Ievads informācijas sistēmu drošībā

Uldis Sukovskis, CISA

Vai IT drošība ir priekšrocība?

- Augstas kvalitātes pakalpojumi
- Jaunākās tehnoloģijas (papildus risks!)
- Publiskais tēls un zīmols
- Atbilstība likumiem un noteikumiem

- **Drošība un uzticamība – konkurences faktors**

- Konkurences priekšrocība
  - uzņēmumiem
  - valstīm

IT drošības riski

- Bažas par tehnoloģiju drošību
  - Konfidenciālas informācijas izpaušana
  - Uzņēmuma darbības pārtraukumi
  - Intelektuālā īpašuma zagšana
  - utt.

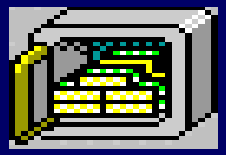
- “The wonder of the Web is that the customer knows about IT problems the same time you do. There’s no camouflage.”
  Senior VP of Electronic Brokerage Technology

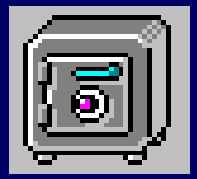
Informācijas drošības mērķi

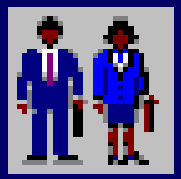
- Aizsargāt vērtīgus informācijas resursus
- Aizsargāt privātumu
- Ievērot likumus, normatīvos aktus un līgumsaistības

Informācijas drošība

AGRĀK



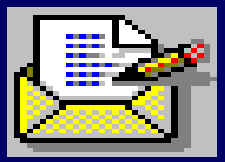




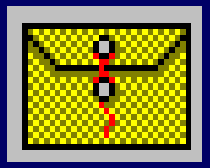
- **Glabāšana**
- Konfidenciālu informāciju glabājam seifā
- Vērtīgu informāciju (piemēram, banku čekus) glabājam seifā
- Drošas atslēgas ir tikai īpašnieku rīcībā

Informācijas drošība
AGRĀK

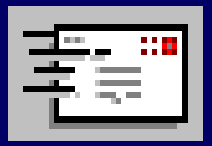
- **Pārsūtīšana**



- Dokumentus paraksta



- Aploksnes aizzīmogo



- Izmanto pasta pakalpojumus

Informācijas drošība
AGRĀK UN TAGAD

- Tradicionālās informācijas pārsūtīšanas un glabāšanas sistēmas balstās uz **uzticēšanās** principiem, kas izveidojušies gadu simtos un pat tūkstošos.

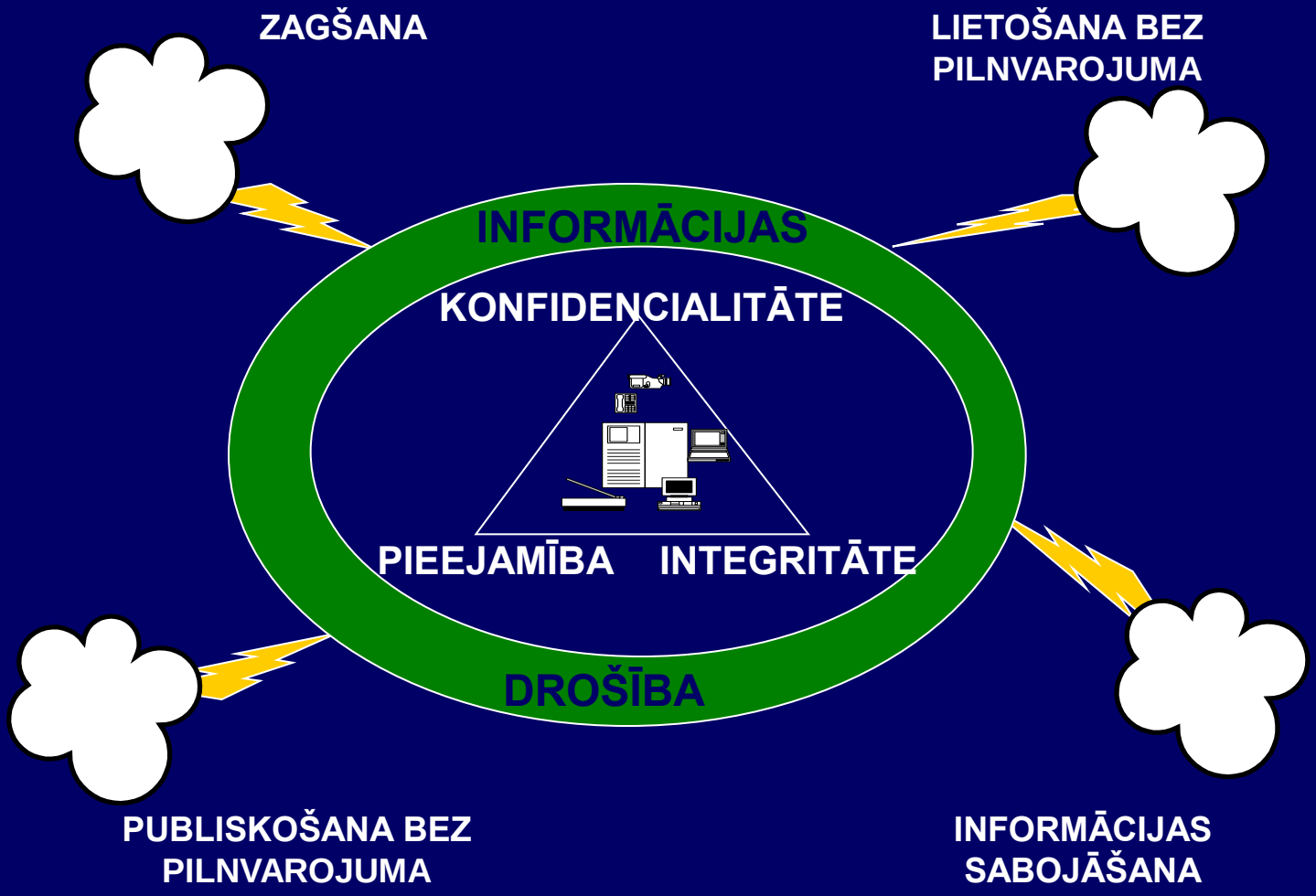
Informācijas drošības mērķi

- Aizsargāt informācijas resursus
- Aizsargāt personas privāto informāciju
- Ievērot likumus un kontraktus

