatsioon

Meetmete jagunemine aja alusel

- Ennetavad
  - Enne intsidenti
- Avastavad ja vähendavad (leevendavad)
  - Intsidendi ajal
- Taastavad
  - Pärast intsidenti
- Tagasiside ja analüüs
  - Valmisolek sarnasteks intsidentideks

Meetmete jagunemine toime järgi

- **Organisatsioonilised** – INIMESTELE (protseduurid, korrad, poliitikad, …)
- **Füüsilised** – RUUMIDELE ja FÜÜSILISTELE VAHENDITELE (uksed, aknad, lukud, …)
- **Infotehnoloogilised** – INFOSÜSTEEMIDELE (pääsuõigused, ID kaart, viirusetõrje, krüpto, varukoopiad, …)

- Ühe arvelt saab teisi (natuke) kompenseerida
- Üks ei toimi ilma teiseta

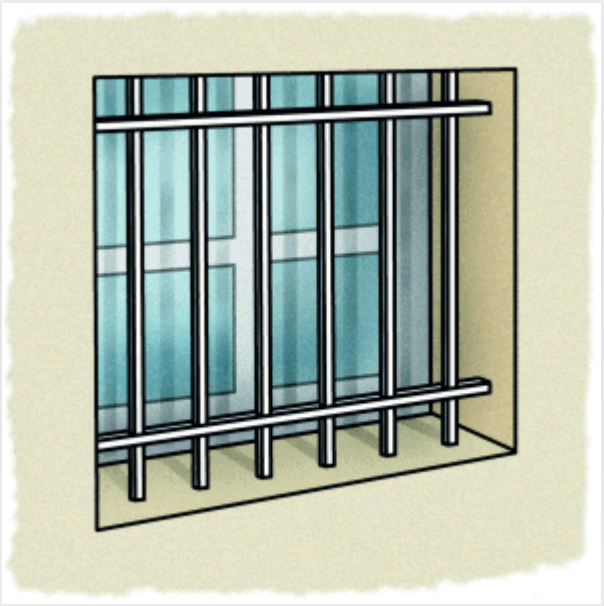
Turvameetmed taktikaliselt

Kehtib kohast ja ajast sõltumatult

- **Avasta** võimalik rünne
- **Tuvasta** millega on tegemist
- **Tõkesta** kui tegemist on ründega
- **Taasta** kui jõudis kahju teha

- Turvameetmed tuleb valida selle järgi, kus neist kõige rohkem kasu on

Füüsilised turvameetmed (näited)



Infotehnoloogilised turvameetmed

- Kasutajaõigused ja Paroolid
- Erinevad tehnilised meetmed
  - Viirustõrje
  - Tulemüür
  - Monitooring
- [...]

Organisatsioonilised turvameetmed (1)

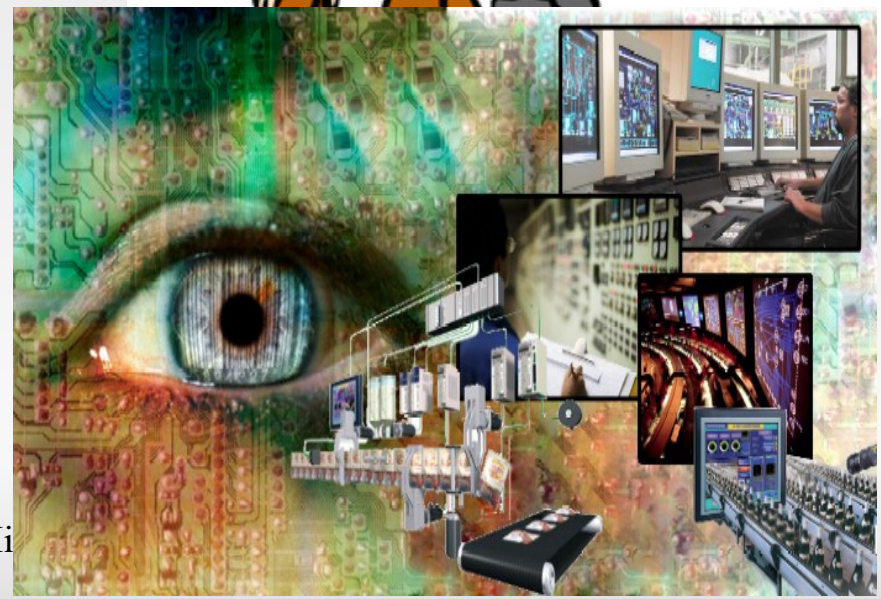
- Eeskirjad
- Korrad
- Juhendid

- Dokumentatsioon

Organisatsioonilised turvameetmed (2)

