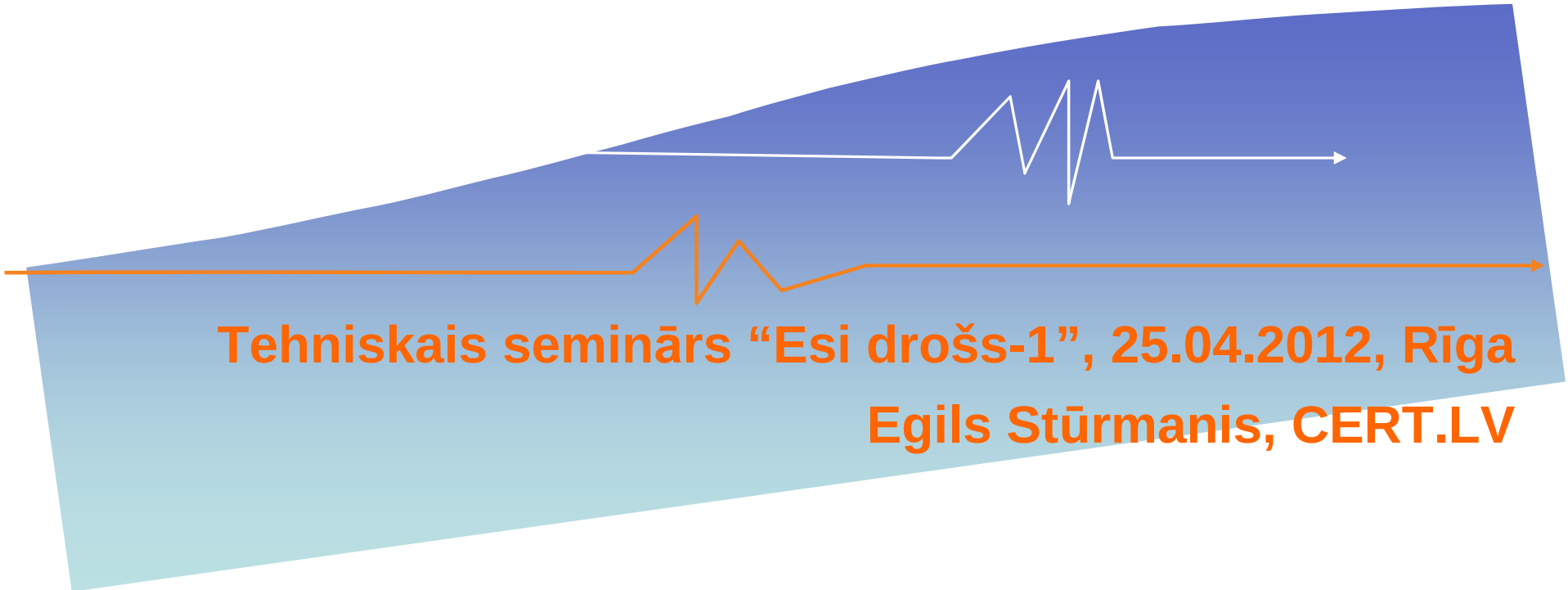
„IT drošības pamatjēdzieni, lomas un atbildības”



Tehniskais seminārs “Esi drošs-1”, 25.04.2012, Rīga

Egils Stūrmanis, CERT.LV

Standarti

- ISO 27000 series
- ITIL, ISO 20000
- COBIT
- ISO 13335
- ISF Standard of Good Practice for Information Security

IT drošības likums

Nosaka:

- Valsts un pašvaldību institūcijām izstrādāt IT drošības noteikumus.

Paredz:

- Rakstiski norīkot atbildīgo personu par IT drošības pārvaldību.
- Dokumentētus IT drošības noteikumus.

Atbildīgā persona

Pienākumi:

- Organizēt IT drošības pārvaldību.
- Veikt IT drošības pārbaudes (ne retāk kā reizi gadā).
- Celt savu kvalifikāciju, apmeklējot kursus (vismaz reizi gadā).
- Veikt darbinieku instruktāžu / apmācības (ne retāk kā reizi gadā).