Informācijas drošības pamatprincipi

- **Konfidencialitāte** – jānodrošina, lai piekļuve informācijai ir tikai pilnvarotiem lietotājiem
- **Pieejamība** – jānodrošina, lai lietotājs ar atbilstošām pilnvarām var izmantot tam nepieciešamo informāciju un modificēt to
- **Integritāte** – jānodrošina, lai informācija tiktu saglabāta pilnīga un neizmainīta, neatkarīgi no apstrādes metodēm

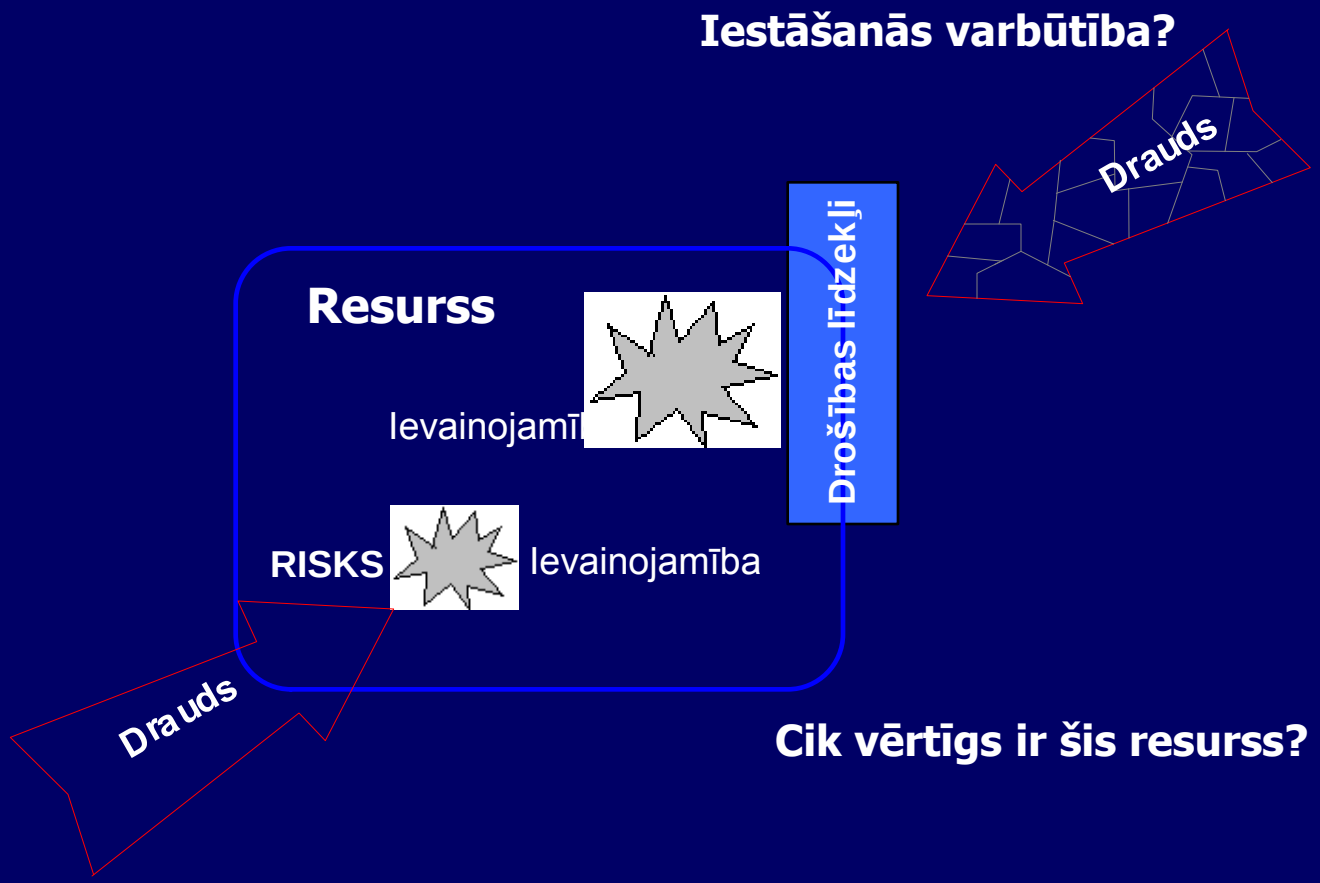
Informācijas sistēmu drošība



Pamatjēdzieni

- Resursi (*assets*)
- Ievainojamības (*vulnerabilities*)
- Draudi (*threats*)
- Drošības līdzekļi (*controls*)
- Risks, risku analīze, risku pārvaldība

Pamatjēdzieni (turpinājums)



