Infoturbe haldus

Hillar Põldmaa

Kursuse kava

- Vormilised teemad
- Kursuse kirjeldus (lektor)
- Kursuse läbimine
- Ootused kursuse kohta (kuulajad)

Materjalid

- Loengu slaidid ja kõik lisamaterjalid moodles
- Kursuse nimetus

  IFI7045.DT Infoturbe haldus

Loengud

1) loeng L 10.09.2016 10:00 - 14:00
2) loeng L 24.09.2016 10:00 - 14:00
3) **seminar L** 03.12.2016 10:00 - 14:00
4) loeng L 17.12.2016 10:00 - 14:00
5) **seminar** kusagil jaanuaris – iseseisvate tööde ettekanded

Kursuse läbimiseks

- Iga üliõpilane
- Esitab iseseisva töö
- osaleb grupitööna valmivas arvestustöös ja selle kaitsmisel seminaris
- sooritab eksami.
- Eksamile pääsemise eelduseks on arvestustööde esitamine ja kaitsmine.
- Kõik ühes rühmas osalenud üliõpilased saavad arvestustöö eest sama palju punkte.

Arvestustöö rühmatööna

- kaardistatakse ettevõtte infovarad – maksimaalselt 10 punkti;
- tehakse riskianalüüs – maksimaalselt 10 punkti;
- planeeritakse turvameetmed – maksimaalselt 10 punkti;
- koostatakse infoturbe poliitika – maksimaalselt 10 punkti;
- koostatakse jätkusuutlikkuse plaan – maksimaalselt 10 punkti.
- Arvestustöö koostamise juhised Moodles

Eksam

- Moodles
- 30 küsimust (igast kursuse teemast paar);
- Loengumaterjalide põhjal;
- Aega 90 minutit;

Hindamine

- A – 91-100 punkti
- B - 81-90 punkti
- C – 71-80 punkti
- D – 61-70 punkti
- E – 51-60 punkti

Loeng
10.09.2016

Loengus käsitletakse (1/2)

- Mis on info, mida me turvame?
- Mis on infoturve?
- Olulised mõisted;
- Miks on vaja infoturvet?
- Infoturbe lähtekohad;
- Infoturbe seosed üldise juhtimisega ja IT-juhtimisega;
- Infoturve, kui protsess.

Loengus käsitletakse (2/2)

- Kuidas selgitada välja turbe vajadused?
- Turvariskide kaalutlemine;
- Infoturbeohud;
- Riskide määratlemine ja analüüs;
- Riskide kaalumine ja riskiskaalad;
- Jääkriski määramine ja kinnitamine.

Praktika

- kaardistatakse ettevõtte infovarad;
- tehakse riskianalüüs

Loeng
24.09.2016

Loengus käsitletakse (1/2)

- Infoturbe standardid ja hea tava;
- Infoturbe halduse protsess.
- Infoturbe halduse meetmed:
- ISO 27001/27002

Loengus käsitletakse (2/2)

- Füüsilised infoturbe meetmed;
- Organisatsioonilised infoturbe meetmed;
- Tehnoloogilised infoturbe meetmed.
- Infoturbepoliitika:
- Infoturbepoliitika dokument;
- Infoturbe poliitika rakendamine ja kontroll;
- Infoturbepoliitika läbivaatus.

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.

Praktika

- planeeritakse turvameetmed;
- koostatakse infoturbe poliitika.

Loeng
17.12.2016

Loengus käsitletakse (1/2)

- Riskijuhtimine;
- Intsidendihalduse ja jätkusuutlikuse plaanimine
- Intsidendi tuvastamine ja kindlaks tegemine
  - Seire (monitooring);
  - Seirelogide kaitse;
  - Tõrgete logimine.
- Intsidendi hindamine;
- Infoturbeintsidendist või -nõrkusest teavitamine
  - Kommunikatsioon ja raporteerimine.
- Intsidendi tagajärgede leevendamine;
- Intsidendist taastamine.

Loengus käsitletakse (2/2)

- Jätkusuutlikkuse tagamine:
- Talitluspidevuse protsess;
- Talitluspidevuse planeerimine;
- Taaste planeerimine;
- Talitluspidevuse testimine.
- Turbenõuete vastavus:
  - Vastavus õigusaktide nõuetele;
  - Vastavus infoturbepoliitikale;
  - Infosüsteemide auditeerimisvajadus;
  - Infoturbe dokumentide auditeerimine;
  - Infoturbe korralduse auditeerimine.
- Infoturbe järelevalve ja audteerimine.

Praktika

- koostatakse jätkusuutlikkuse plaan.

INFOTURVE

Tuletame meelde põhimõisteid

Informatsioon ehk teave

- **Informatsioon** ehk teave (*information*) – teadmine, mis puudutab objekte ja fakte, sündmusi, asju, protsesse või ideid ning millel on teatavas kontekstis eritähendus
- Informatsioonil iseenesest puudub vorm. See tekib alles esituse (andmete) kaudu
- **Andmed** (data) – informatsiooni esitus formaliseeritud kujul, mis sobib edastuseks, tõlgenduseks või töötluseks

Andmed ja informatsioon

Kui meil on mingi number

12 aastat vanglas

- Andmed muutuvad informatsiooniks läbi **konteksti** ja läbi inimese poolse **tõlgenduse**
- Andmeid andmete kohta nimetatatakse metaandmeteks. **Metaandmed** aitavad andmetest informatsiooni kujundada

Informatsiooni omadused

- Kättesaadavus (accessibility)
- Vorming (format)
- Ühilduvus (compatibility)
- Asjakohasus (relevance)
- Ajakohasus (timeliness)
- Õigsus (validity),
- Täpsus (accuracy),
- Täielikkus (completeness),
- Sidusus (koherentsus) (coherence)
- Konfidentsiaalsus (Confidentiality)

Informatsiooni omadused on kvaliteedi näitajad

Informatsiooni omadused infoturbes

Omadused on kokku võetud kolme gruppi

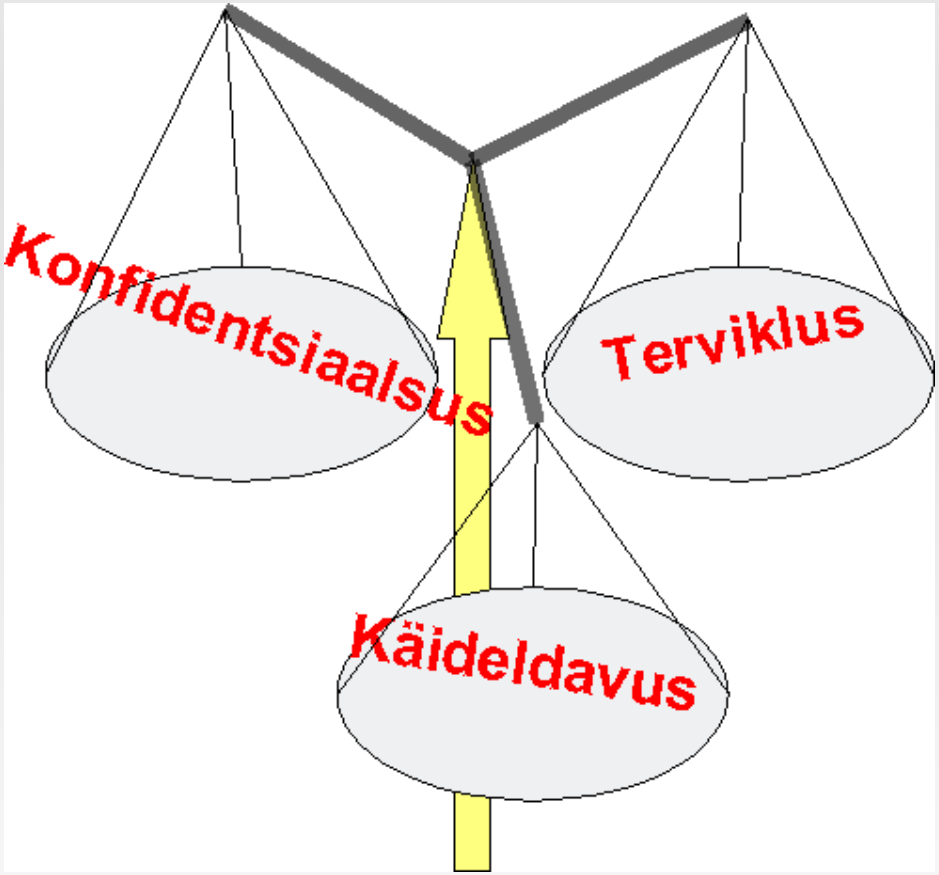
- **Käideldavus** (availability) – kättesaadavus (accessibility), vorming (format), ühilduvus (compatibility), asjakohasus (relevance), ajakohasus (timeliness)
- **Terviklus** (integrity) – õigsus (validity), täpsus (accuracy), täielikkus (completeness), sidusus (koherentsus) (coherence)
  - Siia juurde käib ka info muutmise kohta
- **Konfidentsiaalsus** (Confidentiality)

Põhimõisted

- **Käideldavus** tähendab, et andmed on kättesaadavad **õigeaegselt** ja **mugavalt**.
  - See on andmetöötluse juures kõige olulisem aspekt – kui käideldavus rikutud, siis on väga raske rääkida terviklusest ja konfidentsiaalsusest
- **Terviklus** tähendab, et andmed on õiged, täielikud ja pärinevad autentsest allikast.
  - Infoturbe kontekstis tuleb jälgida, et lisaks andmetele ei oleks volitamata muudetud ka andmete looja, loomisaeg jms.
- **Konfidentsiaalsus** tähendab, et andmed on kättesaadavad ainult volitatud isikutele ja kättesaamatud kõigile teistele.
  - See on ajalooliselt infoturbe kõige esimene aspekt (salakirjad, paroolid sõjaajal, täna krüptograafia).

Infoturbe komponentide seosed

- Kolm komponenti
  - Terviklus
  - Käideldavus
  - Konfidentsiaalsus
- Vajab tasakaalustamist
  - Ühega on natuke võimalik teist kompenseerida
- **Ettevaatust** – ühele õlale liigselt panustades võib uppi minna



Käideldavus vs konfidentsiaalsus

- Konfidentsiaalsuse tagamine on lihtne
  - Keerame käideldavuse kinni
  - Kui keegi andmeid ei näe, on konfidentsiaalsus tagatud absoluutselt
- Käideldavus tähendab eelkõige informatsiooni olemasolu ja tema kasutusmugavust

Konfidentsiaalsus vs terviklus

- Kui meil on mingi number

  36710140248 = Hillar Põldmaa

- Isikukood defineerib inimese üheselt
- Terviklus on 100%, konfidentsiaalsust ei ole

Põhimõisted

- **Infoturve** (*information security*) – riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele, sealhulgas andmekaitse realiseerimise vahend
- **Vara** (*Asset*) – kõik asutuse objektid, mis vajavad kaitset ja omavad väärtust.
  - Näited: Andmed, meiliteenus, tarkvara, server, protsessid, mööbel, ruumid, inimesed, immateriaalsed varad nagu maine
- **Oht** (*Threat*) – võimalik soovimatu sündmus, mis võib avaldada negatiivset mõju varale

Põhimõisted

- **Nõrkus/haavatavus** (*Vulnerability*) – vara, süsteemi või protsessi nõrk koht. Turvameetme puudumine või ebapiisavus
- **Avatus/Kaitsetus** (*Exposure*) – vara kaitsetus ohu realiseerumise eest nõrkuse tõttu
- **Risk** (*Risk*) – tõenäosus, et oht realiseerub läbi nõrkuse ja tekib kahju
- **Turvameede** (*Safeguard, security measure*) – riski vähendamise abinõu, poliitika, protseduur, seade vms

Põhimõisted

- **Andmekogu** – andmete korrastatud kogum
- **El pea** olema elektrooniline
  - Perfokaardid
  - Kaustik ja pastakas

Põhimõisted

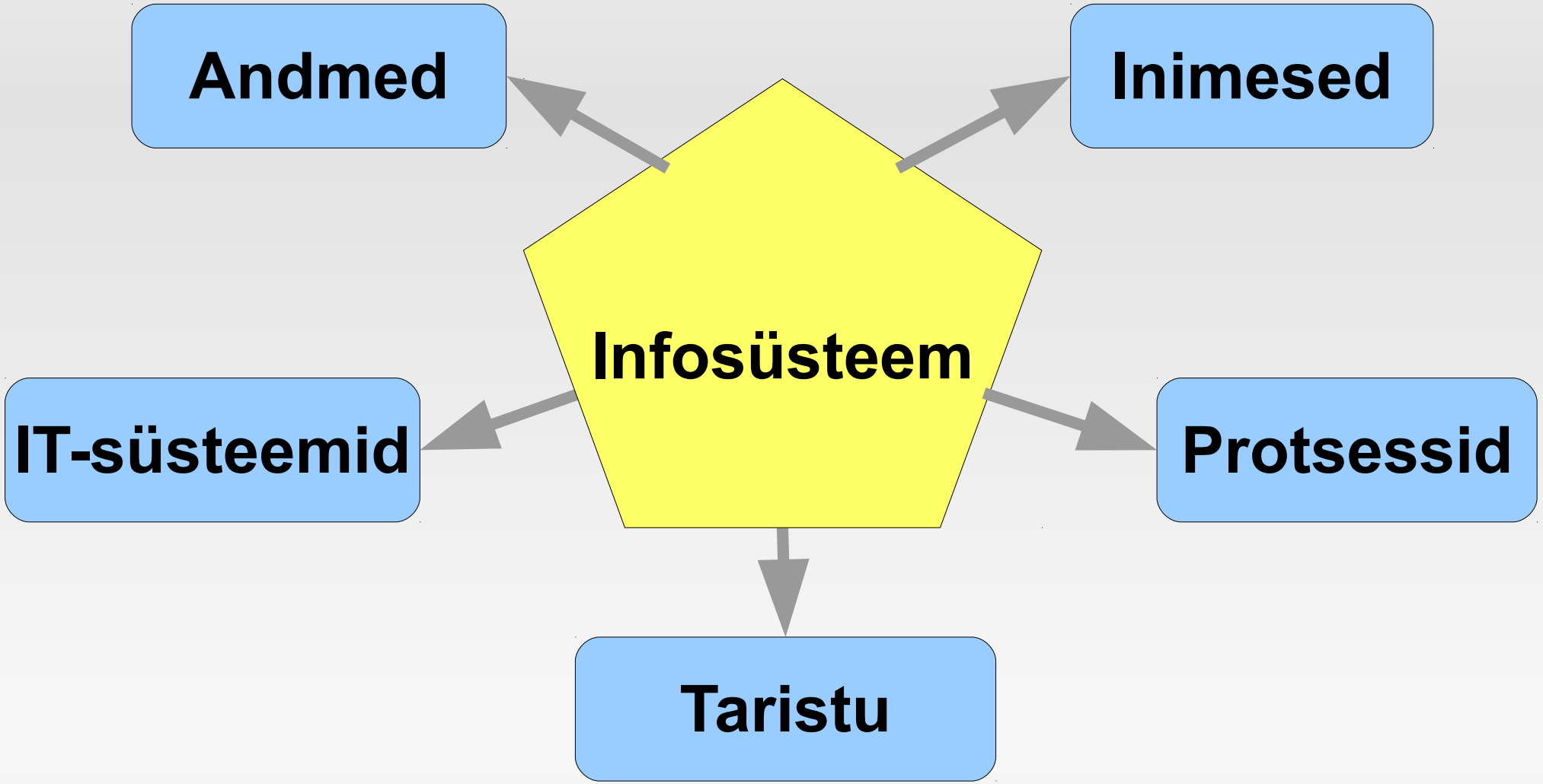
- **Andmekaitse** (Data Protection) – tähistab tänapäeval isikuandmete kaitset
- **Isikuandmed** – kõik isikut üheselt kirjeldavad andmed

Põhimõisted

Infovarad

- **Informatsioon** (andmed) – mida me igapäevatööks vajame ja milleta me funktsiooni täita ei saa;
- **Infosüsteemid** ja **andmekogud** – andmete töötlemise jaoks vajalik (eritarkvara, standardtarkvara, andmebaasid jms);
- **Vahendid** – arvuti (lauaarvuti, sülearvuti, pihuarvuti), lisaseadmed (printer, fax), võrguühendus (Internet, sisevõrk), andmekandjad (mälupulgad, CD, DVD jms.)
- **Protsessid** – informatsiooni töötlemine