IT drošības likums

IT drošību paredz nodrošināt balstoties uz:

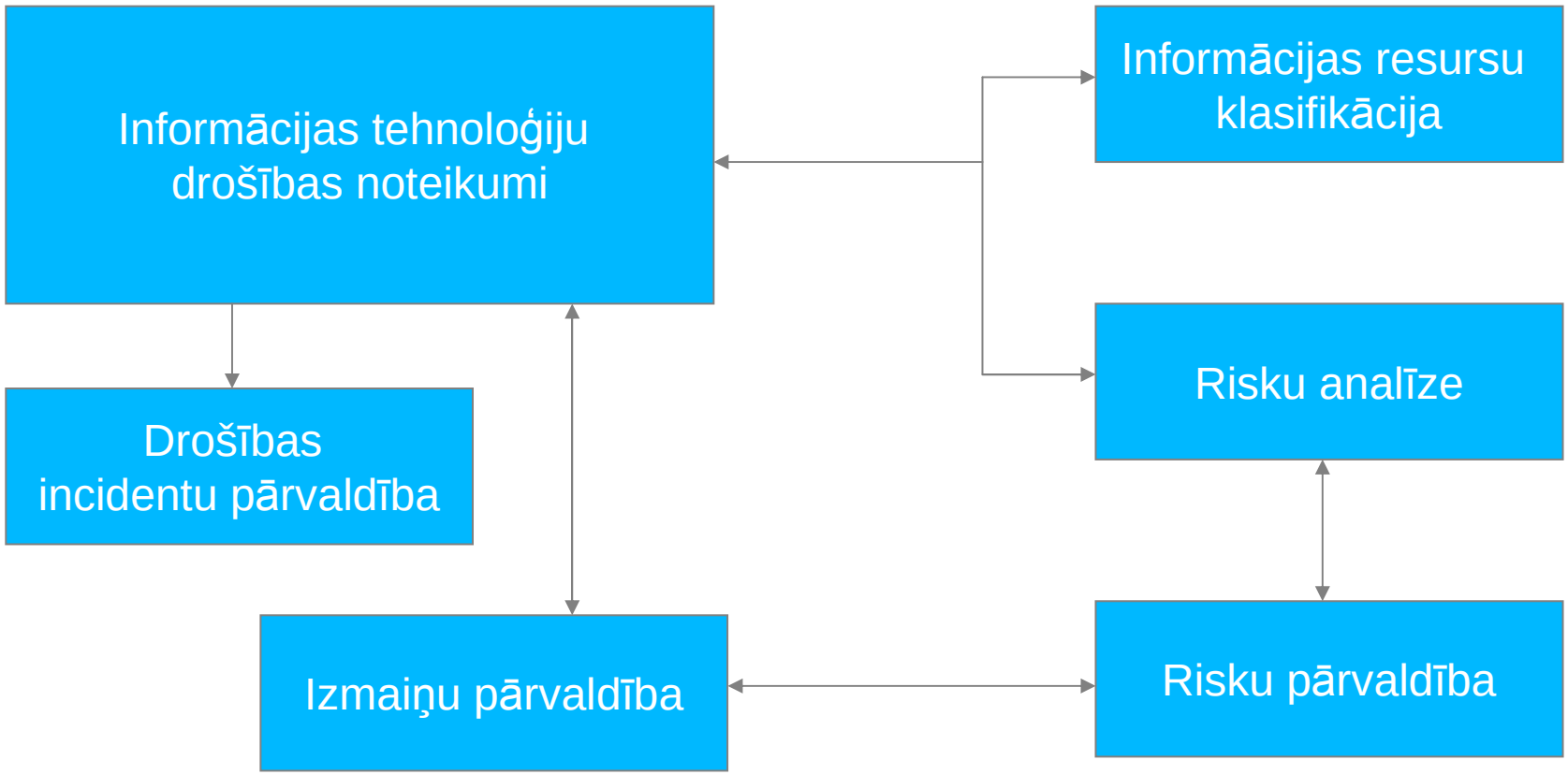
- **Informācijas integritāti** – raksturo, cik lielā mērā informācija ir pilnīga, patiesa, precīza un aktuāla.
- **Informācijas pieejamību** – raksturo to, vai lietotāji var piekļūt nepieciešamajai informācijai ne vēlāk kā noteiktā laikā pēc informācijas pieprasīšanas brīža.
- **Informācijas konfidencialitāti** – raksturo to, cik lielā mērā informācija ir pieejama tikai šīs informācijas saņemšanai paredzētajiem lietotājiem.

IT drošības noteikumi

Mērķi:

- **Apliecināt** iestādes vadības apņemšanos nodrošināt iestādē resursu drošību, lai uzturētu to integritāti, pieejamību un konfidencialitāti.
- **Nodrošināt** iestādē vienādu un sistemātisku pieeju informācijas tehnoloģiju drošības jautājumu risināšanai.
- **Panākt** iestādes darbinieku izpratni par informācijas tehnoloģiju drošības jautājumiem.
- **Būt par pamatu** procedūru, instrukciju un citu nepieciešamo drošības dokumentu izstrādē un ieviešanā.