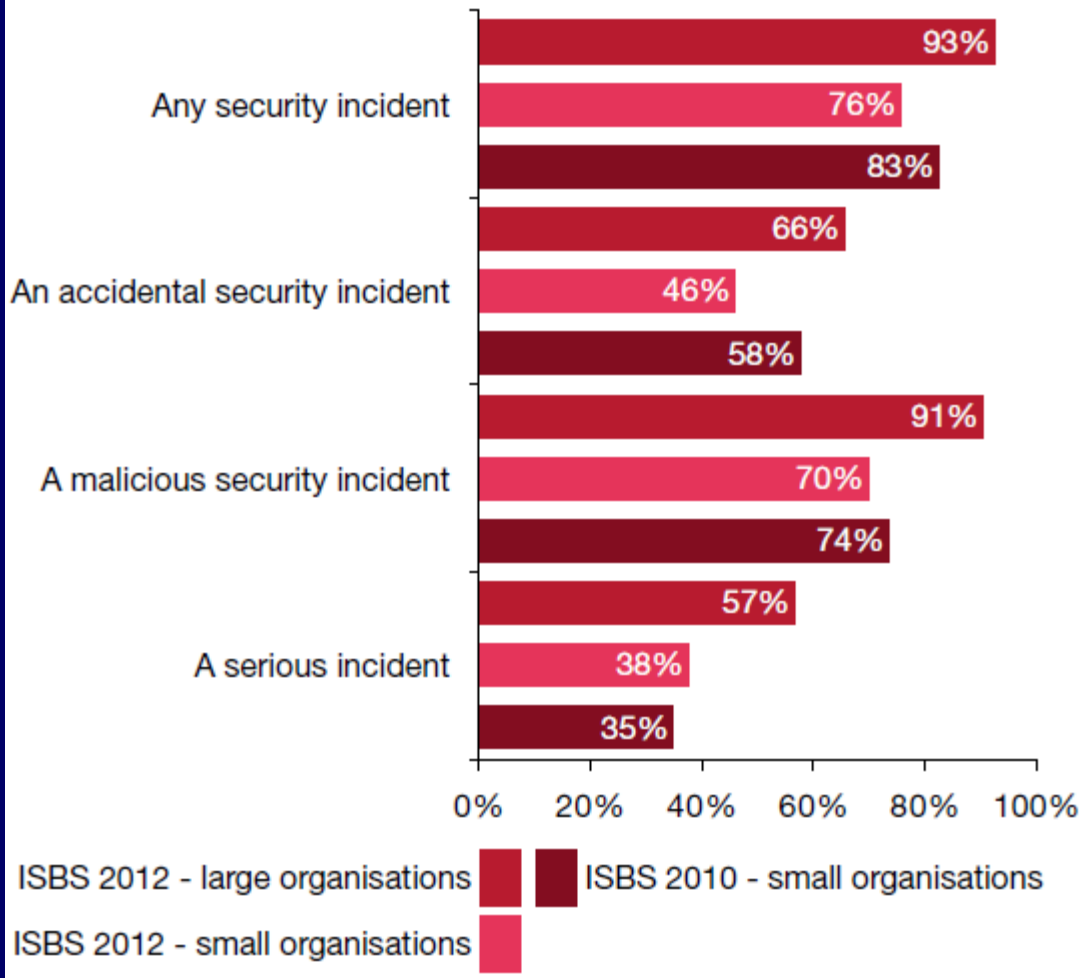
Tipiskas IS ievainojamības

- Neadekvāta serveru un datortīkla fiziskā aizsardzība
- Vājas paroles
- Anonīmo lietotāju piekļuves tiesības
- Neaizsargāts bezvadu tīkls
- Atklāta teksta komunikācijas
- Slikti sagatavoti un/vai pārslogoti administratori

Tipiski uzbrukumu veidi

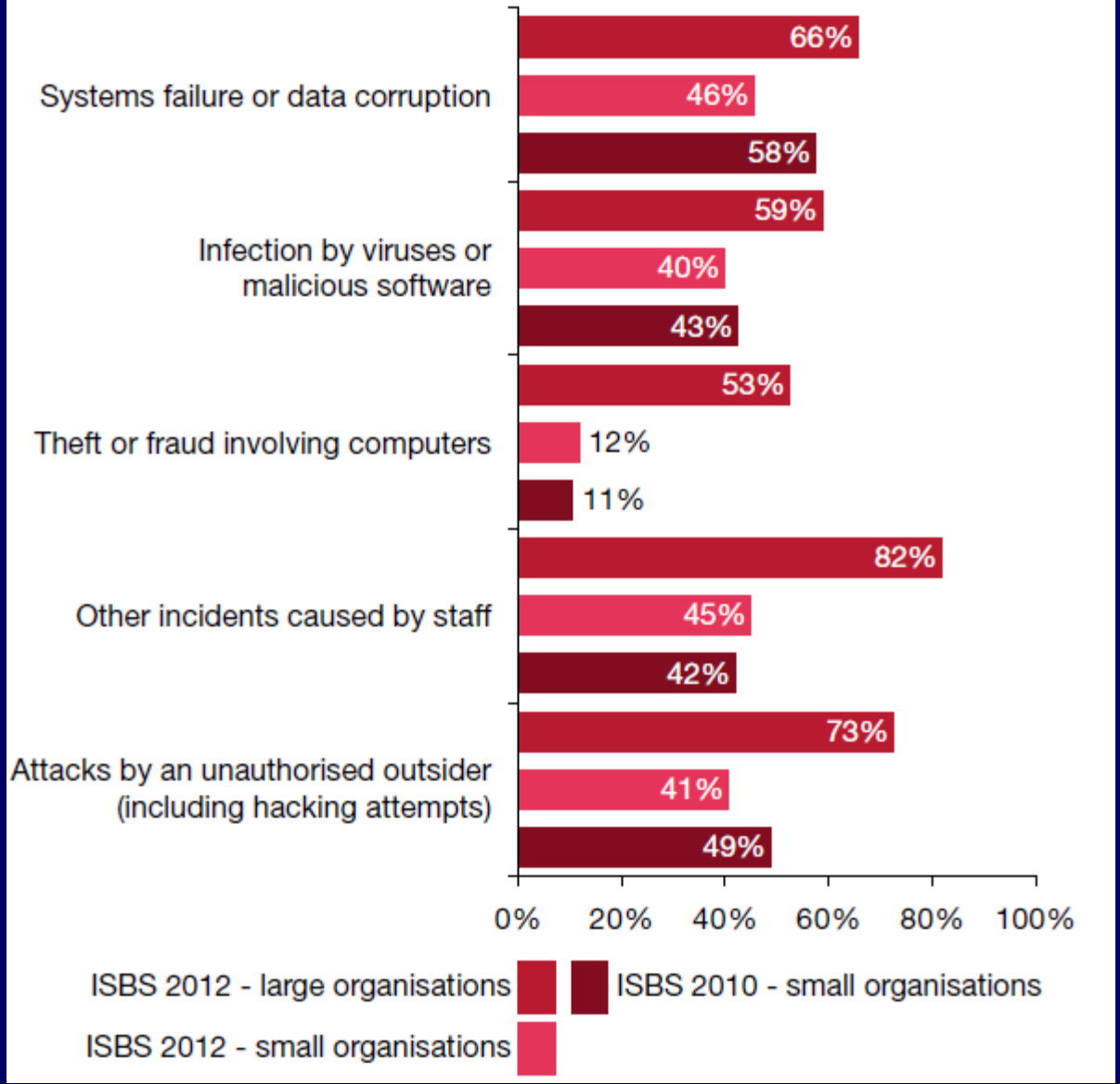
- Datu zādzības
- Iekārtu zādzības
- *Denial-of-service* (*DoS*) uzbrukumi
- Datorvīrusi un ļauprātīgas programmas (*Malicious code*)

Figure 19: In the last year, how many respondents had...



Source: Information security breaches survey 2012 - technical report, PwC

Figure 22: What type of breaches did respondents suffer?