- Koolitused
- Juhendamised

- Organisatsioon ise



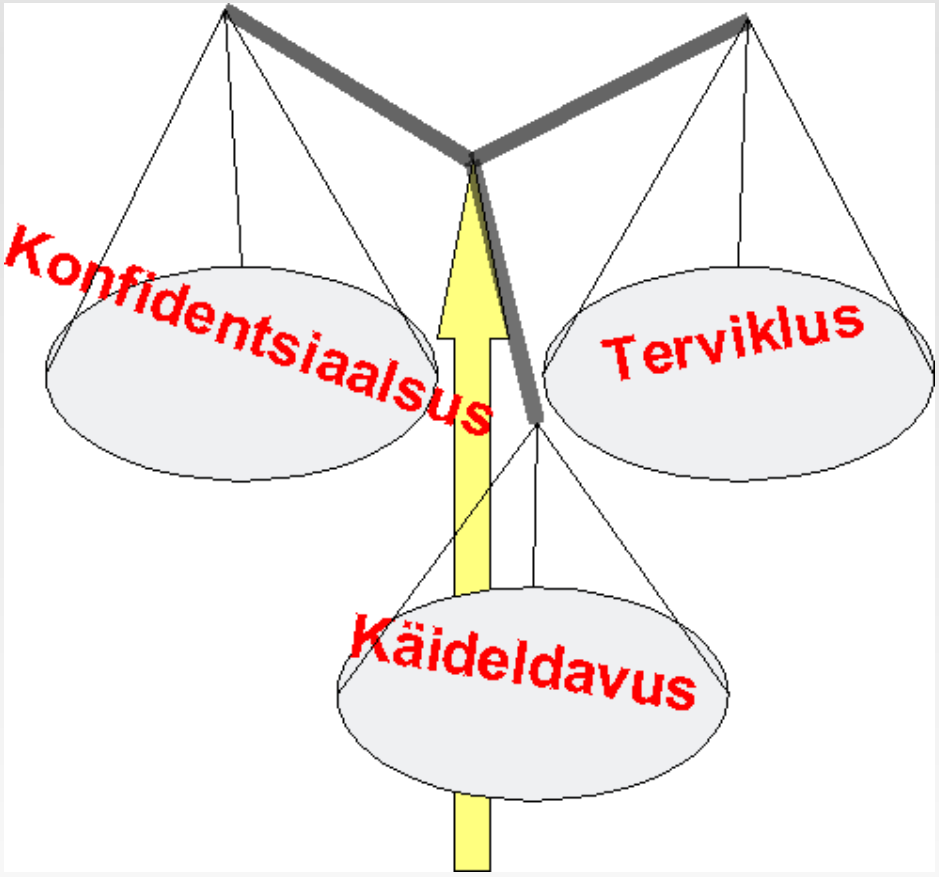
Turvaülesande lahendmine

Turvaülesande lahendamine

- Kirjeldada varad
- Fikseerida ohtude loetelu.
- Hinnata ohtudega seotud kahjusid.
- Hinnata ohtude tõenäosusi, vajaduse korral asendades reaalse maailma mingi abstraktse mudeliga.
- Valida välja need ohud, millega seotud risk (tõenäosuse ja kahju korrutis) on lubatust suurem.
- Valida turvameetmed, hinnates nende maksumust ja võrreldes neid riskiga.

Turbe tasakaalustamine

- Riskianalüüsid
- Mustad stsenaariumid
- Kasutajate soovid
- Olemasolevad ressursid