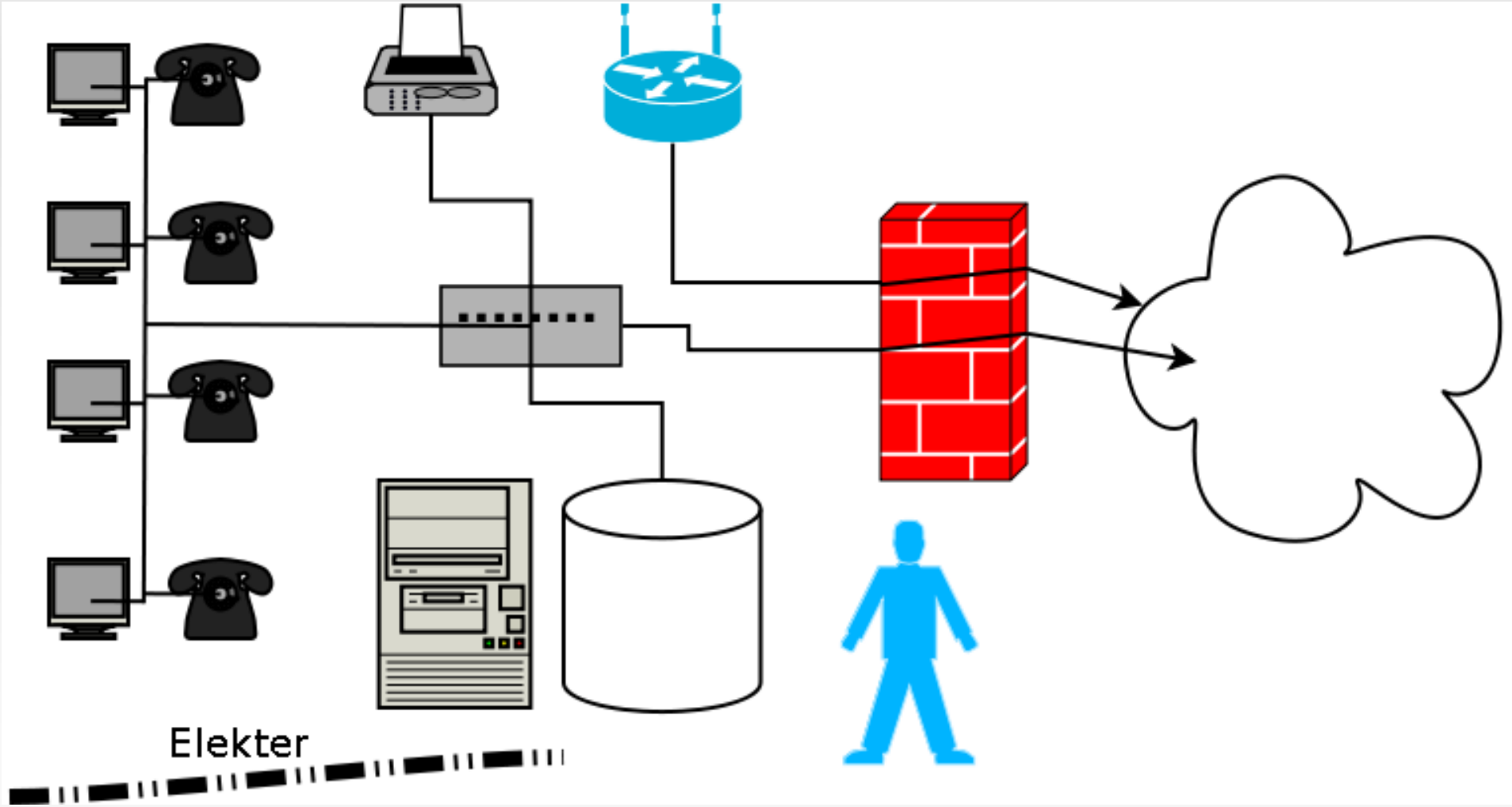
Infosüsteem



Infosüsteem

- Põhifunktsioone toetavad rakendussüsteemid (riistvara; tarkvara; sideseadmed)
- Infosüsteemi juurde kuuluvad ka tugiteenused, -seadmed ja -süsteemid
  - Elekter, varugeneraator, kaablid, ruumid
- **Infosüsteemid algavad ja lõppevad inimesega**

Infosüsteem



Infosüsteemi kaardistus

- Serverid
- Võrk
- Tööjaamad
  - Mis siia alla kuulub?
- Muud seadmed ja vahendid
- Tarkvara
- Juhendid ja korrad
- Inimesed
- **Kaardistuse detailsuse probleem**

Infoturbe eesmärk

Infoturve on informatsiooni kaitsmine:

- Läbi turvameetmete rakendamise
- Mitmesuguste ohtude eest
- Majanduslikult mõttekalt/optimaalselt

Eesmärgiga:

- tagada talitluse jätkuvus
- minimeerida äririski
- maksimeerida investeeringute tasuvust
- maksimeerida soodsaid ärilisi võimalusi.

Infoturbe tegevused

Infoturve on informatsiooni kaitsmine:

- Läbi turvameetmete rakendamise
- Mitmesuguste ohtude eest
- Majanduslikult mõttekalt/optimaalselt

Turvameetmete liigid

- **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

Erinevatest turvameetetest ja nende rakendamisest räägime edaspidistes loengutes

Infoturbe tegevused

Infoturve on informatsiooni kaitsmine:

- Läbi turvameetmete rakendamise
- Mitmesuguste ohtude eest
- Majanduslikult mõttekalt/optimaalselt

Ohud

- Inimtegevusest tulenev
- Loodussündmused
- Tehnoloogia
- Majanduslikud ning õiguslikud ohud

Inimtegevusest tulenevad ohud

- Sisemised ja välimised
- Pareto (80:20) printsiip
  - 80% intsidentidest on põhjustatud oma töötajate poolt
  - Teadmatus, oskamatus, tahtlik reeglite rikkumine
- Välimised
  - Küberkuritegevus

Küberkuritegevuse areng

- 20 sajand
  - Ülekaalus huvi ja „tahan teada“
- 21 sajand
  - Küberkuritegevus on muutunud äriks
- Alates 2002 võib rääkida organiseeritud küberkuritegevusest

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 = tulu - kulu
- 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

Infoturbe tegevused

Infoturve on informatsiooni kaitsmine:

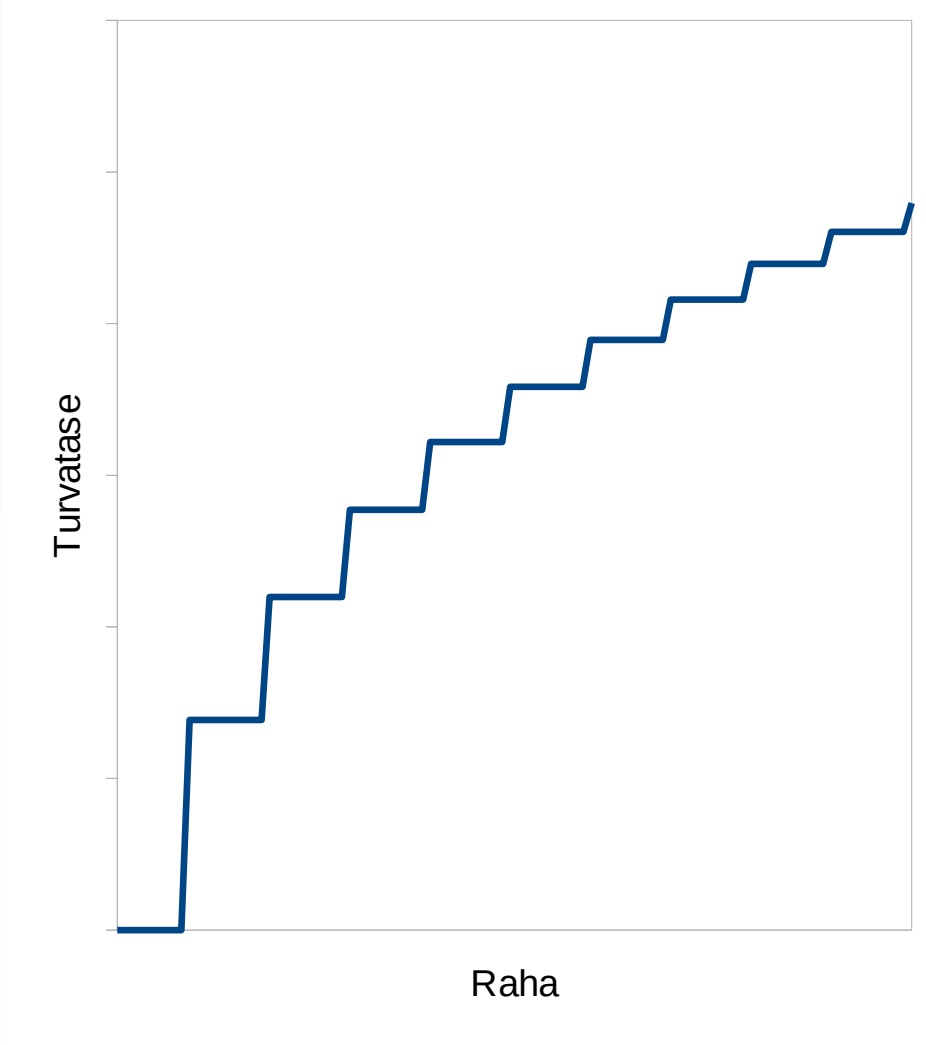
- Läbi turvameetmete rakendamise
- Mitmesuguste ohtude eest
- Majanduslikult mõttekalt/optimaalselt

Infoturbe rahaline külg

- Eelarve antakse äripoole poolt
- Turvalisus on privileeg – see maksab üsnagi palju
- Hea turvalisus on „nähtamatu“
- Probleem: kui näha ei ole, siis milleks seda vaja on?
- Eelarve on alati väiksem, kui vaja

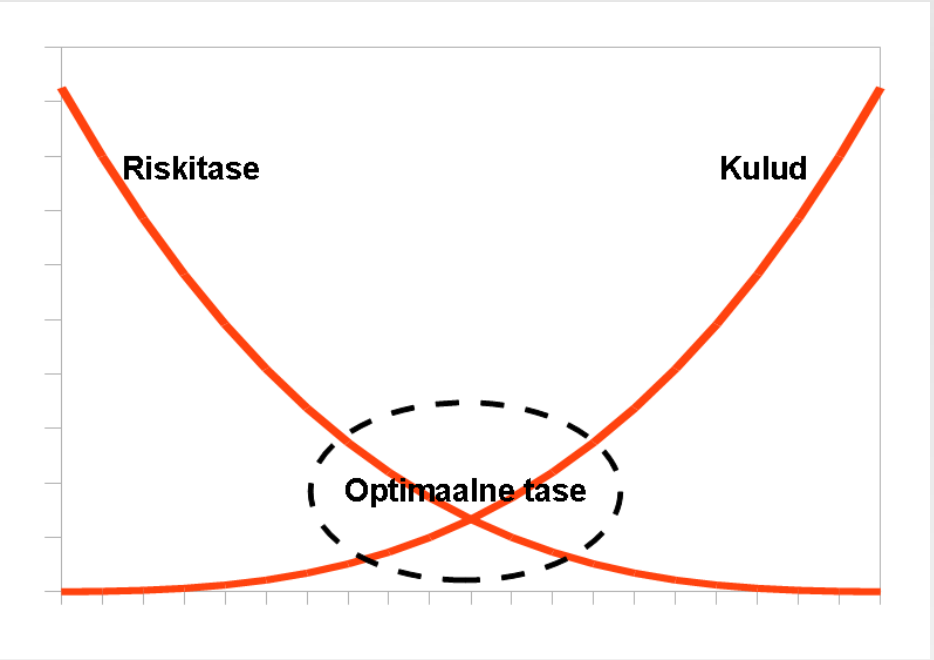
Turvameetmete hind

- Raha hulk ja turvatase on omavahel seotud logaritmiliselt
- Turvatase **ei kasva** proportsionaalselt raha hulga kasvades



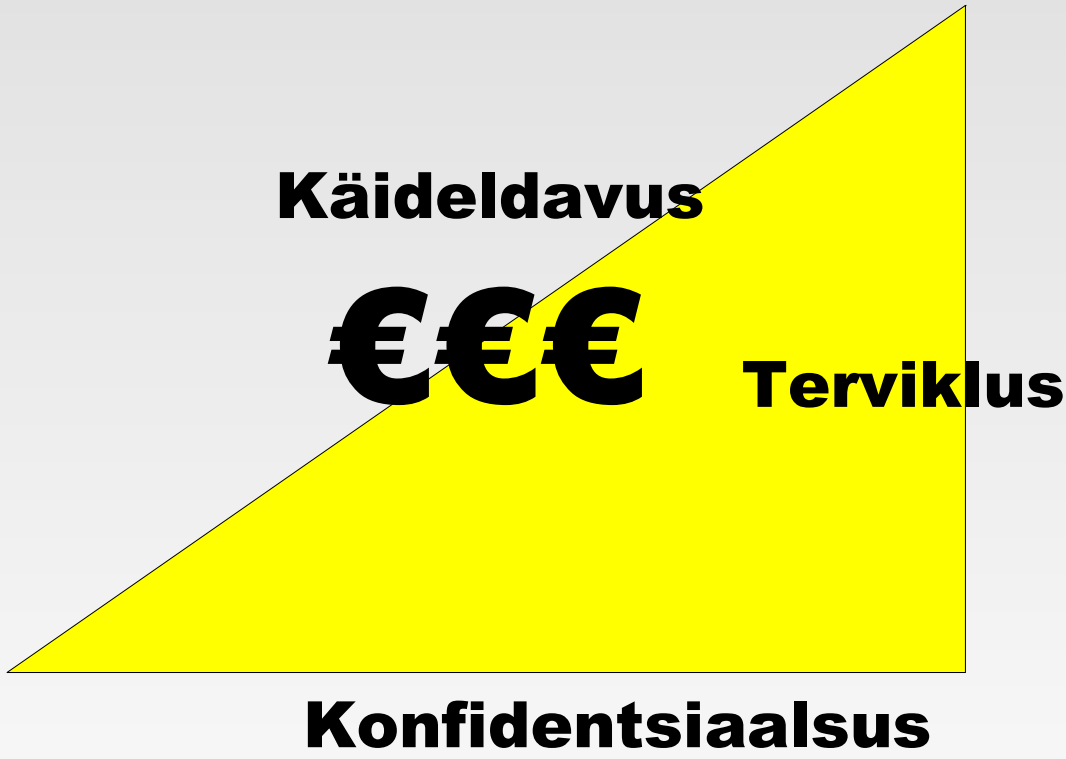
Turvameetmete optimum

- Riskitaseme lõpmatul vähendamisel kasvavad kulud lõpmatusse
- Päris 0-ks ei saa viia mitte ühtegi riski
- Arvestada tuleb ka seadustest tulenevaid nõudeid



Turvakomponentide rahaline seos

- Nõuded esitab äripool
  - Põhiprotsess
  - Õigusaktid
- Ressursid annab äripool
  - konstantse suuruse juures saab muuta küljepikkusi



Turvameetme hind vs. riskitaluvus

- Aktsepteeritava jääkriski suurus
  - Kas on mõttekas turvameetmeid lisada
- Turvameetmete hind versus tekkiva kahju suurus
  - Kas on mõttekas turvameetmeid lisada
- Juhtkonna otsus
  - Kas lisaks rahale on veel mõjutavaid tegureid (näiteks seadused, mainekahjud)

Jätkusuutlikuse perspektiiv

- Alla viie aastase perspektiiviga ei anna turvalisusesse panustamine efekti
  - „**elementaarsed meetmed**“ paika ja ülejäänu osas võib palvetada mõne sobiva jumala poole
- Süstemaatilise turvalisusega tegelemise ja/või turvajuhtimise mõju hakkab ilmnema alles peale kahte-kolme aastat
  - Mõtteviisi muutuseks vajalik aeg
- Süstemaatlise tegevuse peatamine annab tunda peale aastat

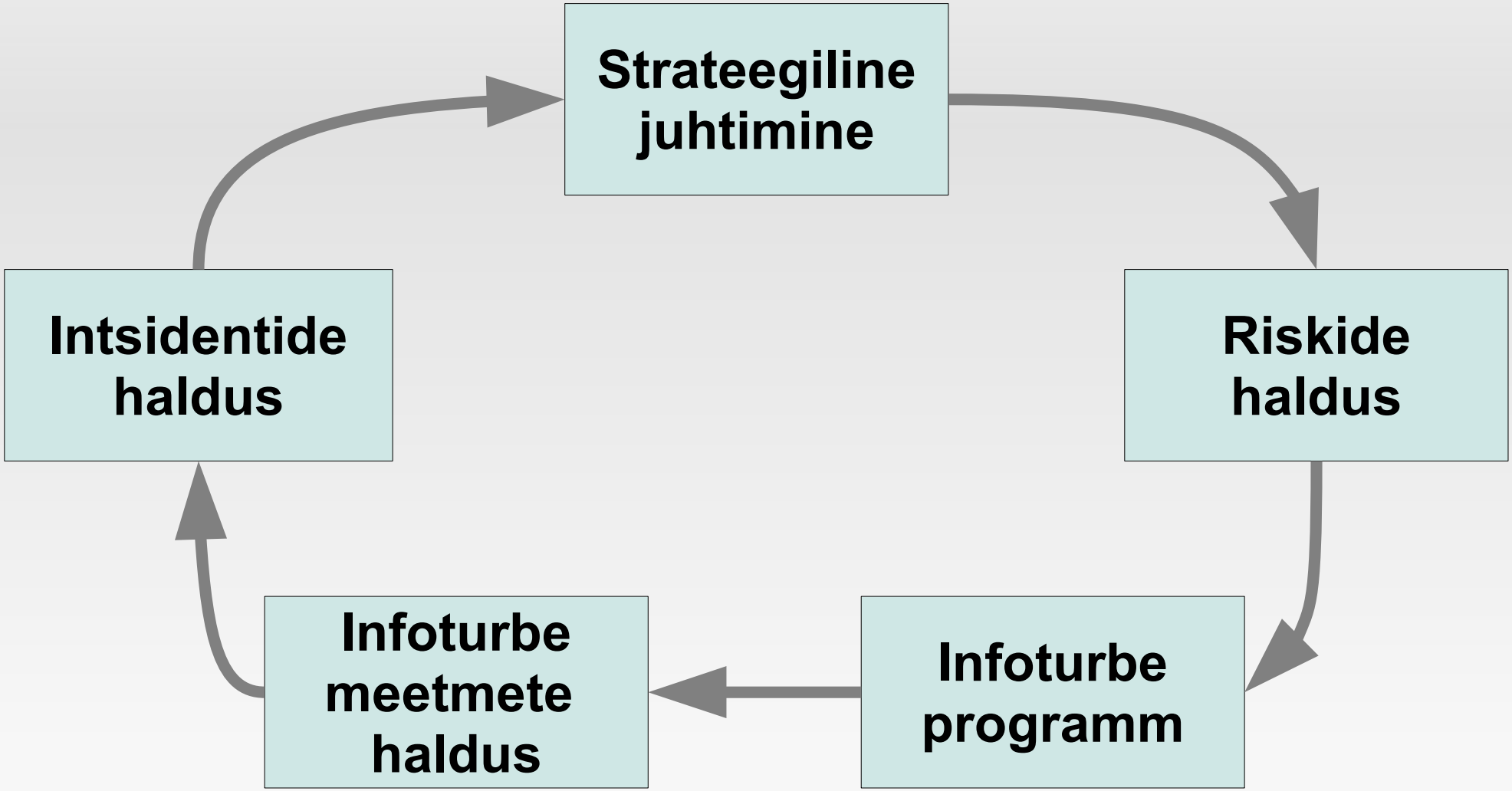
Infoturbe tegevused

Infoturve on informatsiooni kaitsmine:

- Läbi turvameetmete rakendamise
- Mitmesuguste ohtude eest
- Majanduslikult mõttekalt/optimaalselt

Infoturve, kui protsess

Infoturve, kui protsess

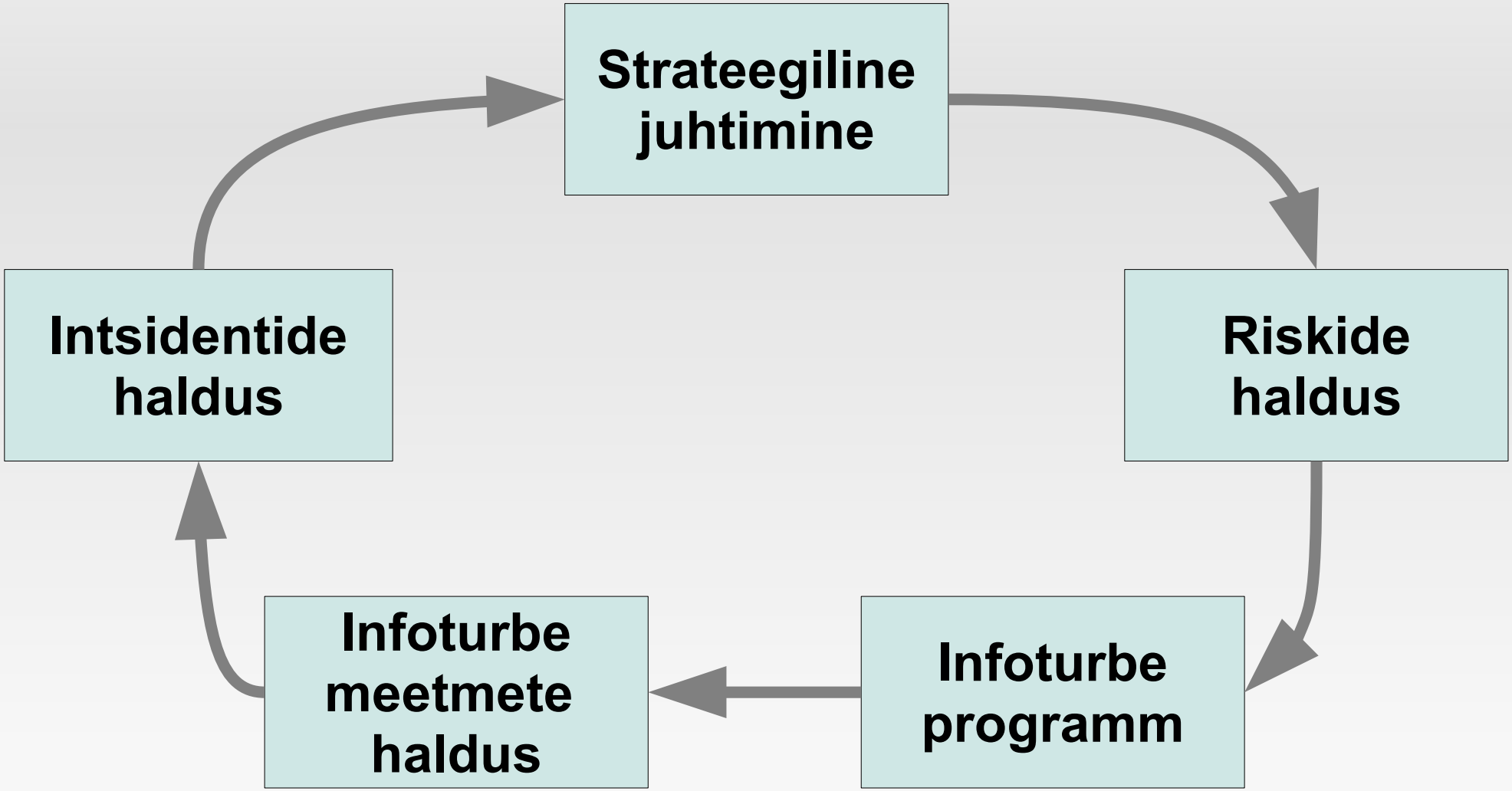


Infoturve, kui protsess

Strateegiline juhtimine

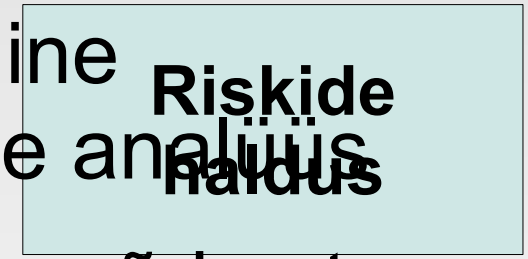
- Kehtestada ja juurutada raamistik, mis kindlustaks, et:
  - Infoturbestrateegiad oleksid kooskõlas ärivajadustega
  - Vastaksid kehtivale seadusandlusele
  - Vastaksid standarditele