Source: Information security breaches survey 2012 - technical report, PwC

Types of Attacks Experienced

By Percent of Respondents

Type of Attack	2005	2006	2007	2008	2009
Malware infection	74%	65%	52%	50%	64%
Bots / zombies within the organization	added in 2007		21%	20%	23%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%
Password sniffing	added in 2007		10%	9%	17%
Financial fraud	7%	9%	12%	12%	20%
Denial of service	32%	25%	25%	21%	29%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%
Web site defacement	5%	6%	10%	6%	14%
Other exploit of public-facing Web site	option altered in 2009				6%
Exploit of wireless network	16%	14%	17%	14%	8%
Exploit of DNS server	added in 2007		6%	8%	7%
Exploit of client Web browser	option added in 2009				11%
Exploit of user's social network profile	option added in 2009				7%
Instant messaging abuse	added in 2007		25%	21%	8%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%
System penetration by outsider	option altered in 2009				14%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%

2009 CSI Computer Crime and Security Survey — 2009: 185 Respondents

Drošības līdzekļu veidi

- Preventīvie līdzekļi
  - apsardze, paroles, šifrēšana, ...
- Atklājošie līdzekļi
  - auditācijas pieraksti, vīrusu kontrole, ...
- Labojošie līdzekļi
  - rezerves kopēšana, apdrošināšana ...

- Fiziskās aizsardzības līdzekļi
- Loģiskās aizsardzības līdzekļi
- Administratīvie līdzekļi

Drošības līdzekļi

Konfidencialitāte	Integritāte	Pieejamība
1. Šifrēšana 2. Piekļuves kontrole	1. Piekļuves kontrole 2. Šifrēšana un elektroniskie paraksti 3. Izmaiņu vadība 4. Vīrusu kontrole	1. Rezerves kopijas 2. Programmatūras droša glabāšana 3. Darbības atjaunošanas plāni

Drošības līdzekļi

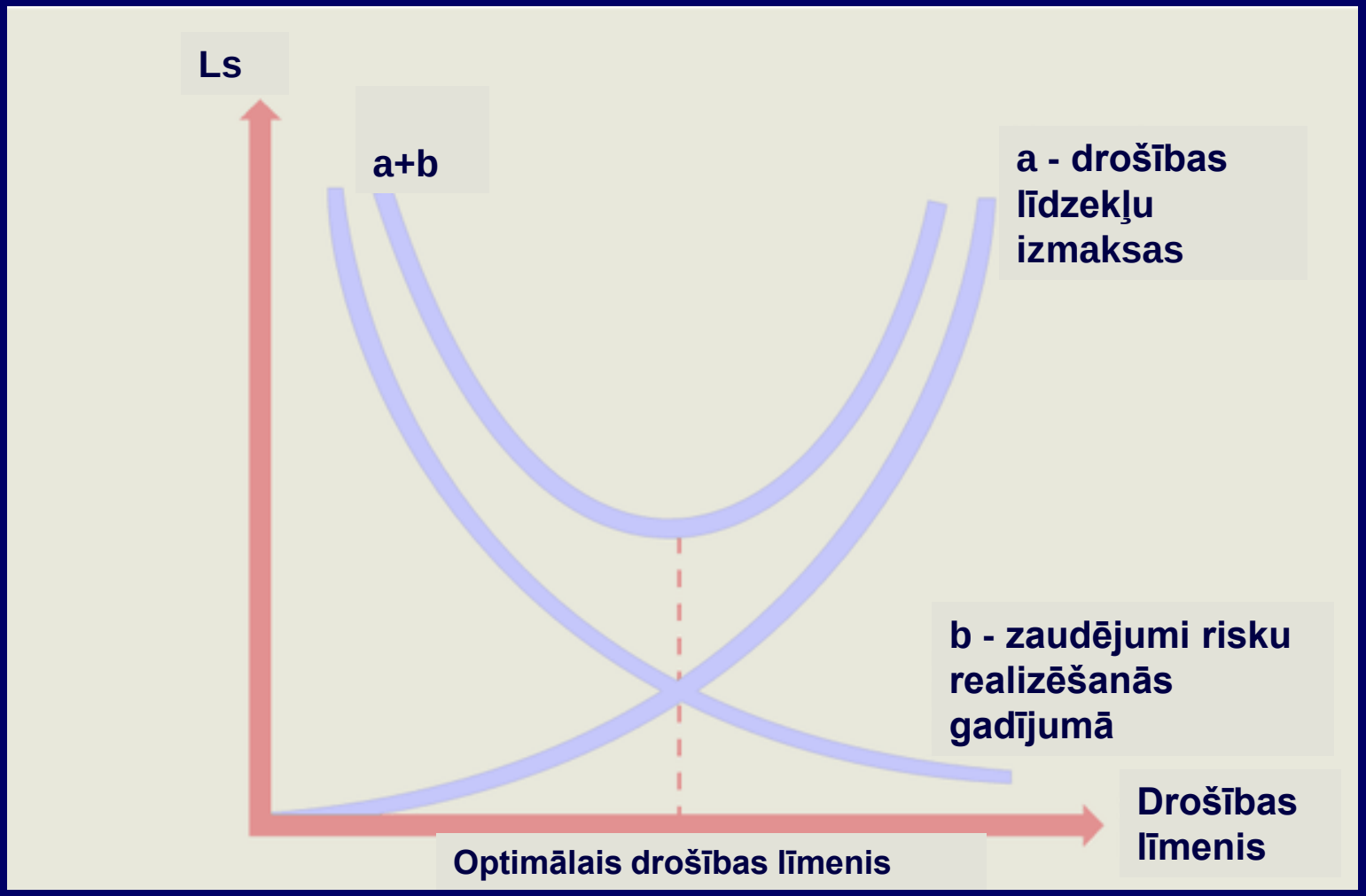
Drošības līdzekļu piemēri

- **Lietotāja autentificēšana**
  - Informācijas resursa lietotāja identitātes pārbaudes procedūra:
    - Kas Jūs esat? (vārds, izskats, pirkstu nospiedumi, ...)
    - Ko Jūs zināt? (parole, kods, īpašas zināšanas, ...)
    - Kas Jums ir? (dokumenti, identifikācijas karte, biļetes, ...)
  - Jāpārbauda vismaz divi nosacījumi.

- **CIK DROŠAS IR PAROLES?**

- **Ziņojuma avota autentificēšana**
  - Ziņojums ir saņemts no zināma un identificējama avota
- **Noliegšanas neiespējamība (*Non-repudiation*)**
  - Ziņojuma sūtītājs nevar noliegt sūtīšanas faktu

Drošības līdzekļu ekonomiskie aspekti



Ar risku jāsadzīvo?