Turvaülesande lahendamisel

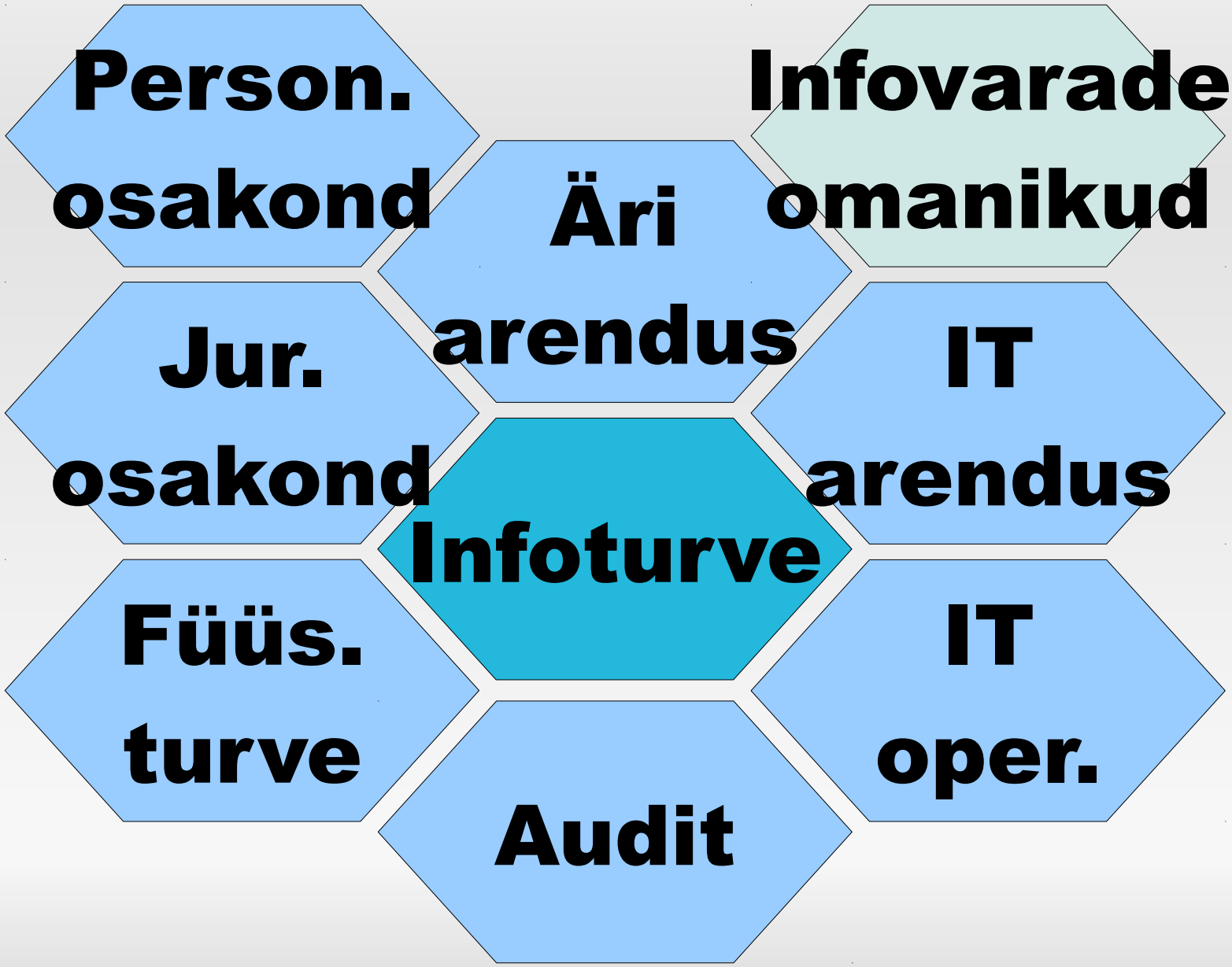
Abiks on:

- Häkkeri mõtteviis (kastist välja mõtlemine)
- Tähelepanelikkus (näeb ja kuuleb) ja seostamisoskus
  - Kergekujuline paranoia
- Tehnilised teadmised (süsteemianalüütik, adminn, progeja)

Infoturbe juhtimine

- “Müüa” turvet kui äri edendajat, mitte ainult kulu
- Nõuda vs ise teha – selged rollide jaotused
- Turbemeetmete läbisurumine (eelarved, töökavad) – alatine võitlus ressursside pärast (v.t. punkt 1)
- Riskide võtmise valmidus organisatsioonis (risk appetite) – kõiki riske ei saa nagunii ravida, kus on organisatsiooni “valulävi”
- Hinda oma org. võimekust (haldus, arendus), rongist pole mõtet ette joosta. Infoturve käib sama takti ülejäänud organisatsiooniga
- “Ma ju rääkisin...” sündroom – vahel paneb alles intsident rattad liikuma, hoia teemad sahtlis valmis

Partnerid


Person. osakond
Äri arendus
Infovarade omanikud
Jur. osakond
Infoturve
IT arendus
Füüs. turve
Audit
IT oper.