Infoturve, kui protsess

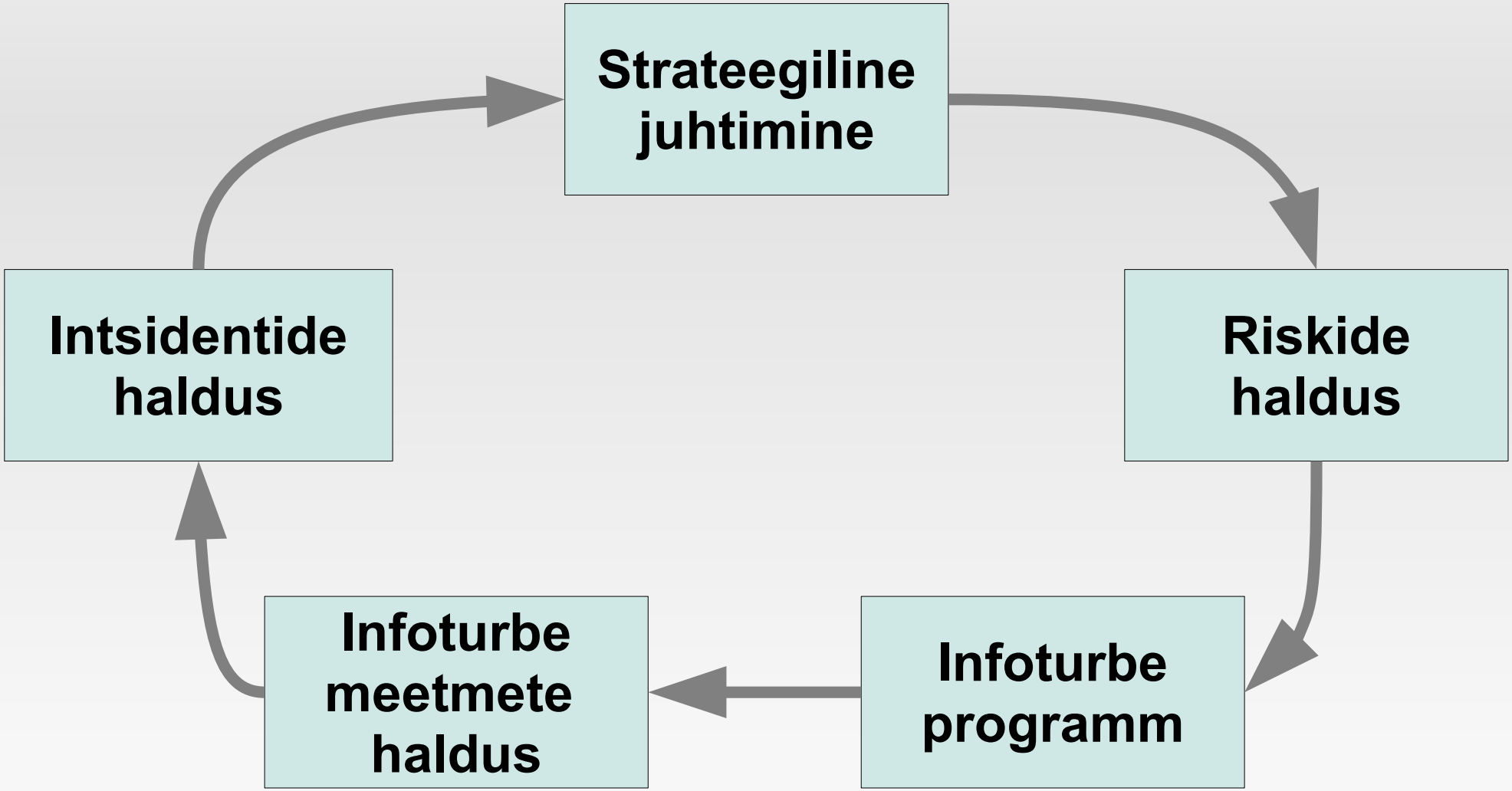


Infoturve, kui protsess

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



Infoturve, kui protsess

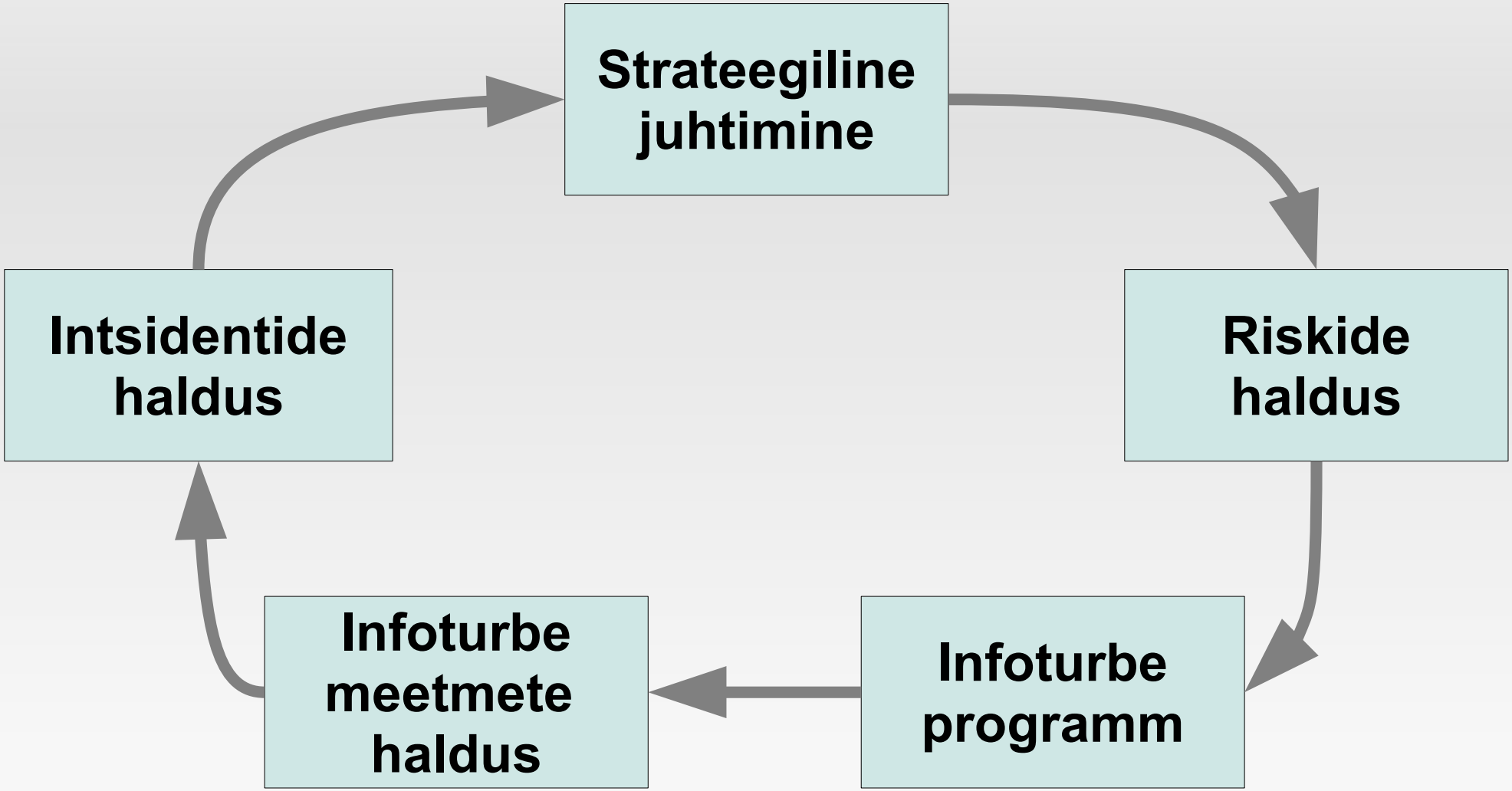


Infoturve, kui protsess

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

Infoturbe programm

Infoturve, kui protsess

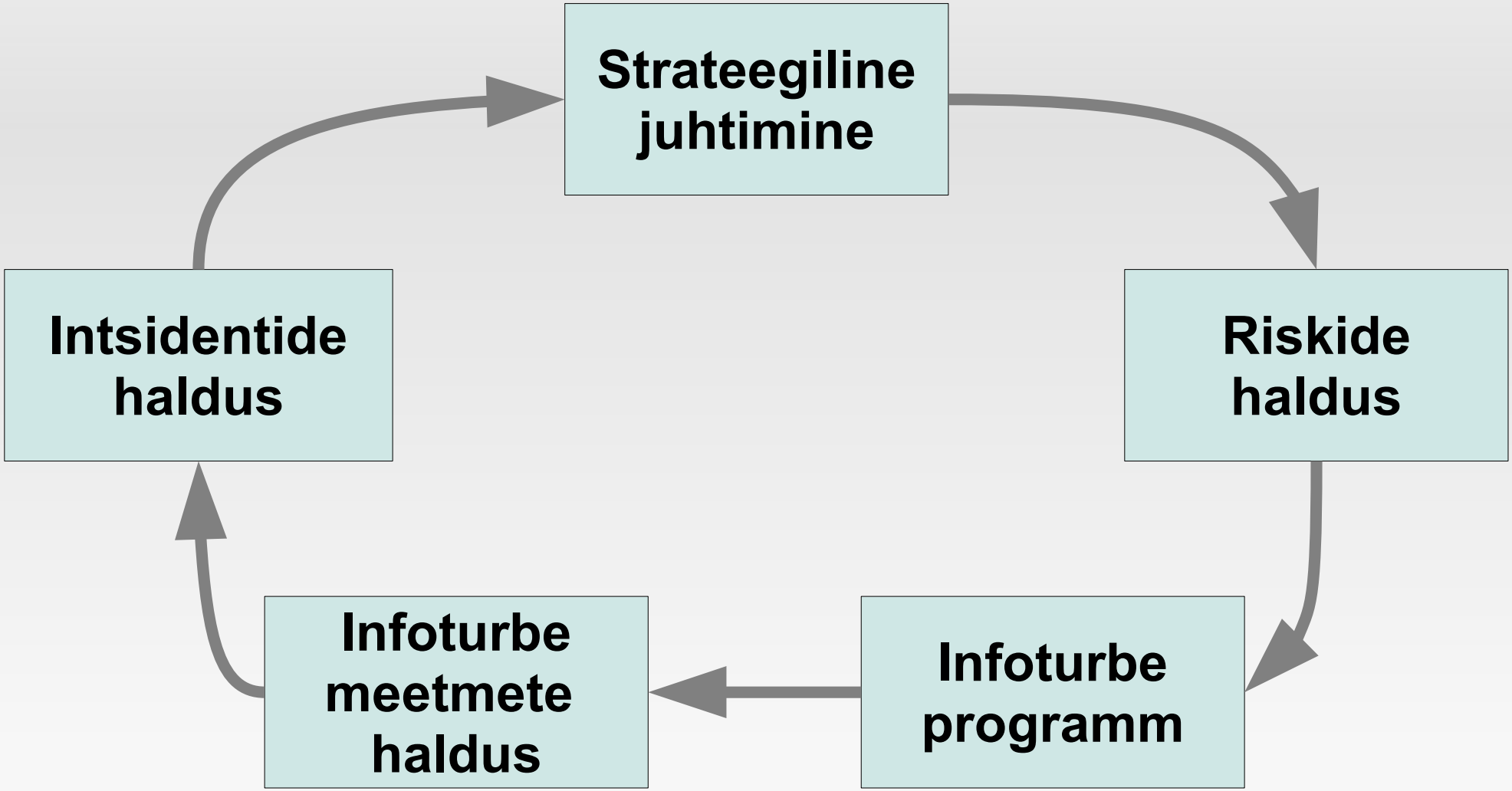


Infoturve, kui protsess

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

Infoturbe meetmete haldus

Infoturve, kui protsess

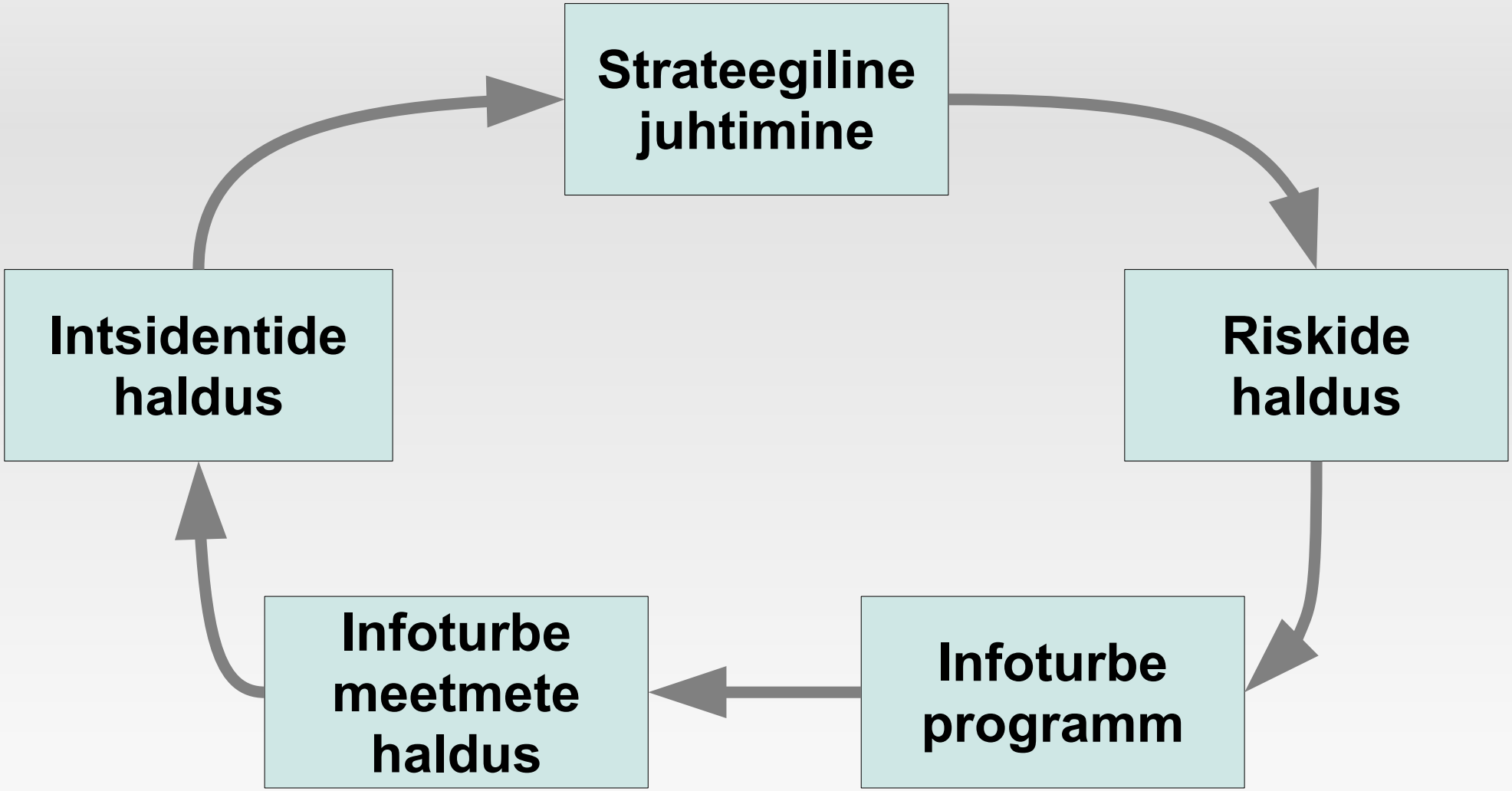


Infoturve, kui protsess

Intsidentide haldus

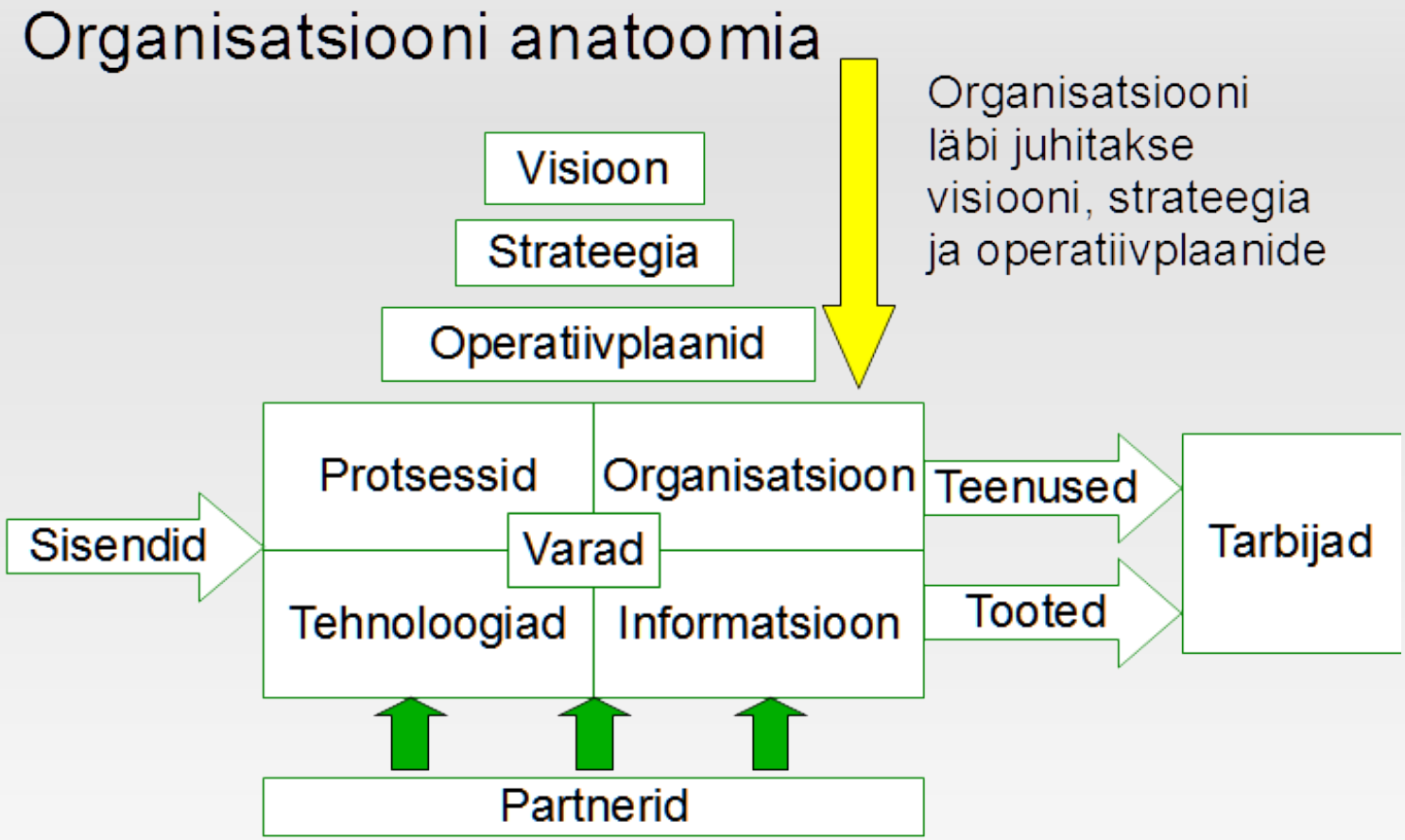
- Intsidentide avastamine, identifitseerimine, analüüs ja reageerimine
- Seiresüsteemid
- Forensic

Klassikaline infoturbe juhtimine



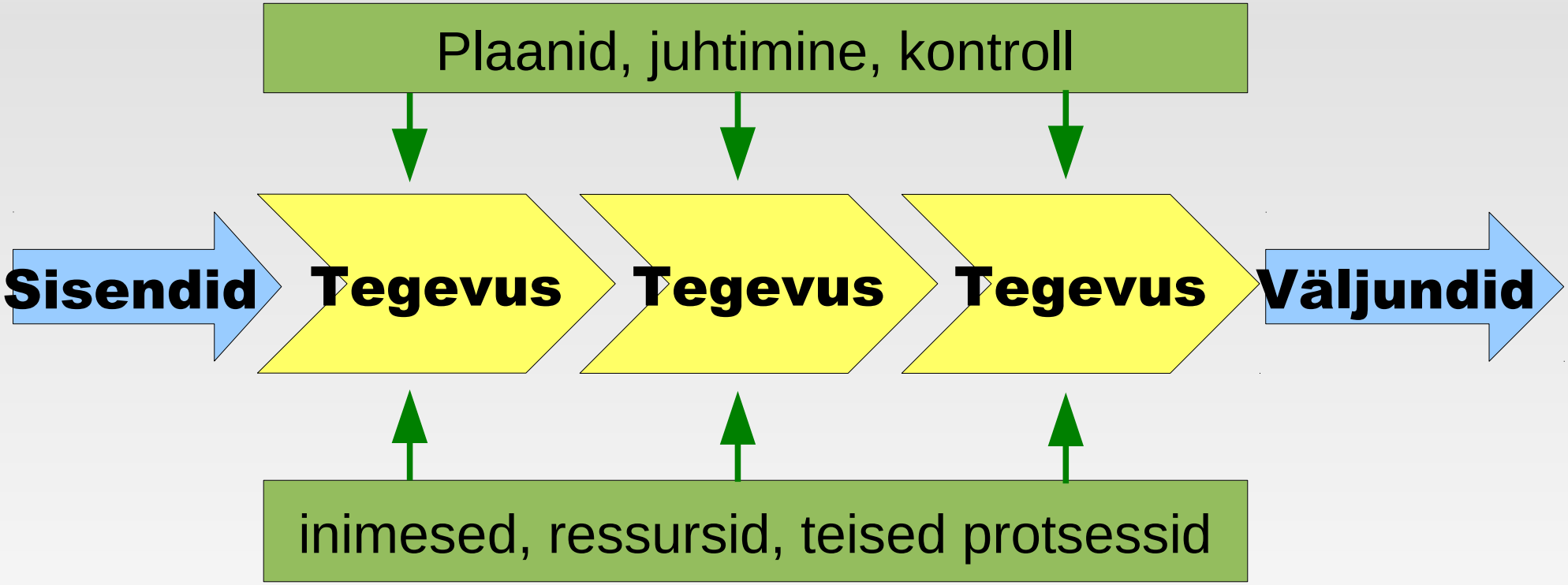
Informatsioon äriprotsessides

Organisatsiooni anatoomia



Tooted ja teenused tarnitakse tarbijale organisatsiooni ja tema partnerite pingutuse tulemusena

Protsessid


Plaanid, juhtimine, kontroll
Sisendid
Tegevus
Tegevus
Tegevus
Väljundid
inimesed, ressursid, teised protsessid

Protsessid

- Põhiprotsess
  - Tegevused ettevõtte või asutuse põhilise eesmärgi täitmiseks („raha teenimiseks“)
  - Põhiprotsessi nimetatakse ka „äriprotsess“ ning selles osalejaid „äripool“
  - Riigiametis on põhiprotsessiks mingi avaliku teenuse osutamine
- Tugiprotsessid
  - Tegevused põhiprotsessi toetuseks
  - **Infotehnoloogia on üldjuhul ressurss ja/või tugiprotsess**

Informatsioon äriprotsessides

- Äriprotsessi toetav funktsioon
  - Õiged otsused
  - Õiged meetodid
- Et saaks teha õigeid otsuseid, peab informatsioon olema kvaliteetne

Informatsioon protsessides

- Informatsiooni töötlemine võib olla vajalik põhieesmärgi täitmiseks
- Informatsioon on vajalik protsessi juhtimiseks

- **Kuna informatsioon on vajalik eelkõige äripoolele, siis on kõik sellega seonduvad projektid eelkõige äripoole projektid**

Infoturbe vajadus

- Andmete väärtuste ja omaduste tagamine protsessides kasutamiseks
- Käideldavuse, tervikluse ja konfidentsiaalsuse tagamine
- Sõltuvalt andmete tähendusest ja väärtusest, tuleneb ka infoturbe tähtsus.
- Andmete tähenduse ja väärtuse saab määrata ainult äripool (see kes andmeid kasutab)

Turvanõuete klassifikatsioon

Infoturbe põhimõisted

- **Käideldavus** (*availability*) –andmed on kättesaadavad **õigeaegselt** ja **mugavalt**.
- **Terviklus** (*integrity*) – andmed on õiged, täielikud ja pärinevad autentsest allikast.
- **Konfidentsiaalsus** (c*onfidentiality*) – andmed on kättesaadavad ainult volitatud isikutele ja kättesaamatud kõigile teistele.

Neid nimetatakse ka turvaklassideks

Nõuete tasemed

- Taseme määrab äripool
- Lihtsustamiseks jagada tasemeteks
  - Näiteks kolm või viis taset
- Konkreetsed tasemete piirid sõltuvad konkretsetest vajadustest

Käideldavuse tasemed

	Käideldavuse nõue	Seisak tundides	Kumulatiivne seisak aastas
1	99,99999%	0,000876	3 sekundit
2	99,9999%	0,00876	32 sekundit
3	99,999%	0,0876	Ligikaudu 5 minutit
4	99,99%	0,876	Ligikaudu 53 minutit
5	99,90%	8,76	Ligikaudu 9 tundi
6	99,00%	87,6	Ligikaudu 4 ööpäeva
7	98,00%	175,2	Ligikaudu 1 nädal
8	97,00%	262,8	Ligikaudu 11 ööpäeva
9	95,00%	438	Ligikaudu 18 ööpäeva
10	90,00%	876	36 ööpäeva

Käideldavuse kolm taset (näide ISKE-st)

- Tase 1 – suurem või võrdne 80% ja väiksem kui 99% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 24 tundi
- Tase 2 – suurem või võrdne kui 99% ja väiksem kui 99,9% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 4 tundi
- Tase 3 – suurem ja võrdne kui 99,9 % aastas ja maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal 1 tund kuni 0 sekundit

Tervikluse kolm taset (näide ISKE-st)

- Tase 1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse, ajakohasuse kontrollid erijuhtudel ja vastavalt vajadusele;
- Tase 2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalikud on perioodilised info õigsuse, täielikkuse ja ajakohasuse kontrollid;
- Tase 3 – infol allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

Konfidentsiaalsuse kolm taset (näide ISKE-st)

- Tase 1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
- Tase 2 – salajane info: info kasutamine lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral,
- Tase 3 – ülisalajane info: info kasutamine lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Riskihaldus

Riskihalduse loeng

NB! räägime IT riskide haldusest

- Riskihalduse eesmärgid
- Riskihalduse etapid
- Riskihalduse tulemid

Riskihalduse mõisted (allikad)

- AKIT – Andmekaitse ja infoturbe seletussõnastik http://akit.cyber.ee/
  - andmekaitse ja infoturbe väljatöötajad, korraldajad, järelevalvajad ja auditeerijad, süsteemi-, võrgu- ja turbeülematele või -administraatoritele
  - Hetkel on baasis üle 4000 märksõna (täieneb pidevalt)
- e-teatmik on ingliskeelsete info- ja sidetehnoloogia terminite seletav sõnaraamat tavalisele arvuti- ja telefonikasutajale http://vallaste.ee/

Riskihalduse mõisted

- **RISK** – mingit määramatut mõju omava sündmuse (**OHT**) toime esinemise tõenäosuse ja selle sündmuse tagajärje kombinatsioon (mõõdetav suurus)