Normatīvie akti

- **Fizisko personu datu aizsardzības likums, pieņemts 2000.g.**
- MK noteikumi Nr. 40. "Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības", pieņemti 2001.gada 30.janvārī

Normatīvie akti (turpinājums)

- **Valsts informācijas sistēmu likums, pieņemts 2002.g.**
- MK noteikumi Nr. 765 "Valsts informācijas sistēmu vispārējās drošības prasības", pieņemti 2005.g. 11.oktobrī
- MK noteikumi Nr. 764, "Valsts informācijas sistēmu vispārējās tehniskās prasības", pieņemti 2005.g. 11.oktobrī

Normatīvie akti (turpinājums)

- **Elektronisko dokumentu likums, pieņemts 2002.g.**

- MK noteikumi Nr. 473 "Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām", pieņemti 2005.g. 28.jūnijā

- MK noteikumi Nr. 358 “Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi”, pieņemti 2003.g. 1.jūlijā
- MK noteikumi Nr. 357 “Noteikumi par sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības aprakstā norādāmo informāciju”

Normatīvie akti (turpinājums)

- **Par valsts noslēpumu,** spēkā no 01.01.1997.
- MK noteikumi Nr. 21 "Valsts noslēpuma, Ziemeļatlantijas līguma organizācijas, Eiropas Savienības un ārvalstu institūciju klasificētās informācijas aizsardzības noteikumi ", pieņemti 06.01.2004.
- **Informācijas sabiedrības pakalpojumu likums**, 17.11.2004.

Normatīvie akti (turpinājums)

- **Finanšu un kapitāla tirgus komisijas izdotie noteikumi**

- Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības noteikumi
- Informācijas šifrēšanas un elektroniskās parakstīšanas noteikumi
- Elektroniski sagatavoto pārskatu iesniegšanas normatīvie noteikumi
- Operacionālā riska pārvaldīšanas ieteikumi

Standarti

www.lvs.lv

- LVS ISO/IEC 27002:2008 (identisks agrākajam LVS ISO/IEC 17799:2005) Informācijas tehnoloģija - Prakses kodekss informācijas drošības pārvaldībai
- LVS ISO/IEC 15408:2003 Informācijas tehnoloģija - Drošības metodes - Kritēriji informācijas tehnoloģiju drošības novērtēšanai
- LVS ISO/IEC TR 13335:2003 Informācijas tehnoloģija - Vadlīnijas informācijas tehnoloģijas pārvaldīšanai
- LVS ISO/IEC 12207:2002 Informācijas tehnoloģija - Programmatūras dzīves cikla procesi

Kas ir LVS ISO/IEC 27002?

- Starptautisks standarts, kas definē prasības informācijas sistēmu drošības pārvaldībai no dažādiem aspektiem:
  - pārvaldības politika
  - personāls
  - informācijas un tehniskie resursi
  - normatīvie akti
- Drošības līdzekļu kopa, kas balstīta uz labāko praksi IS drošības jomā
- 2007. g. 15. jūnijā ISO/IEC 17799:2005 mainīts numurs uz ISO/IEC 27002.
- Jaunā drošības standartu sērija sākas no numura ISO 27000

ISO 27000 standartu sērija

www.27000.org

- 27000 - terminu vārdnīca
- 27001 - drošības pārvaldība, balstoties uz ISO 27002. Tas veidots uz BS 7799:2 pamata, nosaka prasības organizācijas informācijas drošības sistēmai un tiek izmantots organizāciju sertificēšanai
- 27002 - praktiski sakrīt ar ISO/IEC 17799:2005
- 27003 - drošības pārvaldības ieviešana
- 27004 - drošības pārvaldības metrikas
- 27005 - drošības risku pārvaldība
- 27006 - prasības sertifikācijas institūcijām
- 27007 - informācijas drošības audita vadlīnijas

ISO/IEC 27002 komponenti

Personas datu aizsardzība

www.dvi.gov.lv

- Fizisko personu datu aizsardzības likums, pieņemts 2000.g.
- MK noteikumi Nr. 40. "Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības", pieņemti 2001.gada 30.janvārī

- Personas dati — jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu
- Personas datu apstrādes sistēma — jebkādā formā fiksēta strukturizēta personas datu kopa, kas ir pieejama, ievērojot attiecīgus personu identificējošus kritērijus
- Sensitīvi personas dati — personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi

- Likuma 21.pants, kas nosaka obligātu personas datu apstrādes reģistrāciju ir grozīts 2007. gada 15. martā.

Personas datu aizsardzība

(turpinājums)

- 21.pants. (1) Visas valsts un pašvaldību institūcijas, fiziskās un juridiskās personas, kas veic vai vēlas uzsākt personas datu apstrādi, reģistrē to šajā likumā noteiktajā kārtībā.
- (2) Šajā likumā noteiktā reģistrācijas kārtība neattiecas uz personas datu apstrādi:
  1) grāmatvedības un personāla uzskaites mērķiem;
  2) valsts vai pašvaldību informācijas sistēmās, kurās savāktie personas dati ir publiski pieejami;
  3) žurnālistiskiem mērķiem saskaņā ar likumu "Par presi un citiem masu informācijas līdzekļiem";
  4) arhivēšanas mērķiem saskaņā ar likumu "Par arhīviem";
  5) ja to veic reliģiskās organizācijas;
  6) ja pārzinis likumā noteiktajā kārtībā ir reģistrējis personas datu aizsardzības speciālistu.
- 21.1 pants. (1) Pārzinis var nereģistrēt personas datu apstrādi, ja viņš norīko personas datu aizsardzības speciālistu. Personas datu aizsardzības speciālists nav personas datu operators.
- (2) Par personas datu aizsardzības speciālistu norīko fizisko personu, kurai ir augstākā izglītība tiesību zinātņu, informācijas tehnoloģiju vai līdzīgā jomā un kura ir apmācīta Ministru kabineta noteiktajā kārtībā.

Personas datu aizsardzība

(turpinājums)

- **Personas datu aizsardzības speciālists** – persona, kura organizē, kontrolē un uzrauga pārziņa veiktās personas datu apstrādes atbilstību likuma prasībām.

- **Fizisko personu reģistrē par personas datu aizsardzības speciālistu, ja:**
  1. persona ir rīcībspējīga;
  2. personai ir augstākā izglītība tiesību zinātņu, informācijas tehnoloģiju vai līdzīgā jomā;
  3. persona ir apmācīta Ministru kabineta noteiktajā kartībā.

- Ja personas datu aizsardzības speciālists veic personas datu apstrādes auditu, tad papildus akreditācija Datu valsts inspekcijā nav nepieciešama.

- Pārzinis piešķir personas datu aizsardzības speciālistam līdzekļus, nodrošina informāciju un darba laika ietvaros paredz laiku, lai viņš varētu veikt arī datu aizsardzības speciālista pienākumus.

Personas datu aizsardzība

(turpinājums)

- **Personas datu apstrāde** — jebkuras ar personas datiem veiktas darbības, tādas, kā:
- • datu vākšana,
  • reģistrēšana,
  • ievadīšana,
  • glabāšana,
  • sakārtošana,
  • pārveidošana,
  • izmantošana,
  • nodošana,
  • pārraidīšana,
  • izpaušana,
  • bloķēšana,
  • dzēšana.