Nõuanded ja soovitused (1/2)

- Sotsiaalne kapital – head suhted ja usaldusväärsus
  - Organisatsioonis sees
  - Turvakommuun
  - CERT.ee
- Leida juhtumite kohta näiteid avalikust meediast
  - Püüdke aru saada mis konkreetselt kõnetab
  - Vastavalt modifitseerida oma oma organisatsiooni jaoks
  - Hea abivahend ka riskistsenaariumite jaoks

Nõuanded ja soovitused (2/2)

Info hankimiseks head kohad (kasutage RSS-i)

- SANS.org (standardid, õppematerjalid jms)
- crebsonsecurity.com (artikleid silmaringi laiendamiseks)
- darkreading.com (artikleid silmaringi laiendamiseks)
- csoonline.com (artikleid silmaringi laiendamiseks)
- full disclosure (postilist avastatud turvanõrkustest)
- securityfocus.com (uuenduste info ja bugtrag)
- RIA.ee (eesti kohta käiv info, sh. artikleid silmaringi laiendamiseks)

Kirjutamata reegleid

- Fooriprotokoll (traffic light protocol)
- Osalemine koosviibimistel
  - Chatham House'i reegel
- Netikett – neti etikett

Fooriprotokoll

- Tähistatakse FP:VÄRV või TLP:COLOR
- Kasutusel neli värvi
  - Punane
  - Kollane
  - Roheline
  - Valge
- Mõnes kohas on kasutusel rohkem värve
- Eestis kehtivad reeglid https://www.ria.ee/fooriprotokoll/

Fooriprotokoll – punane

- FP:PUNANE või TLP:RED
- Allikas võib kasutada FP PUNAST värvi, kui kõrvalised osalised ei tohi teabe põhjal mingil viisil tegutseda ning kui teave võib väärkasutuse korral avaldada mõju asjaosalise privaatsusele, mainele või tegevusele.
- Saaja ei tohi FP PUNASE värviga tähistatud teavet jagada ühegi osalisega, kes ei ole seotud konkreetse teabevahetuse, kohtumise või vestlusega, mille käigus teavet algselt avaldatakse.

Fooriprotokoll – kollane

- FP:KOLLANE või TLP:YELLOW
- Allikas võib kasutada FP KOLLAST värvi, kui teabe põhjal tulemuslikuks tegutsemiseks on vaja kellegi toetust, kuid sellega kaasneb oht privaatsusele, mainele või tegevusele, kui teavet jagatakse väljaspool seotud organisatsioone.
- Saaja tohib jagada FP KOLLASE värviga tähistatud teavet üksnes oma organisatsiooni liikmetega ja/või parteritega, kellel on otsene teadmisvajadus, ning vaid sellises ulatuses, kuivõrd on vajalik teabe põhjal tegutsemiseks.

Fooriprotokoll – roheline

- FP:ROHELINE või TLP:GREEN
- Allikas võib kasutada FP ROHELIST värvi, kui teave on kasulik kõikidele osalevatele organisatsioonidele ning laiema ringkonna või valdkonna partneritele.
- Saaja võib jagada FP ROHELISE värviga tähistatud teavet oma valdkonna või ringkonna partnerite ja partnerorganisatsioonidega, kuid seda ei tohi teha avalike kanalite kaudu.

Fooriprotokoll – valge

- FP:VALGE või TLP:WHITE
- Allikas võib kasutada FP VALGET värvi, kui teabega kaasneb minimaalne tõenäoline väärkasutuse oht või puudub see üldse, järgides seejuures kohaldatavaid eeskirju ja üldsusele avaldamise korda.
- FP VALGE värviga tähistatud teavet võib levitada piiramatult kooskõlas autoriõigust käsitlevate sätetega.

Chatham House’i reegel

- Kui kohtumine või osa sellest toimub Chatham House’i reegli põhjal, on sellel osalenuil vaba voli kasutada neile avaldatud teavet ja seisukohti kahel tingimusel:
- Avalikustada ei tohi ei kõneisikute ega ühegi teise kohtumisel osalenu identiteeti ega liikmelisust.
- Avalikustada ei tohi, et informatsioon saadi just tollelt kohtumiselt.