Tagajärgedeks on

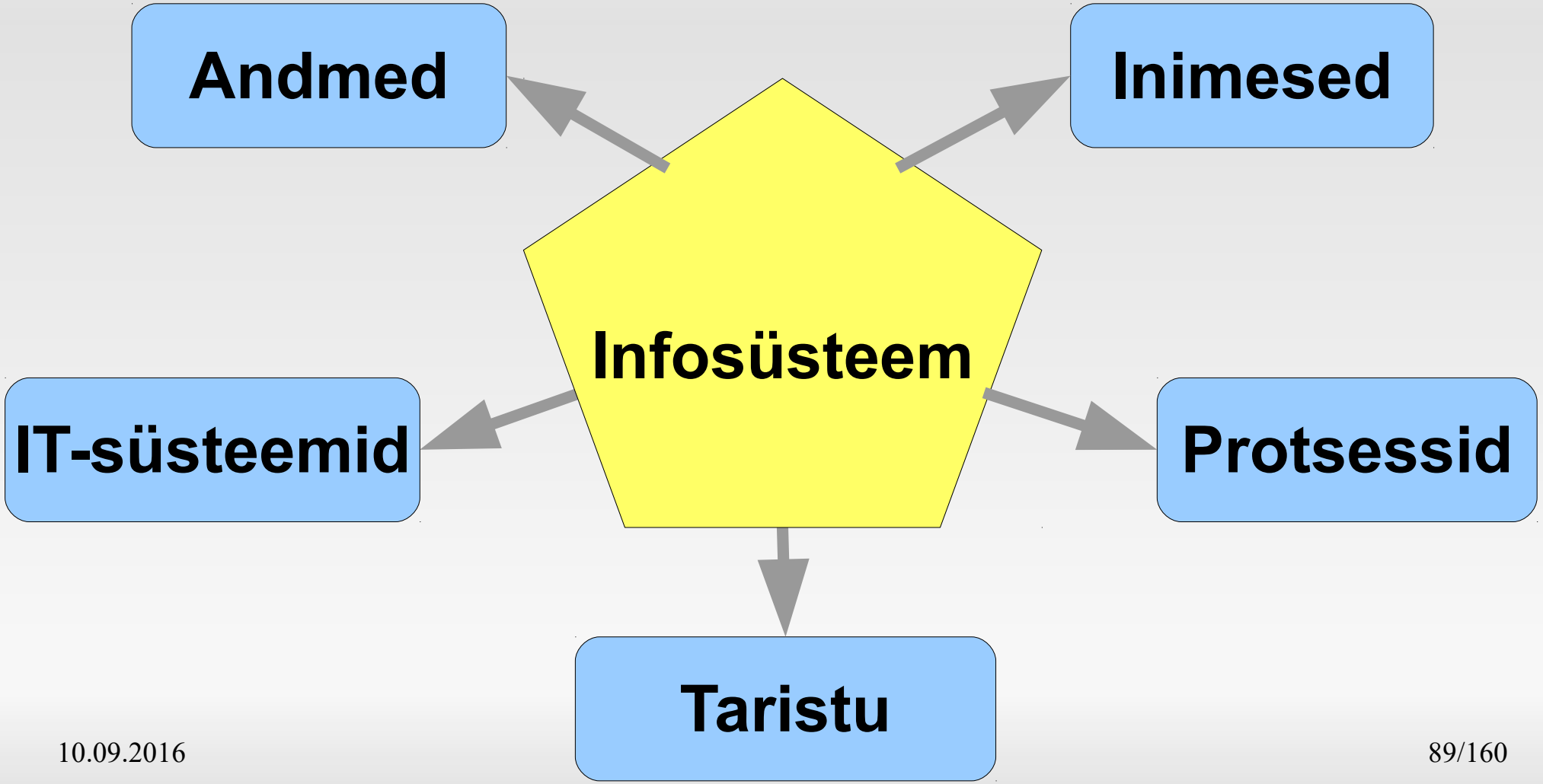
- Otsene kahju
- Põhitegevuse protsesside katkestus
- Taastamisele kuluv ressurss (aeg=raha)
- Kaudsed kahjud (maine...)

Riskihalduse mõisted

- **Infovara** - teadmus või andmed, millel on organisatsiooni jaoks väärtus, või nendega seotud infotöötlusvahend
- **Nõrkus** – vara nõrk koht, turvaauk, mida võib kasutada tagajärjega sündmuseks (oht realiseerub)

Riskihalduse mõisted

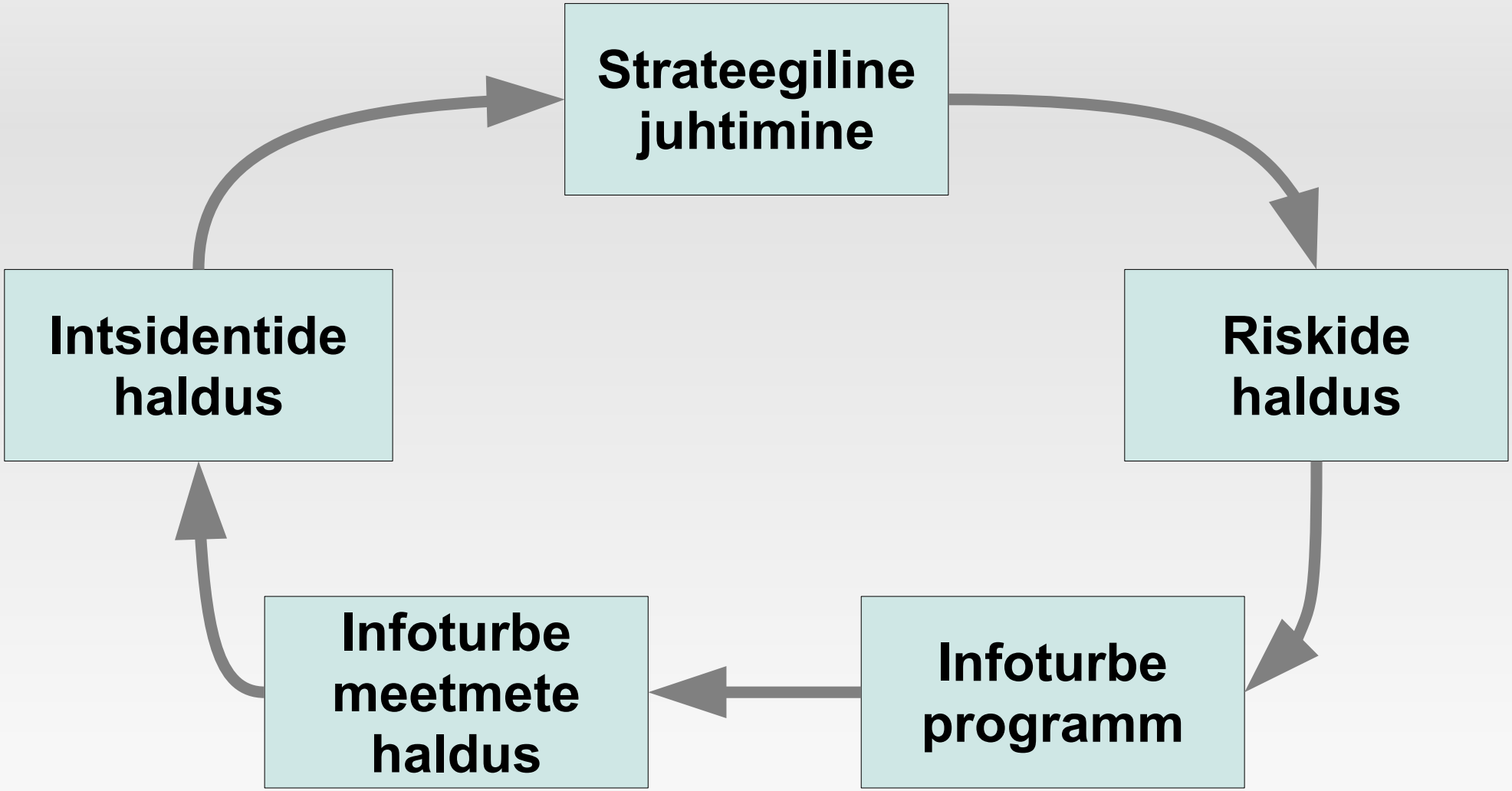
Infosüsteemi osad



Metoodikad

- Erinevaid metoodikaid on palju
  - ISO 27005 / COBIT
  - NIST
  - …
- Üldine metoodika ISO 31000
- Eestis on ainuke kohustuslik Hädaolukorra seaduses antud riskihindamise metoodika
- Käesoleva loengu raames järgime ISO27005 põhimõtteid

Klassikaline infoturbe juhtimine

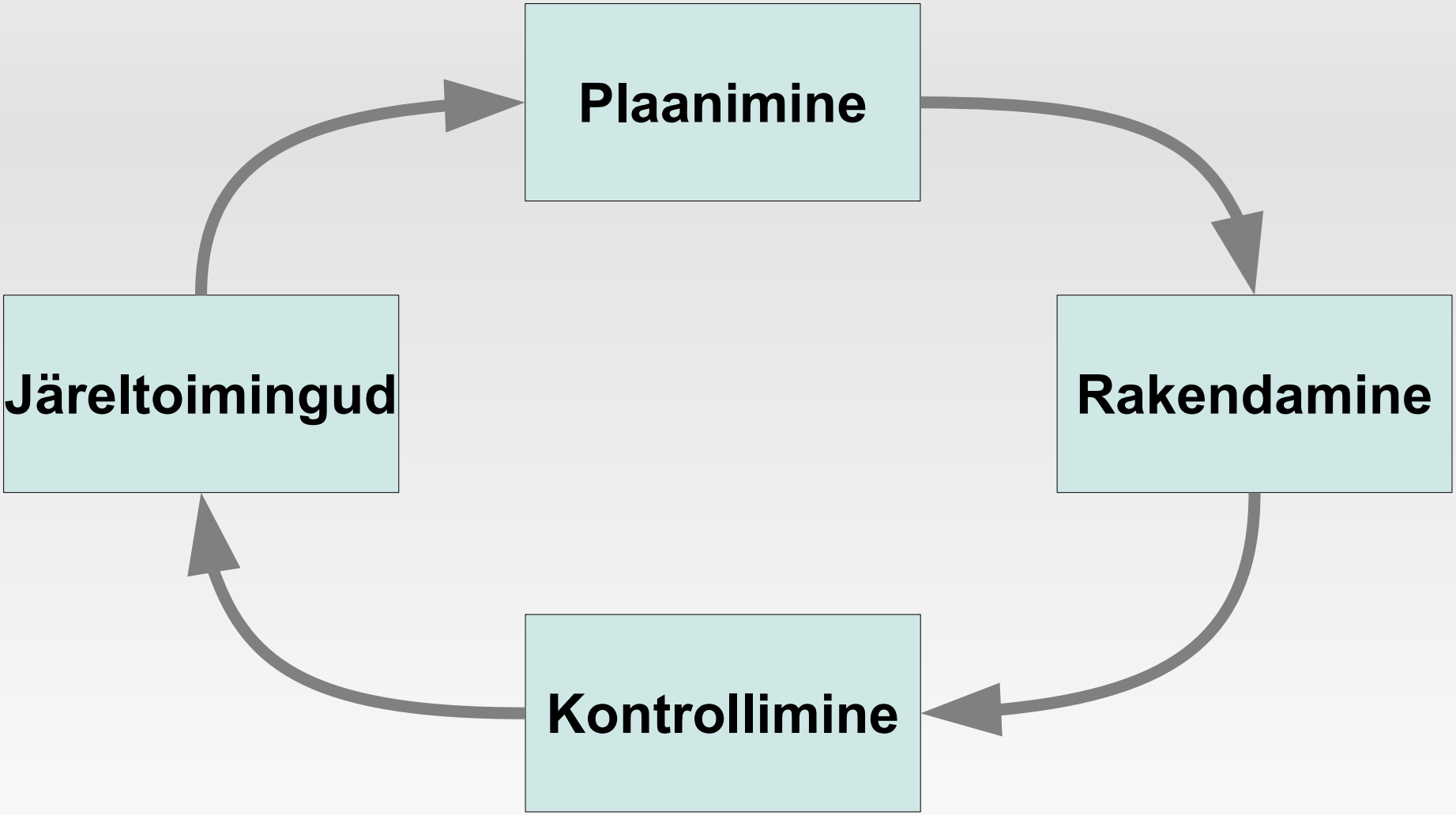


Klassikaline infoturbe juhtimine

- Plaanimine
- Rakendamine
- Kontrollimine
- Järeltoiminguid

Riskide haldus

Riskihalduse sammud

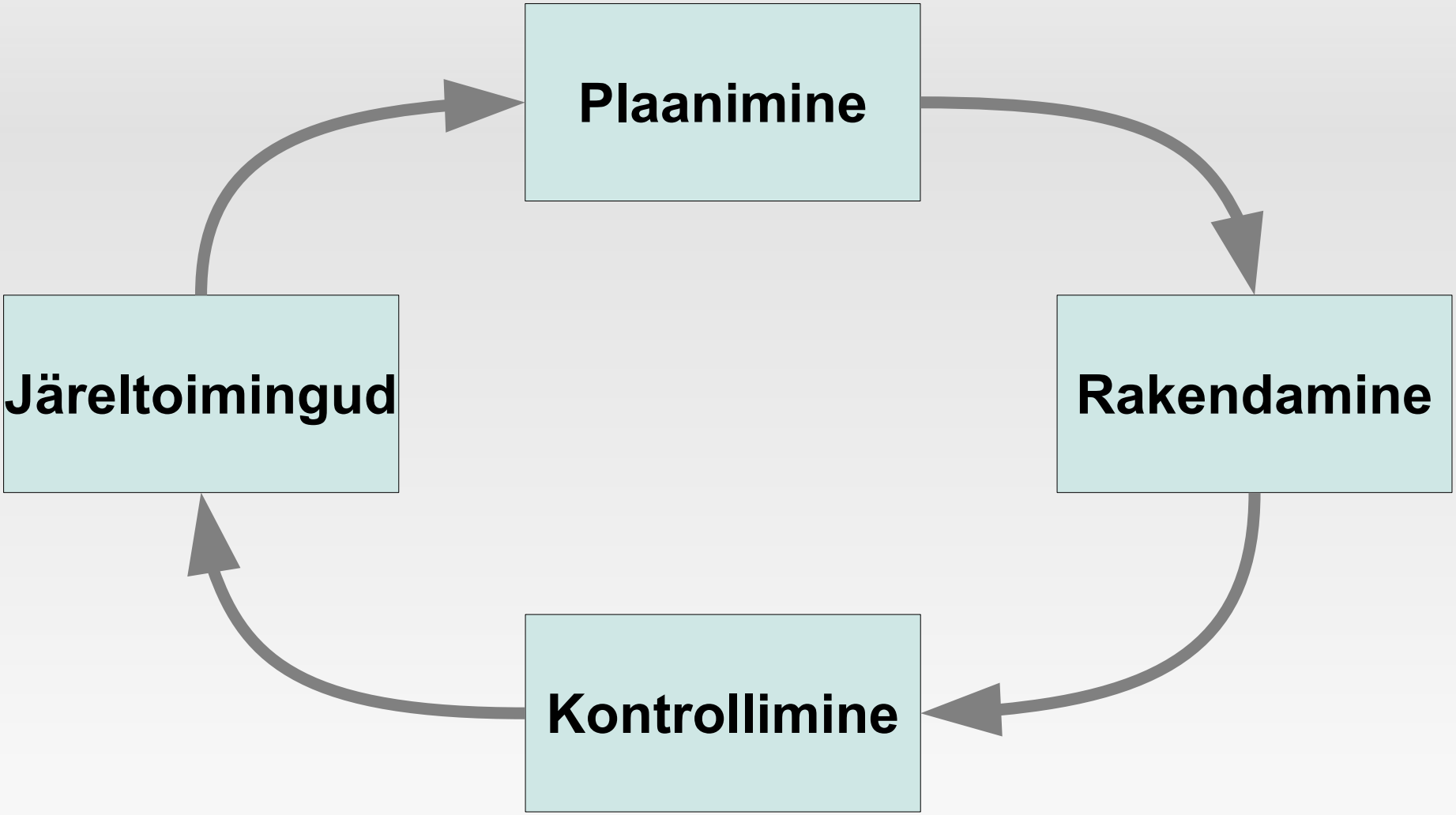


Riskihalduse sammud

Plaanimine

- Konteksti loomine
- Riski kaalutlemine
- Riskikäsitlusplaani koostamine
- Riski aktsepteerimine