Personas datu aizsardzība

(turpinājums)

- 7.pants. Personas datu apstrāde ir atļauta tikai tad, ja likumā nav noteikts citādi un ja ir vismaz viens no šādiem nosacījumiem:
- 1) ir datu subjekta piekrišana;
- 2) datu apstrāde izriet no datu subjekta līgumsaistībām vai, ievērojot datu subjekta lūgumu, datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;
- 3) datu apstrāde nepieciešama sistēmas pārzinim likumā noteikto pienākumu veikšanai;
- 4) datu apstrāde nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību;
- 5) datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ievērošanu vai realizētu publiskās varas uzdevumus, kuru veikšanai personas dati ir nodoti sistēmas pārzinim vai pārraidīti trešajai personai;
- 6) datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu sistēmas pārziņa vai tās trešās personas likumiskās intereses, kurai personas dati atklāti.

Personas datu aizsardzība

(turpinājums)

- **11.pants.** Sensitīvo personas datu apstrāde ir aizliegta, izņemot gadījumus, kad:
- 1) datu subjekts ir devis rakstveida piekrišanu savu sensitīvo datu apstrādei;
- 2) speciāla personas datu apstrāde, neprasot datu subjekta piekrišanu, ir paredzēta normatīvajos aktos [...];
- 3) personas datu apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas personas dzīvību un veselību, un datu subjekts tiesiski vai fiziski nav spējīgs dot savu piekrišanu;
- 4) personas datu apstrāde ir nepieciešama, lai sasniegtu likumīgus nekomerciālus sabiedrisko organizāciju un to apvienību mērķus, ja šī datu apstrāde ir saistīta tikai ar šo organizāciju vai to apvienību biedriem un personas dati netiek nodoti trešajām personām;
- 5) personas datu apstrāde ir nepieciešama ārstniecības vajadzībām, veselības aprūpes pakalpojumu sniegšanai vai to administrēšanai [...];
- 6) apstrāde attiecas uz tādiem personas datiem, kuri ir nepieciešami fiziskās vai juridiskās personas likumīgo tiesību un interešu aizsardzībai tiesā;
- 7) personas datu apstrāde ir nepieciešama sociālās palīdzības sniegšanai un to veic sociālās palīdzības pakalpojumu sniedzējs;
- 8) personas datu apstrāde ir nepieciešama Latvijas nacionālā arhīva fonda veidošanai un to veic valsts arhīvi [...];
- 9) personas datu apstrāde ir nepieciešama statistiskiem pētījumiem, ko veic Centrālā statistikas pārvalde;
- 10) apstrāde attiecas uz tādiem personas datiem, kurus datu subjekts pats ir publiskojis;
- 11) personas datu apstrāde ir nepieciešama, pildot valsts pārvaldes funkcijas vai veidojot likumā noteiktās valsts informācijas sistēmas.

Personas datu aizsardzība

(turpinājums)

- **personas identifikācijas kods — numurs, kas tiek piešķirts datu subjekta identifikācijai**

- **13.1 pants. Personas identifikācijas kodus drīkst apstrādāt vienā no šādiem gadījumiem:**
- **1) ir saņemta datu subjekta piekrišana;**
- **2) identifikācijas kodu apstrāde izriet no personas datu apstrādes mērķa;**
- **3) identifikācijas kodu apstrāde nepieciešama turpmākas datu subjekta anonimitātes nodrošināšanai;**
- **4) ir saņemta Datu valsts inspekcijas rakstveida atļauja.**

Personas datu aizsardzība

(turpinājums)

- **Datu subjektam ir tiesības pieprasīt un saņemt no personas datu apstrādātāja informāciju:**
- paredzētais personas datu apstrādes mērķis un pamatojums
- iespējamie personas datu saņēmēji
- par tiesībām piekļūt saviem personas datiem un izdarīt tajos labojumus
- visu informāciju, kas par viņu savākta jebkurā personas datu apstrādes sistēmā, ja vien šo informāciju izpaust nav aizliegts ar likumu, nacionālās drošības, aizsardzības un krimināltiesību jomā
- par tām fiziskajām vai juridiskajām personām, kuras noteiktā laikposmā no sistēmas pārziņa ir saņēmušas informāciju par šo datu subjektu (izņemot gadījumus, kad likums aizliedz šādas ziņas izpaust)

Personas datu aizsardzības atbildīgās personas

- **Galvenie jautājumi**
  - Vai organizācijā ir dokumentēta personas datu aizsardzības sistēma, kas pilnībā atbilst visām Fizisko personu datu aizsardzības likuma prasībām?
  - Vai datu aizsardzības sistēma reāli darbojas un vai tā ir efektīva?

- **Atbildīgās personas**
- Pārzinis
  - fiziskā vai juridiskā persona, valsts vai pašvaldību institūcija, kura nosaka personas datu apstrādes mērķus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar šo likumu
- Personas datu operators
  - sistēmas pārziņa pilnvarota persona, kas veic personas datu apstrādi sistēmas pārziņa uzdevumā

Likuma prasības personas datu aizsardzībai

- Godprātīga un likumīga datu apstrāde
- Datu apstrāde tiek veikta tikai atbilstoši paredzētajam mērķim
- Dati ir tikai nepieciešamajā apjomā
- Dati netiek glabāti ilgāk nekā nepieciešams
- Dati tiek apstrādāti saskaņā ar datu subjekta tiesībām

- Dati ir pilnīgi un precīzi
- Dati ir drošībā
- Dati netiek pārsūtīti uz citām organizācijām vai ārvalstīm bez drošas adekvātas aizsardzības

- Avots: Personas datu apstrādes sistēmu audita rokasgrāmata, DVI, 2004

MK noteikumi Nr.40

Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības

- 5. Sistēmas pārzinis katrai personas datu apstrādes sistēmai izstrādā iekšējos datu apstrādes sistēmas aizsardzības noteikumus, kuros nosaka:

MK noteikumi Nr.40 (turpinājums)