Netikett

- Pikk jutt http://netikett.wikispaces.com/
- „Parim praktika” (best practice)
- On kujunenud pika aja jooksul

Turvameetmed ja nende rakendamine

Turvameetmete valik

- Ise välja nuputada
- Lähtuda mingist standardist
  - ISKE
  - ISO 27k
  - ...
- Head ja vead

ISKE

- Kokku 85 moodulit
- Viis gruppi
  - B1: Üldkomponendid
  - B2 Infrastruktuur
  - B3 IT-süsteemid
  - B4 Võrgud
  - B5 Rakendused

ISO 27001/2 standardi peatükid:

- Turvapoliitika;
- Infoturbe korraldus;
- Varade haldus;
- Inimressursi turve;
- Füüsiline ja keskkonna turve;
- Side ja käituse haldus;
- Pääsu reguleerimine;
- Infosüsteemide hankimine, väljatöötamine ja hooldus;
- Infoturbeintsidentide haldus;
- Jätkusuutlikkuse haldus;
- Vastavus.

Klassikaline infoturbe juhtimine

Strateegiline juhtimine

- Kehtestada ja juurutada raamistik, mis kindlustaks, et:
- Infoturbestrateegiad oleksid kooskõlas ärivajadustega
- Vastaksid kehtivale seadusandlusele
- Vastaksid standarditele

Turvapoliitika (1/2)

Strateegiline dokument (policy)

- Minimaalselt sisaldab
  - Juhtkonna kohustumise põhimõtet
  - Turvameetmete valiku aluspõhimõtteid
  - Infoturbe korralduse põhimõtteid
  - Vastavuse põhimõtet
  - Viited õigusaktidele, millest lähtutakse
  - Viited spetsiifilistele poliitikatele või juhenditele
- Sellisel juhul A4 dokument

Turvapoliitika (2/2)

Pikk versioon

- Sisaldab kõik 11 peatükki
- Sellisel juhul on maht …

Nõuandeid ja soovitusi

Isiklik soovitus

- Tõde on kusagil vahepeal
- Mis poliitikasse, mis mujale… ?

Vahelugu

- Poliitikad (policy) – strateegia
- Korrad
- Juhendid
- Tuleks valida – mis tasemel

Infoturbe korraldus (1/2)

- Juhtkonna toetus;
- Kõigi töötajate kaasatus;
- Fikseeritud kokkulepped – kohustused ja vastutus;
- Välised osapooled – kokkulepe mh infoturvalisuse tagamise kohta;
- Sõltumatu läbivaatus, sh audit.

Infoturbe korraldus (rollid)

Õigused, kohustused ja vastutus

- Juhtkond
- Infoturbe kordineerija (turvajuht)
- Infovarade eest vastutajad
- Infovarade kasutajad

Infoturbe korraldus (2/2)

- Riskid on kaardistatud
- Infoturbe intsidentide tekkimise ennetamiseks on rakendatud sobivad meetmed
- Infoturbe intsidentide tekkimisel rakendatakse eeldefineeritud protseduurid
- On olemas tegevuskavad, mis tagavad intsidendi kiire lahenduse kahju minimeerimiseks

Varade haldus (1/2)

- (Info)varade omanikud:
  - Turbe vajadus;
  - Nõuded;
  - Vastutus.
- Ülevaade (info)varadest, nende asukohast ja omanikest - inventuur;
- Riist- ja tarkvara profiilid - kinnitatud;
- Legaalsus – litsentsid, omandiõigus, autoriõigus;

Varade haldus (2/2)

- Andmekandjate haldus – vara väärtus vs info väärtus;
- Hooldus – lepingulised kohustused, tingimused, garantii;
- Tagavara – kriitilised seadmed, tarkvara, SPO (Single Point of Failure)
- Uuendamine ja paikamine:
  - Varajane adopteerija;
  - Hiline kasutuselevõtja

Inimressursi turve (1/2)

- Enne töölevõtmist – sobivuse/vastavuse kontroll;
- Infoturbe tagamine tööülesannete täitmisel on iga töötaja vastutus ja see peab selgelt väljenduma nii organisatsiooni kultuuris kui ka töötajatega sõlmitavates kokkulepetes.
- Kohustused ja vastutus - määratud;
- Turvateadlikkus – tagatud.
  - Koolituse kontseptsioon