Riskihalduse sammud

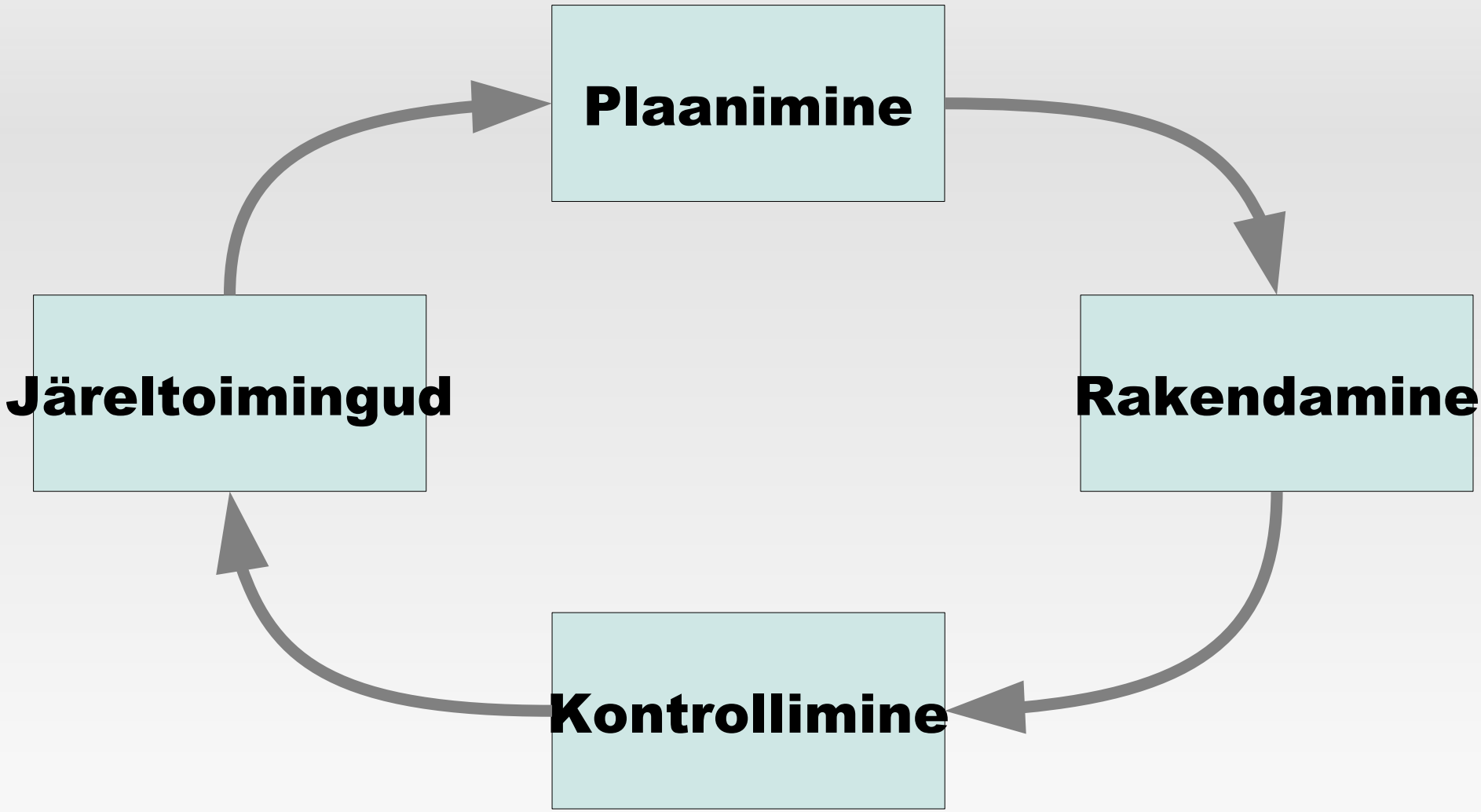


Riskihalduse sammud

- Riskikäsitlusplaani ellu viimine
- Infoturbe juhtimise skeemil
  - infoturbe programm
  - infoturbe meetmed

Rakendamine

Riskihalduse sammud

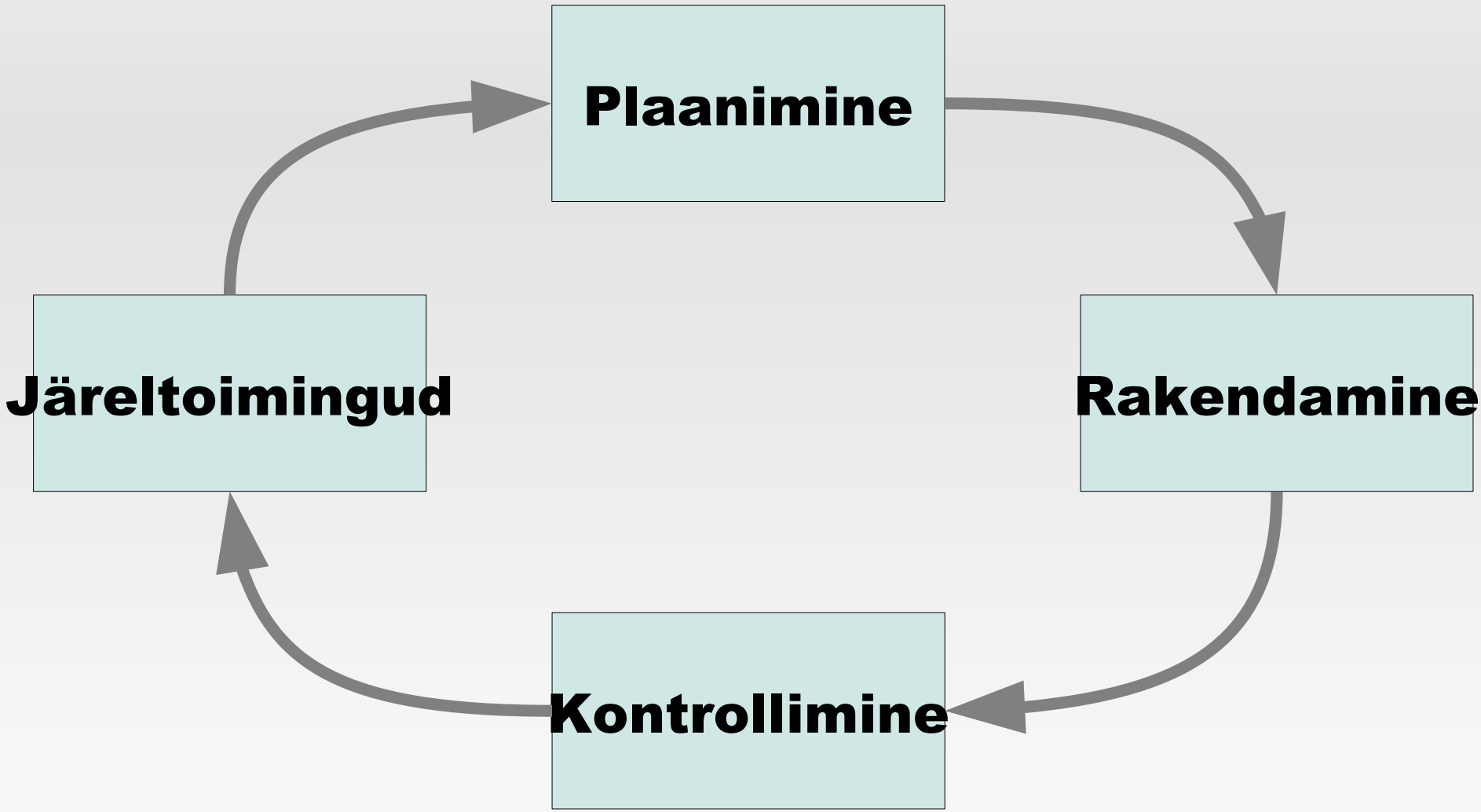


Riskihalduse sammud

- Riskide pidev seire ja läbivaatus
- Sisaldab ka infoturbejuhtimise intsidendihaldust

Kontrollimine

Riskihalduse sammud

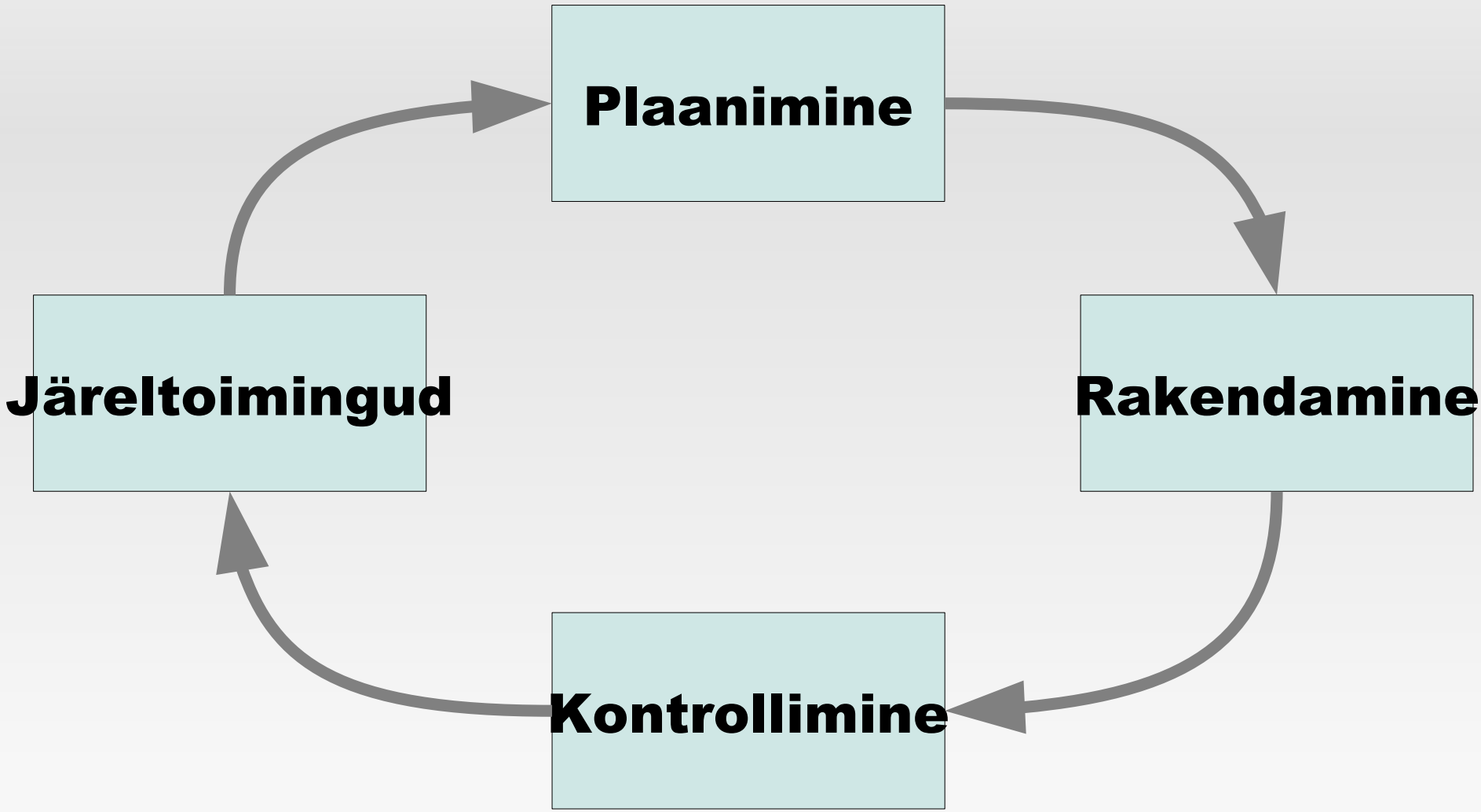


Riskihalduse sammud

Järeltoimingud

- Infoturvariski halduse protsessi käigushoid ja täiustamine
- Infoturbejuhtimise haldussüsteem

Riskihalduse sammud



Riskihalduse sammud

Plaanimine

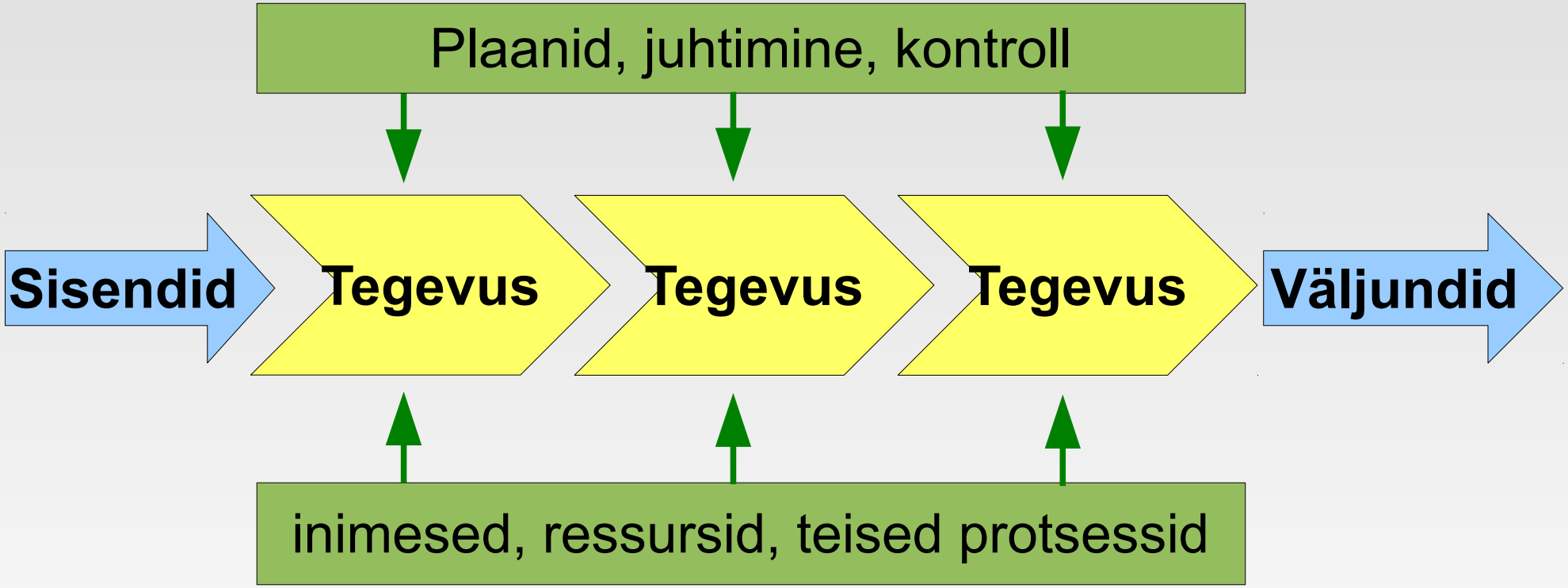
- **Konteksti loomine**
- Riski kaalutlemine
- Riskikäsitlusplaani koostamine
- Riski aktsepteerimine

Konteksti loomine

Riskihalduse käsitlusala

- Nõuded (regulatsioonid, ärinõuded jne)
- Põhiprotsessi(de) kaardistamine – kriitilised tegevused (eesmärk ja seos protsessi tulemusega)
- Kriitiliste tegevuste ressursid (millised inimesed, seadmed, vahendid ja teised protsessid on seotud ning kuidas)
- Sõltuvused naabritest ja partneritest

Protsessi mudel

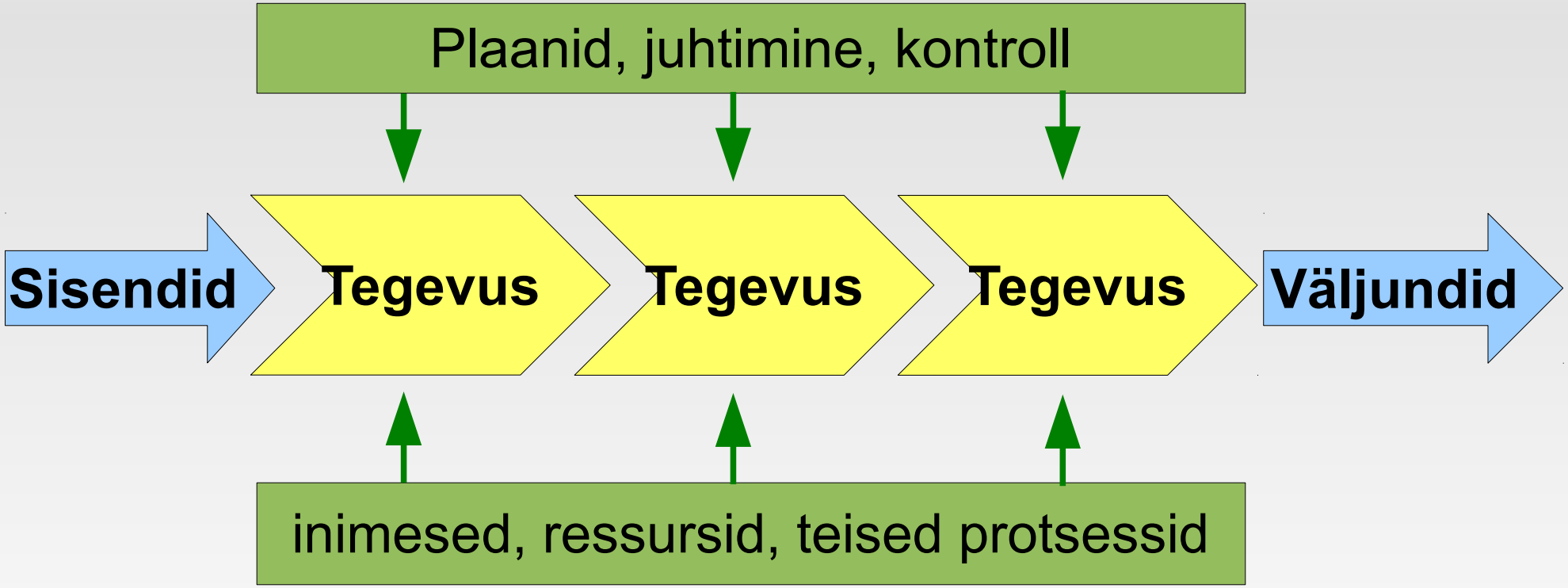


Nõuded põhiprotsessile

Plaanid, juhtimine, kontroll

- Regulatsioonid – õigusaktidest tulenevad nõuded
  - ETO-d
  - Delikaatsete isikuandmete töötlemine
- Ärinõuded – kaua protsess võib olla katkenud
  - Lepingud
  - ...