- Datu apstrādes sistēmas aizsardzības noteikumos jānosaka:
- 5.1. par informācijas resursiem, tehniskajiem resursiem un personas datu aizsardzību **atbildīgās personas**, to tiesības un pienākumus;
- 5.2. personas **datu aizsardzības klasifikāciju** atbilstoši to vērtības un konfidencialitātes pakāpei;
- 5.3. **tehniskos resursus**, ar kādiem tiek nodrošināta personas datu apstrāde;
- 5.4. personas datu apstrādes **organizatorisko procedūru**, nosakot personas datu apstrādes laiku, vietu un kārtību;
- 5.5. pasākumus, kas veicami tehnisko resursu **aizsardzībai pret ārkārtas apstākļiem** (piemēram, ugunsgrēks, plūdi);
- 5.6. līdzekļus, ar kādiem nodrošina tehniskos resursus **pret tīšu bojāšanu un neatļautu iegūšanu**;
- 5.7. informācijas **nesēju glabāšanas un iznīcināšanas kārtību**;
- 5.8. **paroles garumu un uzbūves nosacījumus** (minimālais paroles garums ir astoņi simboli);
- 5.9. **paroles lietošanas kārtību**, kā arī laikposmu, pēc kura nomaināma parole;
- 5.10. **rīcību, ja parole vai kriptoatslēga kļuvusi zināma** citai personai;
- 5.11. personas **datu lietotāju tiesības, pienākumus, ierobežojumus un atbildību**.

Drošības noteikumi

- **Drošības noteikumi būtu jāizstrādā nevis atsevišķām sistēmām, bet visai organizācijai!**

- Sakārtota IT procesu pārvaldība
- Dokumentēta IS drošības politika
- Organizatorisku un tehnoloģisku drošības pasākumu kopums
- Drošību visvairāk apdraud vājākais ķēdes posms!

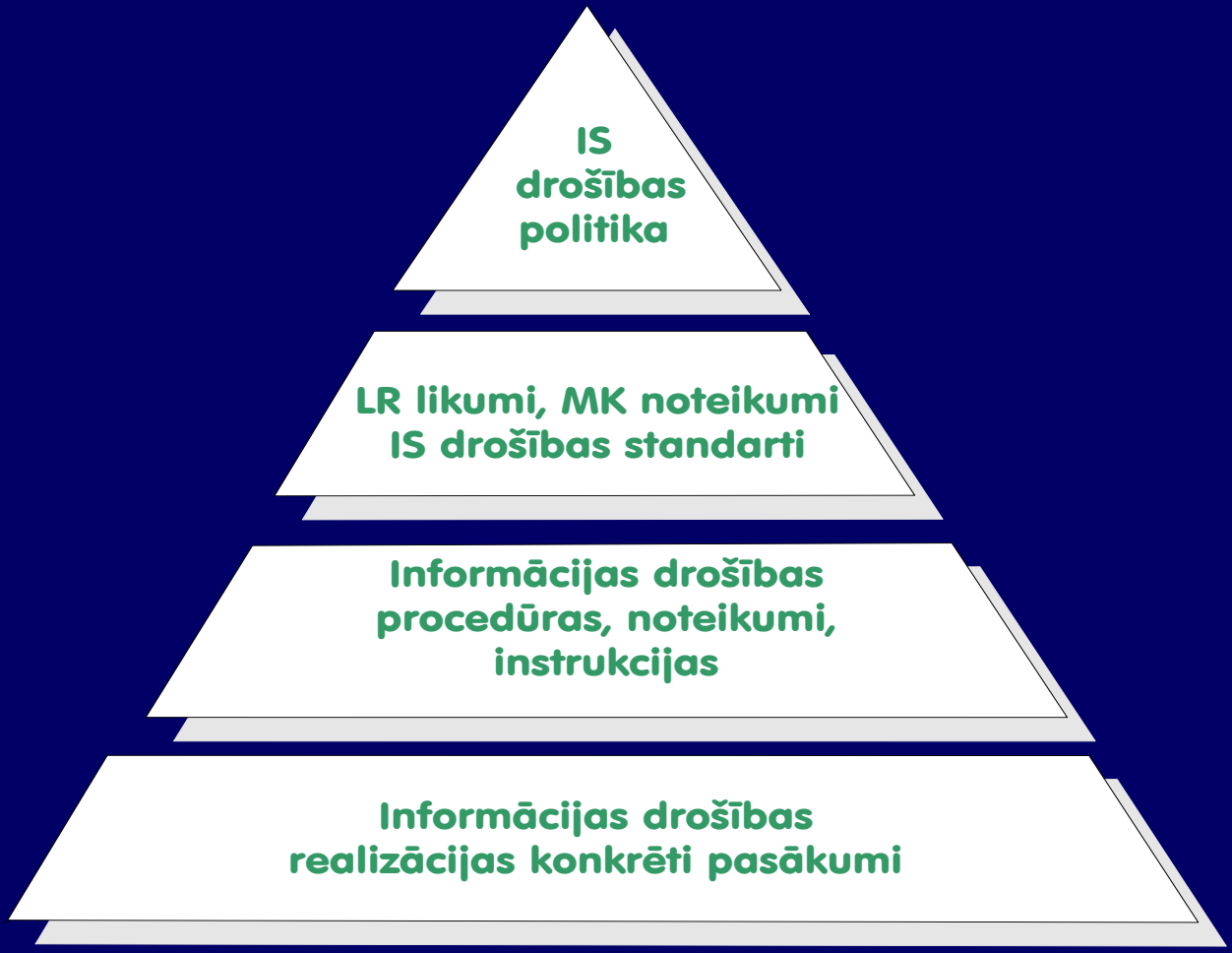
Vai manas organizācijas elektroniskā informācija ir droša?

Personas datu apstrādes sistēmu audits

- Fizisko personu datu aizsardzības likuma 26.panta otrā daļa:

- " Valsts un pašvaldību institūcijas reizi divos gados iesniedz Datu valsts inspekcijai audita atzinumu par personas datu apstrādi, ietverot tajā arī riska analīzi, un pārskatu par informācijas drošības jomā veiktajiem pasākumiem"

Informācijas drošības risinājums



Dokumentēta IS drošības pārvaldība

- Informācijas sistēmas drošības politika
- Informācijas klasificēšanas metodika
- Informācijas sistēmas risku analīzes metodika
- Informācijas sistēmu loģiskās pieejas tiesību procedūra
- Datu rezerves kopēšanas procedūra
- Informācijas sistēmu auditācijas pierakstu noteikumi
- Drošības incidentu pārvaldības procedūra
- Informācijas sistēmas nepārtrauktas darbības nodrošināšanas plāns
- Datorlietotāju instrukcija
- Darbinieku apmācības plāns drošības jautājumos
- Noteikumi attiecībām ar ārējiem pakalpojumu sniedzējiem