Inimressursi turve (2/2)

- Töösuhte lõpetamine:
  - Varade tagastamine
  - Pääsuõiguste sulgemine
  - Ringkäigu leht
- Hilisemad kohustused:
  - Seoses konfidentsiaalse infoga;
  - Seoses ärisaladusega

Füüsiline ja keskkonna turve (1/2)

- Kaardistada piirkonnad, mida infoturbe seisukohast tuleb kaitsta ja millele ligipääsu tuleb piirata.
- Kriitilised infovarad (põhisüsteemid, serverid, võrguseadmed jms) piiratud juurdepääsuga turvaaladele, täiendavad füüsilised meetmed ligipääsu, kahjustuste ja muude keskkonnaohtude (tuli, vesi, niiskus, temperatuur jms) vastu.

Füüsiline ja keskkonna turve

- Punane tsoon
  - Kriitiliste süsteemide asukoht
  - Juurdepääs ainult volitatud isikutel
- Kollane tsoon
  - Töökabinetid
  - Külalised ainult loa ja/või saatjaga
- Roheline tsoon
  - Klienditeeninduse ala

Füüsiline ja keskkonna turve (2/2)

- Seadmete turve – seadmete asukoht, paigutus, kasutamise reeglid jms
- Seadmete tehniline hooldus
  - Panga näide
- Seadmete kaitse väljaspool territooriumi
- Seadmete kõrvaldamine või taaskasutus

Side ja käituse haldus (1/5)

- Muudatuste haldus – uuendamine ja paikamine
- Kohustuste lahusus – tegija ja kontrollija roll
- Arendus, testimine ja töö lahku
  - Ideaalis ongi kolm keskkonda
- Väljasttellimise haldus
  - Teenustasemed
  - Tarnija valimine ja muutmine
  - Teenuse seire

Side ja käituse haldus (2/5)

- Süsteemide plaanimine ja vastuvõtmine
  - Suutvuse planeerimine
  - Vastuvõtmise protseduurid
- Viirustõrje kontseptsioon
- Võrguturbe haldus
  - Võrgutube meetmed (tulemüür...)
  - Teenuste turve (paroolid, piirangud…)

Side ja käituse haldus (3/5)

Varundamine (poliitika ja protseduurid)

- informatsioon, millest on vaja teha varukoopia
- varukoopiate tegemise ulatus ja sagedus
- vastutus varukoopiate tegemise eest
- varukoopiate säilitamise aeg
- varukoopiast andmete taastamine
  - testimine

Side ja käituse haldus (4/5)

- Infokandjate turve
  - Ird-infokandjate haldus
  - Infokandjate kasutuselt kõrvaldamine
- Infovahetuse poliitikad ja protseduurid
  - Infovahetuslepped
  - Infokandjate trantsport
  - Elektrooniline infovahetus

Side ja käituse haldus (5/5)

Seire

- Revisjonilogi (Audit log)
- Süsteemide kasutamise seire
- Logide kaitse
- Administraatorite ja operaatorite tegevuste logimine
- Tõrgete logimine
- Kellade sünkroniseerimine

Pääsu reguleerimine (1/3)

- Nii füüsiline kui ka elektrooniline juurdepääs
- Juurdepääsu poliitika
  - Õiguste andmine
  - Õiguste muutmine
  - Õiguste peatamine või lõpetamine
- *Need to know*
- Pääsuõiguste seire ja ülevaatus
- Pääsuvahendite haldus
  - Paroolid, kaardid, võtmed

Pääsu reguleerimine (2/3)

Juurdepääsukohad:

- töökoha arvutile ligipääs;
- andmesidevõrku pääs;
- operatsioonisüsteemidele ligipääs;
- rakendustele ja andmebaasidele ligipääs;
- Mobiilne- ja kaugjuurdepääs infovaradele
- ajutiste töötajate ja väliste kasutajate ligipääs infosüsteemile

Pääsu reguleerimine (3/3)

- Eriõigustega kasutajate haldus – vajalik ja piisav hulk, kontroll
- Liidesed, kanalid – kellega ja kuidas, milliste kanalite kaudu saab teenustele/infovaradele ligi
- Kaugtöö – tehnoloogiline kaitse, kellele, mis tingimustel, kontroll
- BYOD – Bring Your Own Device