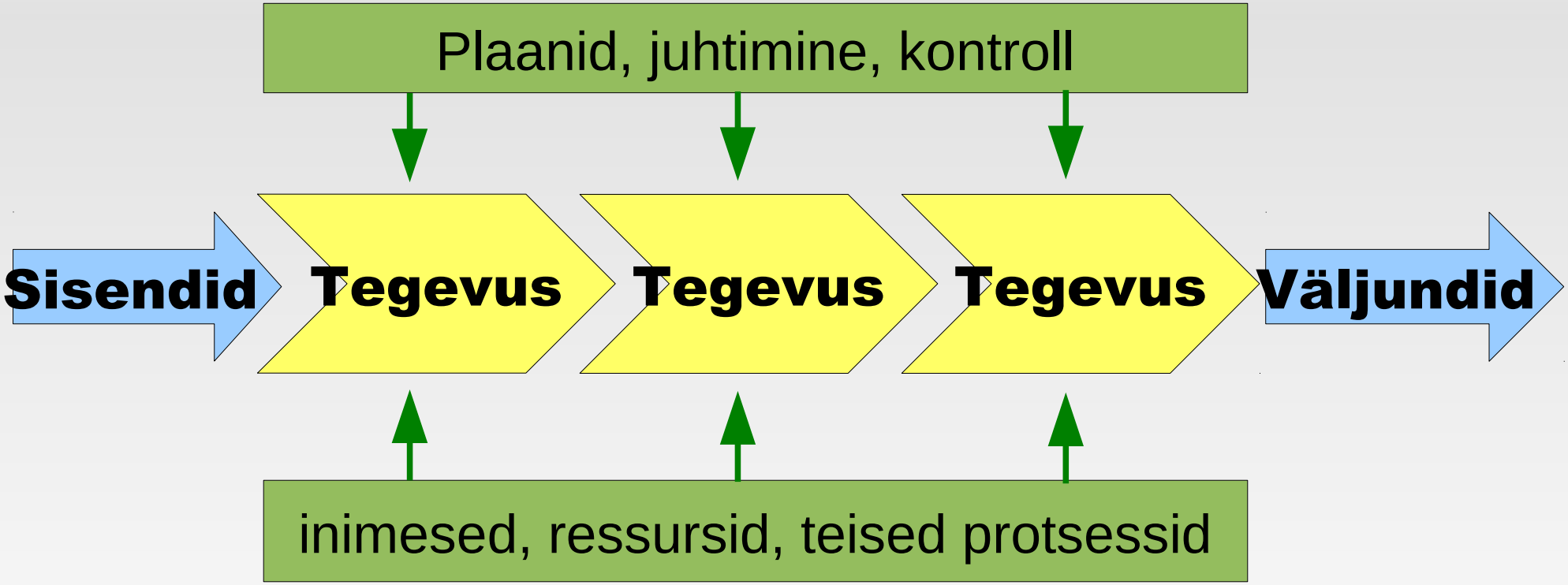
Protsessi mudel



Põhiprotsessi kaardistamine

- Protsessi tegevused
- Milline on tegevuste eesmärk
- Milline on seos protsessi tulemusega
- Millised on (aja)kriitilised

Protsessi mudel



Kriitiliste tegevuste ressursid

- Millised inimesed on seotud
- Millised (IT) seadmed on seotud
- Millised vahendid on seotud
- Millised teised protsessid on seotud
- Kuidas?
  - kui kriitiline see seos on
  - kas ressurss on asendatav

inimesed, ressursid, teised protsessid

Konteksti loomine

Riskihalduse käsitlusala

- Nõuded (regulatsioonid, ärinõuded jne)
- Põhiprotsessi(de) kaardistamine – kriitilised tegevused (eesmärk ja seos protsessi tulemusega)
- Kriitiliste tegevuste ressursid (millised inimesed, seadmed, vahendid ja teised protsessid on seotud ning kuidas)
- Sõltuvused naabritest ja partneritest

Konteksti loomine

Riskihalduse kriteeriumid

- Sündmuse toime kriteeriumite piiritlemine
  - Skaala mõjude suurustega (kahju asutusele v inimesele)
- Riski hindamise kriteeriumid
  - Prioritiseerimine varade kaupa (väärtus asutusele, tähtsus põhiprotsessile v. mainele jne)
- Riski aktsepteerimise kriteeriumid
  - Skaala – tõenäosuse ja kahju korrutis, nt millal on kahju piisavalt väike, et edasi mitte tegutseda

Sündmuse toime

- Kokkulepped riskihindamise tellijaga
- Mõjuulatuse skaala
  - Astmete arv
  - Astmete piirid
- Esinemiste tõenäosuse skaala (sündmuste hulk ajaühikus)
  - Astmete arv
  - Astmete piirid

Mõju ulatus (näide 1)

	Mõju suhtena aasta eelarvesse	Eeldame, et aasta eelarve on 10 miljonit	
1	Olematu	100	(0,1%)
2	Väike	10 000	(1%)
3	Keskmine	1 000 000	(10%)
4	Suur	10 000 000	(100%)
5	Väga suur (Katastroofiline)	100 000 000	(1000%)

Mõju ulatus (näide 2)

	Inimkahjud	
1	Olematu	Kvalifitseeritud arstiabi pole vaja
2	Väike	Haavad, luumurrud
3	Keskmine	Rasked vigastused
4	Suur	Inimohvrid
5	Väga suur (Katastroofiline)	Mitmed (kümned-sajad) inimohvrid

Esinemise tõenäosus (näide)

Aluseks võiks olla ajaühik

Tase	Sagedus	Oht
5	1 x päevas	100,00 %
4	1 x kuus	3,284 %
3	1 x aastas	0,274 %
2	1 x 10 aastas	0,027 %
1	1 x sajandis	0,003 %

Kombinatsioonide matemaatika

- Kui meil on kümme ohtu millest igaüks võib mõjuda kolmel erineval moel, siis

$$C_{10}^{3} = \frac{10!}{3!\cdot(10-3)!} = \frac{10!}{3!\cdot 7!} = 120$$

- Numbrid lähevad väga kiiresti väga suureks
- Haldus muutub võimatuks

Et mahud ei läheks väga suureks, tuleb kategoriseerida

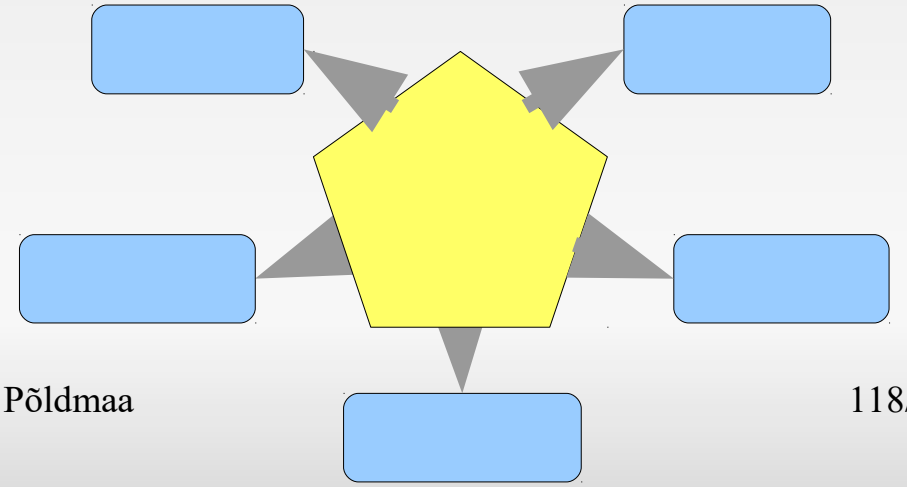
Varade klassifitseerimine

- Varade identifitseerimine
  - Klasside tasemel
- Kindlaks teha, kes on vara „omanik“
  - Saab hiljem riski omanikuks
- Varade väärtustamine
  - Prioriteet põhiprotsessis

Varade kategoriseerimine

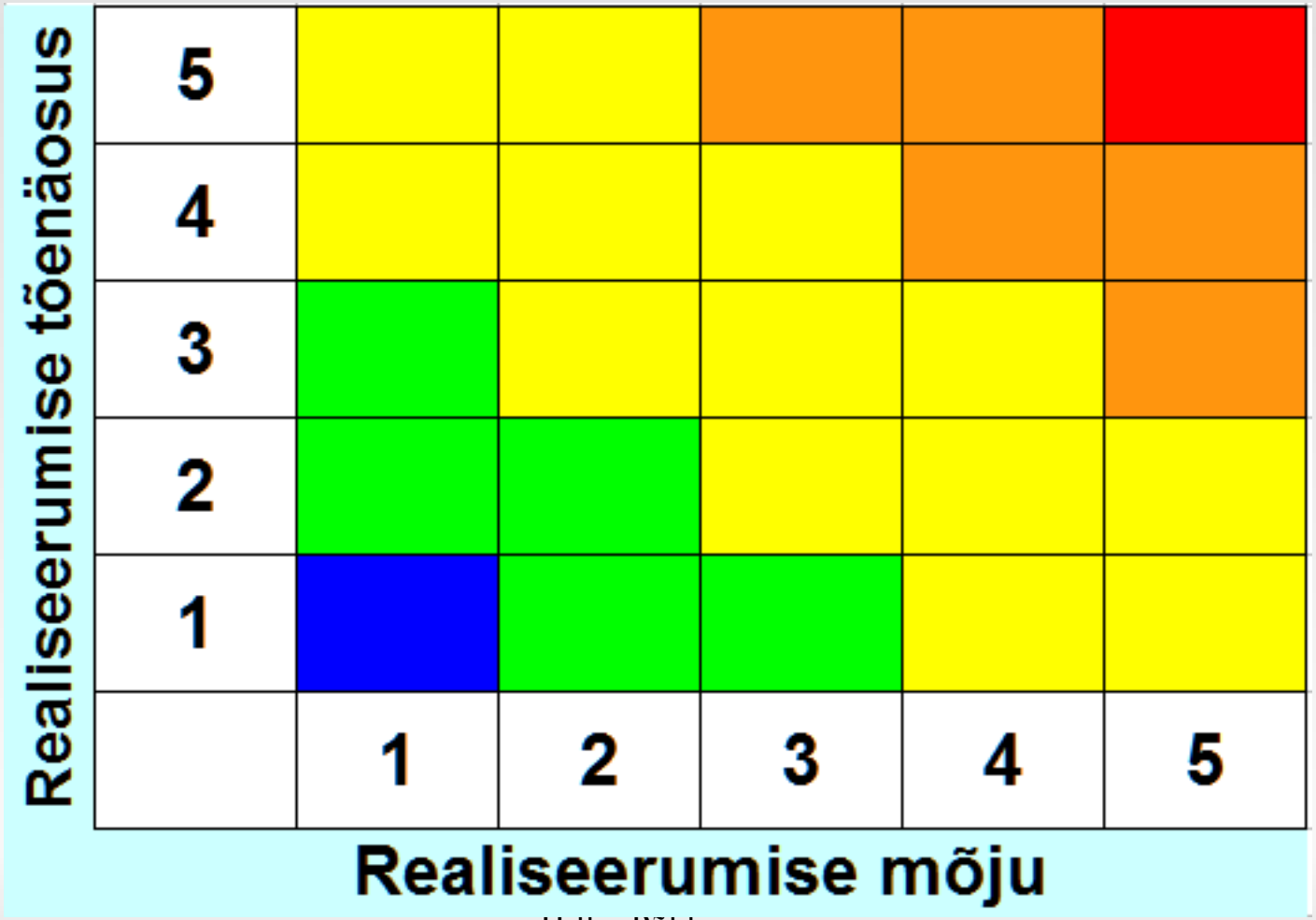
Varade kategooriad

- Protsessid, organisatsioon
- Inimesed ja oskused
- Taristu (füüsilised ruumid, elekter jne)
- IT süsteemid (riist- ja tarkvara)
- Andmed



Riskimaatriks

Prioritiseerimiseks ja aktsepteerimiseks



Praktiline ülesanne 1

Konteksti loomine

- Valida üks põhiprotsess (käsitlusala)
- Kaardistada põhiprotsessiga seonduvad infovarad
- Määratleda riskihalduse kriteeriumid
  - Sündmuse toime = Mõjude skaala
- Määratleda riski hindamise kriteeriumid
  - Varade klassid ja nende prioriteedid
- Riski aktsepteerimise kriteeriumid
  - Skaala, millal on kahju piisavalt väike, et edasi mitte tegutseda

Riskihalduse sammud

Plaanimine

- Konteksti loomine
- **Riski kaalutlemine**
- Riskikäsitlusplaani koostamine
- Riski aktsepteerimine

Kombinatsioonide matemaatika

- Kui meil on kümme ohtu millest igaüks võib mõjuda kolmel erineval moel, siis

$$C_{10}^{3} = \frac{10!}{3!\cdot(10-3)!} = \frac{10!}{3!\cdot 7!} = 120$$

- Numbrid lähevad väga kiiresti väga suureks
- Haldus muutub võimatuks

Et mahud ei läheks väga suureks, tuleb kategoriseerida

Ohtude kategoriseerimine

- Vääramatu jõud
- Organisatsioonilised puudused
- Inimvead
- Tehnilised rikked ja defektid
- Ründed

ISKE ohtude kataloog
https://www.ria.ee/public/ISKE/ISKE_ohtude_kataloog_ver_7.pdf

Nõrkuste tuvastamine

Ohule vastav nõrkus

- Kas me kasutame vara, millele oht mõjub
  - Näide: Windowsile mõjuvad ohud ei mõju Unixis
- Kas konkreetsel varal on konkreetne turvaauk
  - Näide: tarkvara on paigatud

Riski kriteeriumid

Riski olulisuse hindamise võrdlusalused

Esinemise tõenäosus

- Väga väike (olematu)
- Väike (ebatõenäoline)
- Keskmine
- Suur
- Väga suur

Mõju ulatus

- Olematu
- Väike
- Keskmine
- Suur
- Väga suur (Katastroofiline)

Esinemise tõenäosus (näide)

Konteksti loomisel kokku lepitud skaala

Tase	Sagedus	Oht
5	1 x päevas	100,00 %
4	1 x kuus	3,284 %
3	1 x aastas	0,274 %
2	1 x 10 aastas	0,027 %
1	1 x sajandis	0,003 %

Mõju ulatus (näide 1)

Konteksti loomisel kokku lepitud skaala

	Mõju suhtena aasta eelarvesse	Eeldame, et aasta eelarve on 10 miljonit
1	Olematu	100 (0,1%)
2	Väike	10 000 (1%)
3	Keskmine	1 000 000 (10%)
4	Suur	10 000 000 (100%)
5	Väga suur (Katastroofiline)	100 000 000 (1000%)

Mõju ulatus (näide 2)

Konteksti loomisel kokku lepitud skaala

	Inimkahjud	
1	Olematu	Kvalifitseeritud arstiabi ei vajata
2	Väike	Haavad, luumurrud
3	Keskmine	Rasked vigastused
4	Suur	Inimohvrid
5	Väga suur (Katastroofiline)	Mitmed (kümned-sajad) inimohvrid

Riski kaalutlemine

Riski tuvastamine (2/2)

- Ohtude tuvastamine
- Olemasolevate turvameetmete väljaselgitamine
- Nõrkuste tuvastamine
- Võimalike tagajärgede tuvastamine
  - Intsidendi stsenaariumid ja realiseerumise tagajärjed

Ohud ja riskistsenaariumid

- Ohukataloogid
  - ISO 27005 (tasuline, saadaval standardikeskusest)
  - ISKE/BSI https://www.ria.ee/public/ISKE/ISKE_ohtude_kataloog_ver_7.pdf
  - COBIT (tasuline, saadaval ISACA veebis)
  - NIST http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter4.html
- Kogemus
  - Üldised kogemused
  - Eelnevad intsidendid
- Juhtkonna jutule pole mõtet minna jutuga - „siin on oht“
- Tuleb näidata ohu realiseerumise stsenaarium ja tagajärjed

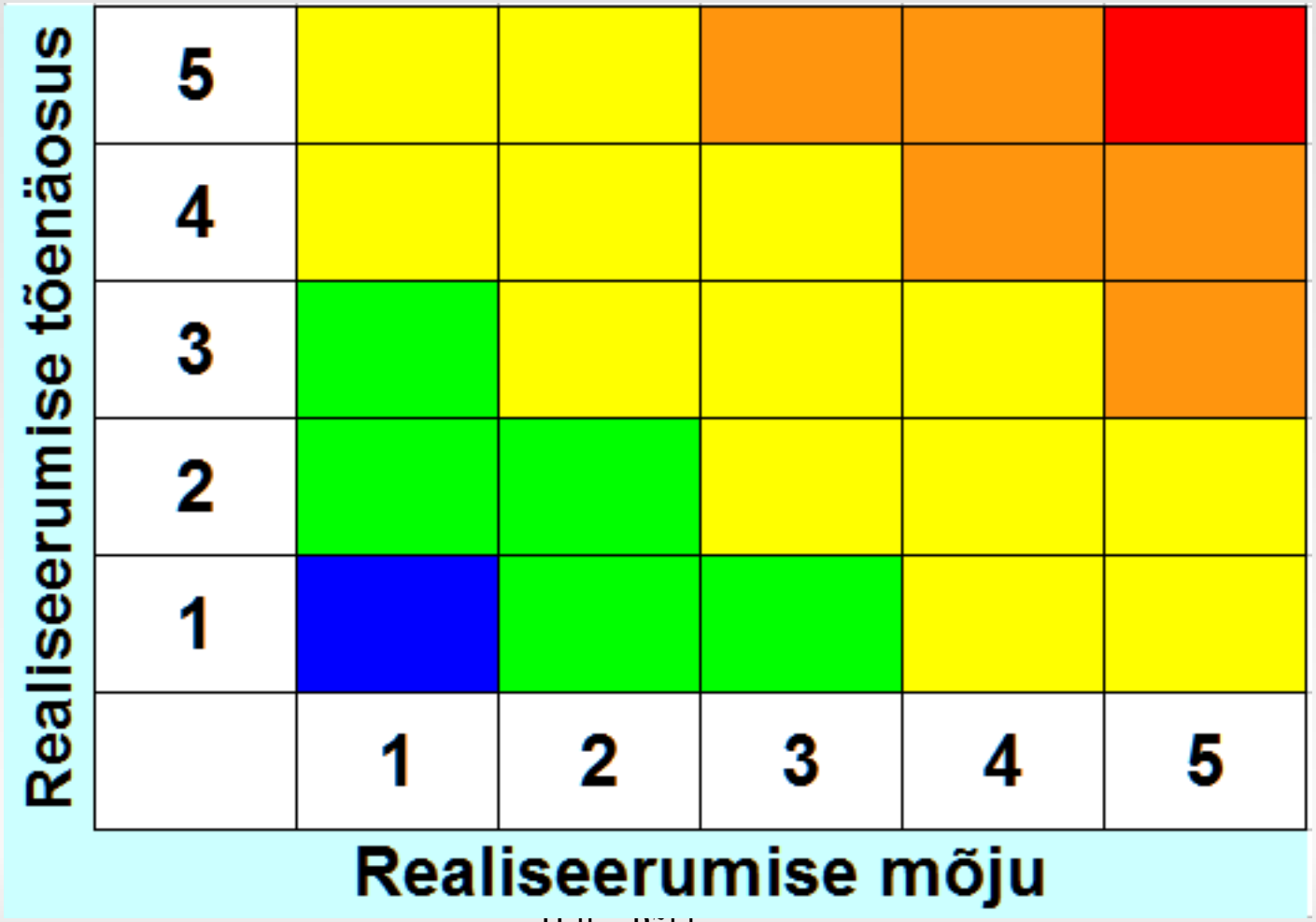
Riskianalüüs ja riskihindamine

Riskistenaarium

- Vara väärtus protsessis
- Kuidas on võimalik, et üks või teine oht realiseerub
- Ohu realiseerumise tõenäosus
- Millised on tagajärjed
- Võimaliku mõju väärtused