Drošības politika

- Drošības organizācija, pienākumu un atbildības sadalījums
- Atbilstība Latvijas un starptautiskajiem standartiem un tiesību aktiem
- Personāla drošības jautājumi
- Informācijas klasifikācijas principi
- Risku analīzes veikšanas kārtība un regularitāte
- Darbības nepārtrauktības nodrošināšana
- Vides un fiziskā drošība
- Loģiskās piekļuves tiesības
- Informācijas sistēmu izstrāde
- IS lietotāju darbību uzskaites kārtība
- Publiskā tīkla pieslēgumu drošība
- E-pasta drošība
- Portatīvo datoru izmantošanas kārtība
- Ārējo pakalpojumu sniedzēju atbildības un līgumattiecību jautājumi
- Drošības uzraudzība un audits

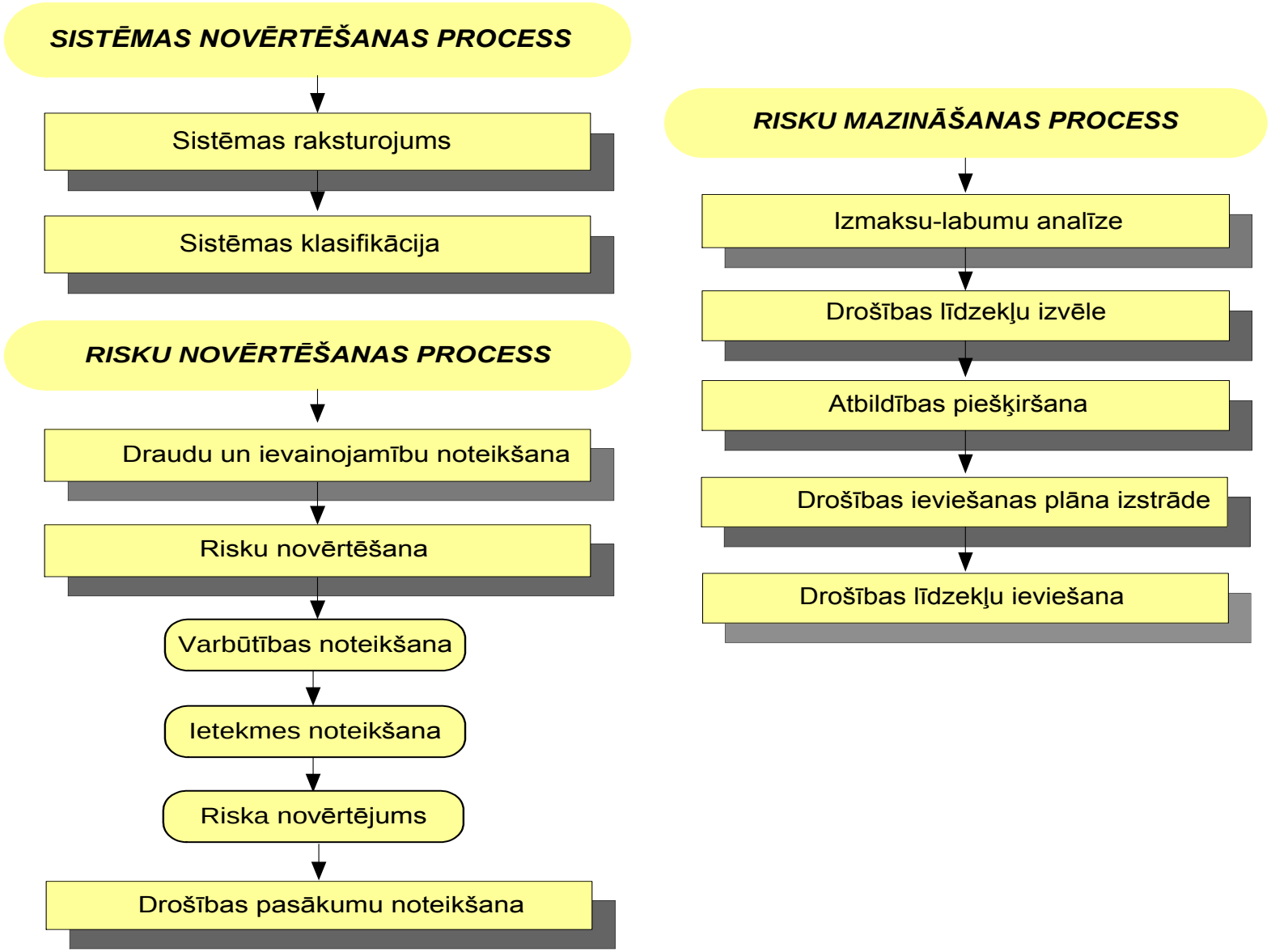
Informācijas klasificēšana

- Informācijas resursu klasificēšanu veic informācijas resursu īpašnieks
  - pēc resursa konfidencialitātes pakāpes
  - pēc resursa svarīguma pakāpes
- Klasificē visus informācijas resursus neatkarīgi no informācijas nesēja (papīrs, cietais disks utt.)
- To dara pēc informācijas resursa izveidošanas un jāatkārto pēc būtiskām izmaiņām
- IS resursu klasificēšana ir pamats drošības risku analīzei

Drošības risku analīze

- Risku analīzi veic, lai noteiktu iespējamo draudu un risku ietekmi un apjomus
- Šī procesa rezultāts palīdz izvēlēties adekvātus līdzekļus risku mazināšanai
- To jāveic atkārtoti, ja informācijas sistēmā notikušas izmaiņas, kuras var ietekmēt organizācijas vai tās partneru informācijas sistēmu drošību

Risku pārvaldība



Atbildīgās personas

- **Informācijas sistēmas turētājs (īpašnieks - *owner*)**
  - persona, kas rīkojas ar informācijas resursiem organizācijas uzdevumā
- **Tehnisko resursu turētājs (aizbildnis - *custodian*)**
  - persona, kura pilnvarota rīkoties ar informācijas sistēmas tehniskajiem resursiem organizācijas uzdevumā
- **IS drošības pārvaldības personāls**
  - veic IS drošības procesu kontroli, darbinieku apmācību, rīkojas drošības pārkāpumu gadījumos, regulāri pārskata un aktualizē drošības dokumentus atbilstoši organizācijas vajadzībām, likumdošanai un standartiem

- Information Systems Audit and Control Association http://www.isaca.org
- European Network and Information Security Agency http://www.enisa.eu.int
- The European Telecommunications Standards Institute http://www.etsi.org
- National Institute of Standards and Technology, Information Technology Laboratory http://www.itl.nist.gov
- The Information Systems Security Association http://www.issaireland.org
- The Open Web Application Security Project http://www.owasp.org

- http://netsecurity.com
- http://www.cert.org
- http://www.sans.org