Infosüsteemide hankimine, väljatöötamine ja hooldus (1/2)

- Infosüsteemide turvalisuse vajadus ja vastavad kontrollid määratakse infovara omaniku poolt või temaga koostöös.
- Andmekvaliteedi tagamise kontrollid rakendatud nii andmete sisestamisel kui väljundi kasutamisel.
- Krüpteerimise vajadus – konfidentsiaalsus ja terviklus vs käideldavus
- Turvanõuded riistvarale ja OpSüsteemile
- Tarkvara arenduse väljasttellimine

Infosüsteemide hankimine, väljatöötamine ja hooldus (2/2)

- Arenduste haldus
  - Lähteülesanne
  - Testimine (moodultest, integratsioonitest, süsteemitest, turvatest);
  - Juurutamine
- Muudatuste haldus
  - Hädamuudatused
- Uuenduste ja turvaparanduste haldus
  - Allikad
  - Sagedus
  - Testimine

Infoturbeintsidentide haldus (1/2)

- Teavitamine turbe rikkumisest, registreerimine, intsidendi verifitseerimine ja vastumeetmete rakendamine
- Analüüs, et välja selgitada põhjused, tuvastada puudused ja välja töötada meetmed puuduste likvideerimiseks ning seeläbi vältida sarnaste intsidentide kordumist tulevikus

Infoturbeintsidentide haldus (2/2)

- Plaanimine
- Tuvastamine
- Kindlaks tegemine
- Hindamine
- Raporteerimine ja kommunikatsioon
  - Erinevad sihtgrupid (juhtkond, töötajad, partnerid, avalikkus, CERT)
- Tagajärgede vähendamine
- Taastamine

Jätkusuutlikkuse haldus (1/5)

Talitluspidevus/toimepidevus

- Talitluspidevuse protsess: kes vastutab (kindlasti ei ole ainult IT mure) ja kes korraldab, kes ja kuidas on kaasatud;
- Talitluspidevuse planeerimine: kriitilised teenused, vastutajad, kommunikatsioon, välised osapooled, varuasukoht;
- Taaste planeerimine: võimalus taastada vähemalt kriitilised teenused/andmed, taastamise stsenaariumid, taasteplaani testimine, taasteplaani hoidmine.

Jätkusuutlikuse akronüüme (2/5)

- BIA - Business Impact Analysis (ärimõjude analüüs)
- RTO – recovery time objective (soovitav taasteaeg) äripoole ootus
- RTA – recovery time actual (tegelik taasteaeg) plaani testimisel saadud
- RPO – recovery point objective (maksimaalne andmekadu) äripoole ootus

Jätkusuutlikkuse haldus (3/5)