Riskimaatriks

Riskide prioritiseerimiseks



Praktiline ülesanne 2

- Vali põhiprotsessi jaoks kriitiline infovara – väärtus?
- Määratle asjakohased ohud
- Hinda ohtude tõenäosused
- Hinda ohtude realiseerumise võimalikke tagajärgi

(**Tulemus** - riskistsenaariumid)

- Koosta riskimaatriks

Riskihalduse sammud

Plaanimine

- Konteksti loomine
- Riski kaalutlemine
- **Riskikäsitlusplaani koostamine**
- Riski aktsepteerimine

Riskikäsitlemise võimalused

- **Riski vältimine** – riski tekitavaid tegevusi ei tehta
- **Riski säilitamine** – kulu riski realiseerumisel ja saadava tulu suhe on nii hea, et risk tasub igal juhul võtmist
- **Riski jagamine** – Kahjuliku sündmuse mõjud suunatakse edasi (kindlustus, leppetrahvid)
- **Riski vähendamine** – rakendatakse turvameetmeid kahjuliku sündmuse toimumise vältimiseks või tema mõju vähendamiseks

Riski vältimine

- Riski tekitavaid tegevusi ei tehta

Modifikatsioonid

- Riske suurendavaid tegevusi ei tehta
- Kasutatakse vähem riskantseid seadmeid
  - Näide: Win vs. Lin veebiserverina

Riski säilitamine

- Kulu riski realiseerumisel ja saadava tulu suhe on nii hea, et risk tasub igal juhul võtmist
  - Näide USA-st – u. veerand ettevõtetest ei kasuta mingeid turvameetmeid. Kõik kahjud loetakse ärikahjudeks. Kui kahjud on fataalsed, siis lastakse firma pankrotti ja alustatakse mujal uuesti
- Riski säilitamine on ka riskihalduse viimane samm
  - Jääkriski aktsepteerimine – kes ja kuidas teeb

Riski jagamine

- Kahjuliku sündmuse mõjud suunatakse edasi
  - Kindlustus
  - Leppetrahvid
- NB! Eestis kindlustatakse küll IT seadmeid, kuid ei kindlustata protsesse ega andmeid

Riski vähendamine

- Rakendatakse turvameetmeid kahjuliku sündmuse toimumise vältimiseks või tema mõju vähendamiseks

- **Riskikäsitlusplaan**

Riskikäsitlusplaan

- Ohtude vähendamise meetmete valik
  - Ise välja mõelda
  - Parim praktika
  - Meetmete kataloogid (ISKE)
- Ressurss, mis rakendamiseks kulub
- Kes teeb, kes vastutab
- Järjekord (prioriteet)

Riskikäsitlusplaani tulemid

Lähevad sisendiks

- Infoturbe programmi
- Infoturbe meetmetesse

Riskihalduse sammud

Plaanimine

- Konteksti loomine
- Riski kaalutlemine
- Riskikäsitlusplaani koostamine
- **Riski aktsepteerimine**

Riski aktsepteerimine

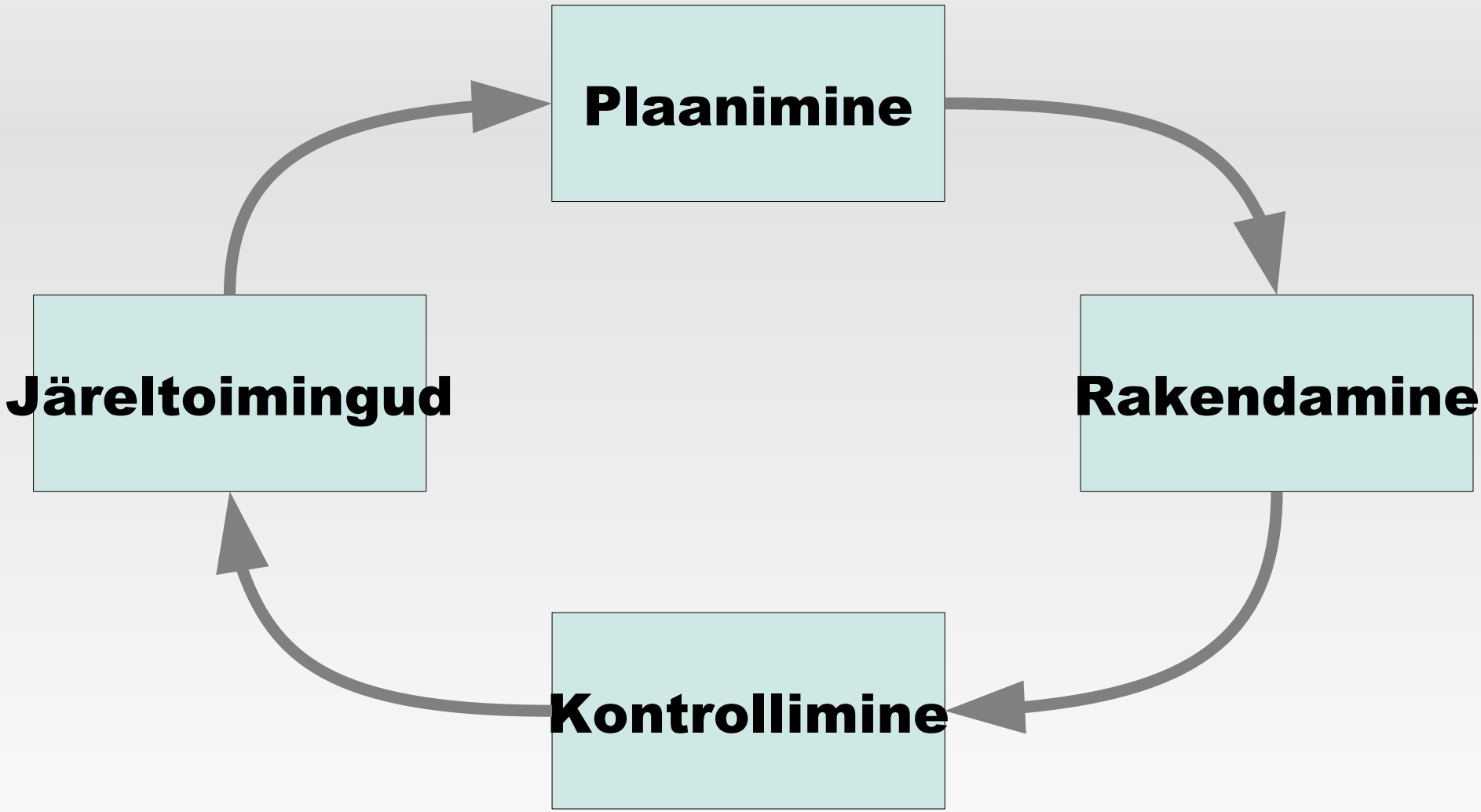
Jääkriskide aktsepteerimine

- Aktsepteerida saab ainult protsessi või vara omanik
- Soovitavalt kirjalikult
  - Riskistenaarium
  - Eeldatavad kahjud
  - Soovitavad turvameetmed
  - Turvameetmete rakendamisele kuluv ressurss (raha, aeg jne)

Praktiline ülesanne 3

- Koosta riskikäsitlusplaan eelnevalt valitud riskide osas
  - Iga meetmete rakendamise kulu (aeg+raha)
  - Kõigi meetmete rakendamise üldsumma
- Rollimäng – iga grupp esitab meetmete riski käsitlusplaani „juhatusele“ aktsepteerimiseks

Riskihalduse sammud



Riskihalduse sammud

- Riskide pidev seire ja läbivaatus
- Sisaldab ka infoturbejuhtimise intsidendihaldust

Kontrollimine

Kontrollimine

Riskide pidev seire ja läbivaatus

- Riskide hindamise protsessi tuleb läbi käia regulaarselt
  - Iga uue protsessi, tegevuse või seadme lisandumisel
  - Iga teatava aja järel – välised mõjutegurid on ajas muutuvad

Kontrollimine

Infoturbejuhtimise intsidendihaldus

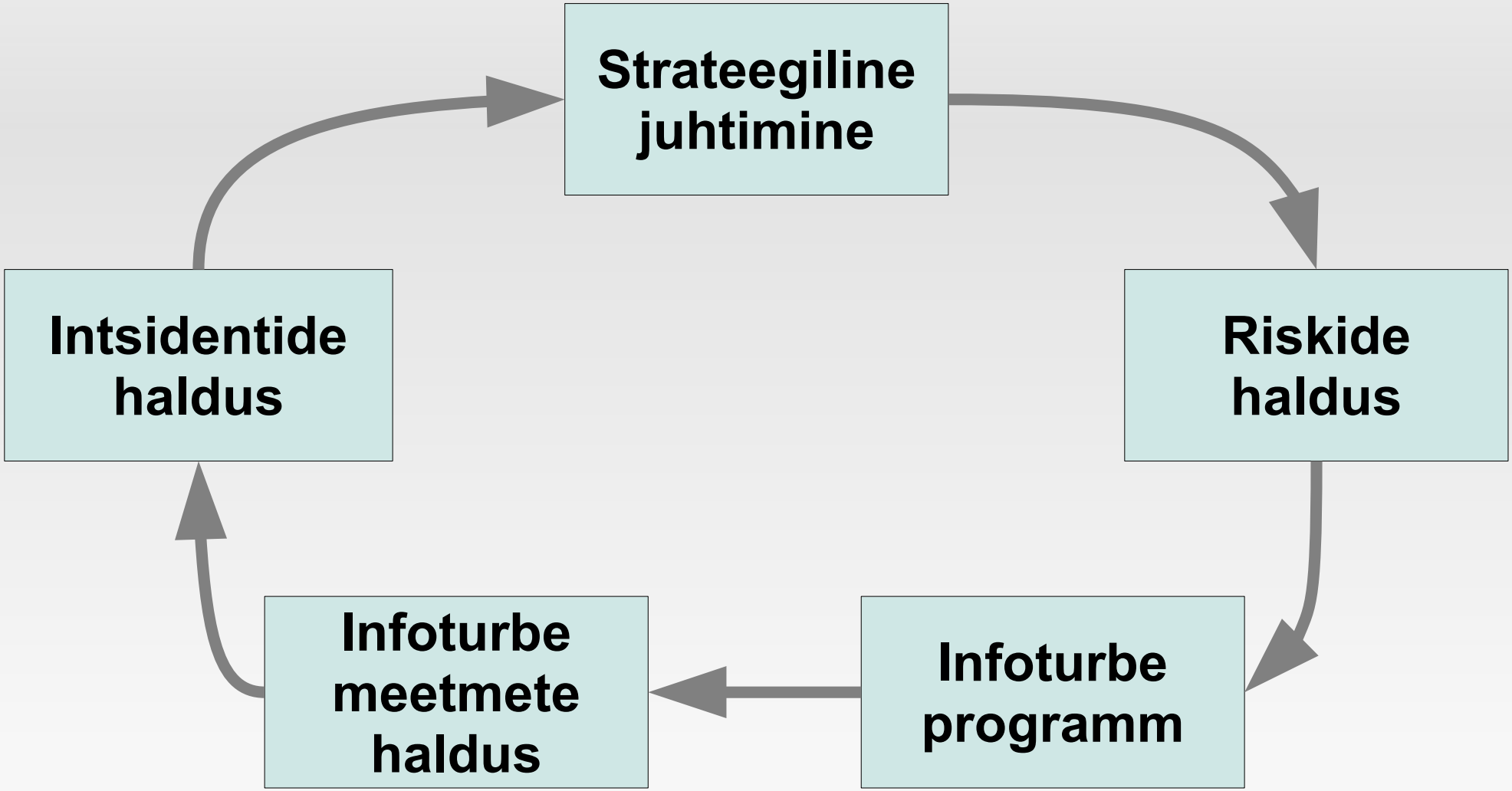
- Intsidendi korrektne uurimine ja dokumenteerimine on sisendiks riskianalüüsile
  - Kas mõni analüüsis käsitletud risk on realiseerunud
  - Kas mõni risk on analüüsis jäänud käsitlemata

Riskihalduse sammud

Järeltoimingud

- Infoturvariski halduse protsessi käigushoid ja täiustamine
- Infoturbejuhtimise haldussüsteem

Klassikaline infoturbe juhtimine



Riskihaldus Praktikas

Riskihaldus praktikas

- Alustav koosolek
  - Riskihalduse skoop
  - Riskihalduse skaalad
  - Osalised
- Intervjuud
- Riskianalüüs
- Meetmete pakkumine
- Riskide aktsepteerimine
- Riskidest teavitamine

Riskianalüüsi kokkuvõte (1/4)

Dokumenteerib mida, milleks ja kuidas tehti – samade sisendite ja sama metoodika korral peab saama sama tulemuse

- Kasutatavad mõisted
- Riskianalüüsi metoodika
- Riskianalüüsi tegevused
- Riskianalüüsi objekti (põhiprotsessi) kirjeldus ja kriitilised tegevused
  - Iga kriitiline tegevus omaette alampeatükk

Riskianalüüsi kokkuvõte (2/4)

Teenuse osutamisel vajalikud ressursid (kategooriad sõltuvad konkreetsest metoodikast)

- Personal
- Infotehnoloogilised süsteemid
- Elutähtsa teenuse osutamiseks vajalik informatsioon
- Finantsvahendid, mis on vajalikud elutähtsa teenuse osutamiseks
- Varustajad ning partnerid, kellest sõltub elutähtsa teenuse osutamine
- Muud teenuse osutamise seisukohast olulised ressursid

Riskianalüüsi kokkuvõte (3/4)

Kriitiliste tegevuste katkestusi põhjustavad ohud ja nende esinemise tõenäosus
(kategooriad sõltuvad valitud metoodikast)

- Inimtegevusest tulenev
- Loodussündmused
- Tehnoloogia
- IT kahjustused
- Majanduslikud ning õiguslikud ohud

Riskistsenariumid on selles peatükis

Riskianalüüsi kokkuvõte (4/4)

Turvameetmete pakkumine
(võib olla riskistsenaariumi juures või eraldi peatükina)

- Turvameede (nimetus ja kirjeldus)
- Millist(eid) riski(e) vähendab
- Rakendamise eeldatav kulu (raha, aeg vms)
- Prioriteet (tulenevalt riski suurusest)
- Kes teeb, kes vastutab (kui osatakse pakkuda)

Nõuanded ja soovitused (1/3)

- Riskihindamise meetoodika valikul tugineda standardile
- Võimalike riskide loetelu võtta standardist
  - Kergem aktsepti saada
- Täiendamiseks ja realiseerumise tõenäosuse hindamiseks
  - Toimunud intsidendid (kohapeal ja laias maailmas)
- Äripool (eelarve eest vastutajad) hindavad riske üldjuhul tegelikkusest allapoole

Nõuanded ja soovitused (2/3)

- Dokumenteerida, nii palju kui võimalik
  - Riskid vajavad põhjendamist ja siis on hea näidata
- Riskistsenaariumid peavad olema reaalsed ja ka võhikule lihtsalt loetavad
  - Otsustajatel on kergem aktsepteerida
- Esimene vasikas läheb aia taha
  - Sageli ka teine, kolmas ja neljas
  - Oskused tulevad läbi kogemuste

Nõuanded ja soovitused (3/3)

Abimaterjalid

- Maakonna/linna kodulehel on üldine riskianalüüs
- Maa-ameti kaardiserveris ohtlike ettevõtete kaart (ohu raadiusega)
- Eesti kohta IT-riskide realiseerumise tabeleid ei ole – tuleb kasutada väljamaised (USA, UK, ...)
- RSS reader – SANS, ENISA, Securityfocus, cert.org, Full Disclosure, ...

Küsimused?