IT drošības noteikumu shēma



Lomas un atbildība

- **Resursu turētājs** – iestādes vadītājs vai ar vadītāja rīkojumu iecelts iestādes darbinieks, kurš atbild par IT drošības pārvaldību.
- **IT drošības pārzinis** – resursu turētājs vai ārpakalpojuma sniedzējs, kurš nodrošina IT drošības pārvaldību. (*likuma izpratnē atbildīgā persona*)
- **Resursu aizbildnis** – resursu turētāja vai ārpakalpojuma sniedzēja norīkota persona, kura atbild par resursu funkcionēšanu un/vai saturu.
- **Resursu lietotājs** – iestādes darbinieks, kurš izpilda noteiktus pienākumus, atbilstoši kuriem darbiniekam ir piešķirtas tiesības lietot noteiktus resursus.

Publicētie dokumentu paraugi

- Piemērs: IT drošības pārvaldības shēma.
- Ieteicamās pašvaldību un valsts iestāžu IT drošības noteikumu vadlīnijas.
- Ieteicamās prasības izmaiņu pārvaldībai.
- Piemērs: Virtuālas iestādes apraksts .
- Piemērs: Resursu klasifikācija.
- Piemērs: Risku analīze.
- Piemērs: Risku pārvaldība.

- Paraugs: Informācijas drošības izpratnes programma.

IT drošības noteikumu vadlīnijas

- Vispārīgie jautājumi.
- Lietotie termini.
- Ārpakalpojuma pārvaldība. (ja nepieciešams)
- Resursu pārvaldība.
- Informācijas resursu klasifikācija.
- Risku analīze.
- Risku pārvaldība.
- Izmaiņu pārvaldība.
- Drošības incidentu pārvaldība.

Ārpakalpojuma pārvaldība

- IT drošības likums neaizliedz valsts un pašvaldību institūcijām šajā likumā uzliktos pienākumus deleģēt:
  - IT pakalpojumu sniedzējam,
  - Citam uzņēmējam.
- Ārpakalpojuma saņemšana **uzliek atbildību** par ārpakalpojuma sniedzēja veikumu tādā pašā mērā kā par savu.
- Ārpakalpojuma līgumā ieteicams iekļaut:
  - IT drošības likumā noteiktos pienākumus,
  - Atbildību par veikumu.

Izmaiņu pārvaldība

IT drošības pārzinis:

- veic informācijas resursu klasifikāciju,
- veic resursu risku analīzi,
- organizē iestādes darbinieku apmācību,
- apstiprina un atceļ lietotāju pieejas tiesības resursiem,
- nodrošina datu rezerves kopiju veidošanu,
- nodrošina resursu konfigurāciju pārvaldību,
- nodrošina atsevišķu iestādei būtisku resursu pārvaldību,
- nodrošina auditācijas pierakstu veikšanu,
- nodrošina drošības incidentu pārvaldību.

Drošības incidentu pārvaldība

Kritēriji:

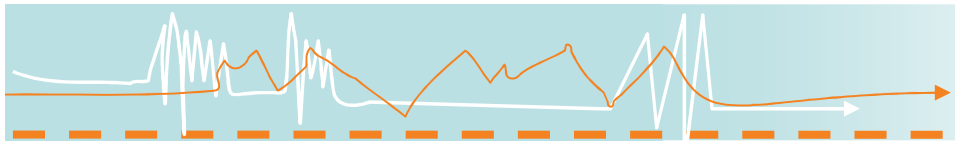
- notiek uzbrukums resursiem no ārpuses,
- notiek svarīgu resursu atteice,
- apgrūtināta iestādes normāla darbība,
- apgrūtināta būtisku pakalpojumu sniegšana.

Rīcība:

- informē CERT.LV,
- saglabā pierādījumus,
- atjauno informācijas sistēmas darbību,
- reģistrē drošības incidentu žurnālā.

KOPSAVILKUMS

- IT drošības likums uzliek pienākumus un prasa atbildību.
- CERT.LV palīdz realizēt ar likumu uzliktos pienākumus.
- CERT.LV piedāvā sagataves nepieciešamo IT drošības dokumentu izveidošanai.
- CERT.LV palīdz drošības incidentu gadījumos.



CERT.LV

Paldies par uzmanību!

http://www.cert.lv/
cert@cert.lv
egils.sturmanis@cert.lv