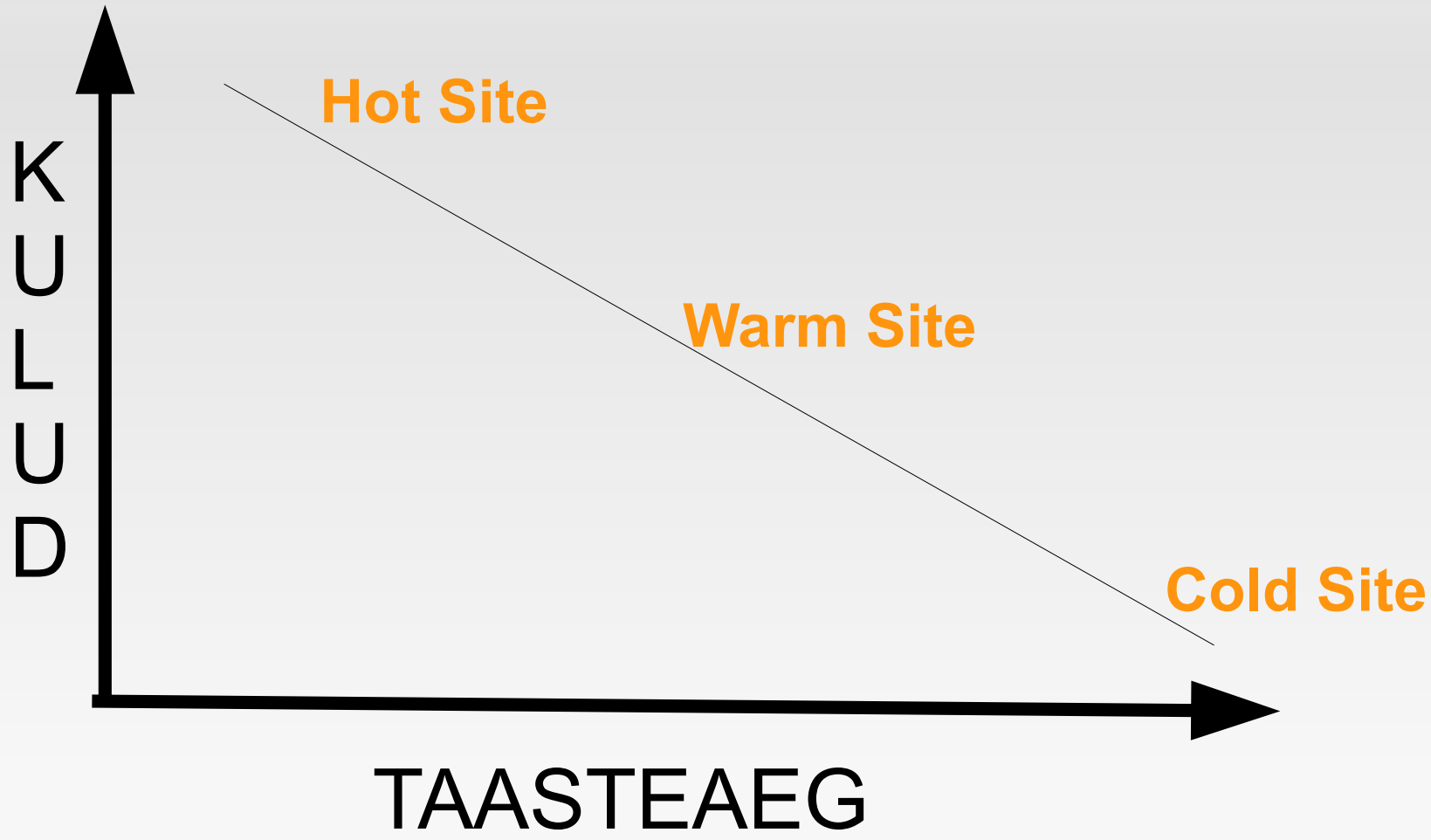
Katkestus (disruption)

- Sündmus < RTO
- Mõjud on limiteeritud ja kontrolli all
- Katkestuse maksumus ei ületa teatud rahalist piiri (näiteks kindlustus)

Hädaolukord (disaster)

- Sündmus > RTO
- Mõjud on ulatuslikud ja kontrollimatud
- Katkestuse maksumus ületab teatud rahalist piiri (näiteks kindlustus)

Jätkusuutlikkuse haldus (4/5)



Jätkusuutlikkuse haldus (5/5)

- Jätkusuutlikkuse plaanid
  - Testimine
  - Haldus
  - Muutmine
- …
- Avariikäsiraamat

Vastavus (1/3)

Compliance

- Seadus, määrus;
- Sisemine poliitika;
- Grupi nõudmised;
- Audit (sise ja välis);
- Järelevalve;
- Vastavussertifikaat;
- Standardid, hea tava

Vastavus (2/3)

- Infoturbe nõuetele vastavust tuleb ettevõttes pidevalt jälgida ja mõõta, rakendada sõltumatu kontrollifunktsioon nõuete täitmise hindamiseks.
- Infoturbe auditi planeerimisel:
  - eesmärk,
  - protseduur,
  - auditi plaan, audiitori tööülesanded
  - auditi plaan, auditeeritava panus.

Vastavus (3/3)

- Täiendus põhjalikule auditile - ründetestide (*penetration testing*) läbiviimine.
- Ründetestide läbiviimisel peab olema tagatud, et ettevõtte normaalne töö ei saaks häiritud ega ettevõtte tööalane informatsioon kahjustatud.
- Ründetestid tuleb teostada kontollitud keskkonnas.

Nõuandeid ja soovitusi

- https://www.ria.ee/raamdokumentide-naidised/
- https://www.ria.ee/iske-dokumendid/

- https://www.sans.org/security-resources/policies/

- Standardid www.evs.ee
  - Eestis on odavam, kui välismaal
  - Tõlkeks kulub aega

Küsimused?