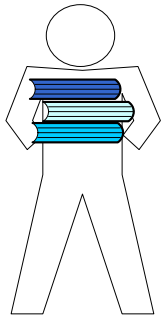
IS drošības risku analīze

Uldis Sukovskis, RTU

Drošības risku analīze

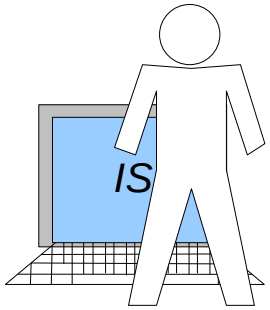
- Risku analīzi veic, lai noteiktu iespējamo ar IS saistīto draudu un risku ietekmi un apjomus.
- Šī procesa rezultāts palīdz izvēlēties adekvātus līdzekļus risku mazināšanai.
- Riska analīzi nepieciešams veikt katrai esošai, plānotai vai ieviešamai IS.
- To jāveic atkārtoti, ja informācijas sistēmā notikušas izmaiņas, kuras var ietekmēt organizācijas vai tās partneru informācijas sistēmu drošību.

Procesā iesaistītas puses



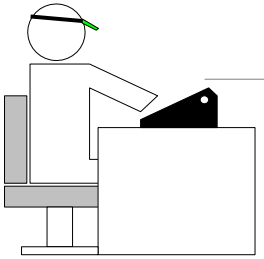
IS drošības administrators

Uzsāk un vada risku pārvaldības procesu un pieņem lēmumus par drošības līdzekļu ieviešanu



IS turētājs

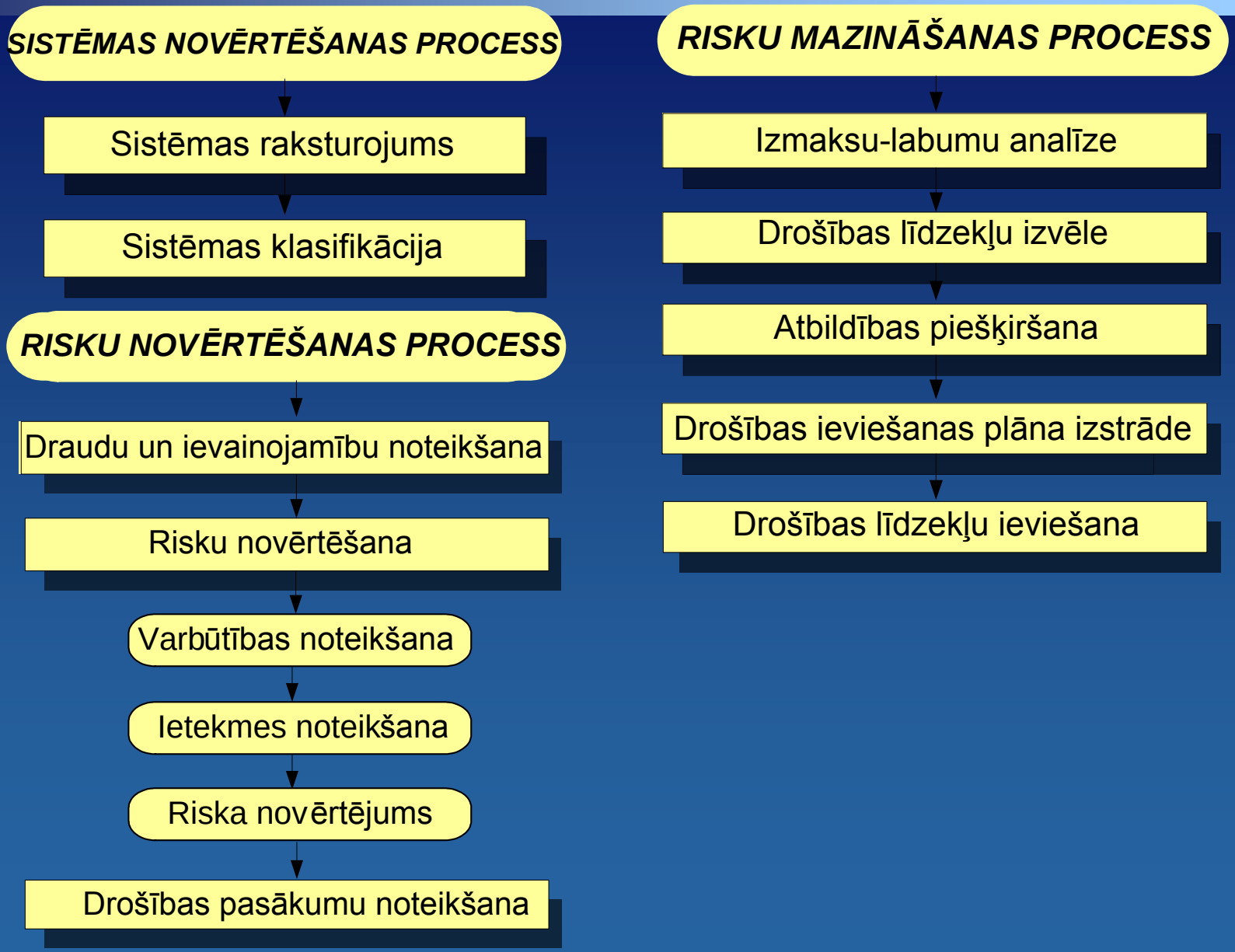
Piedalās risku pārvaldības procesā un drošības pasākumu ieviešanas lēmumu pieņemšanā



Tehnisko resursu turētājs

Sniedz informāciju par esošajiem drošības aizsardzības pasākumiem

Risku pārvaldības process



Sistēmas novērtēšana

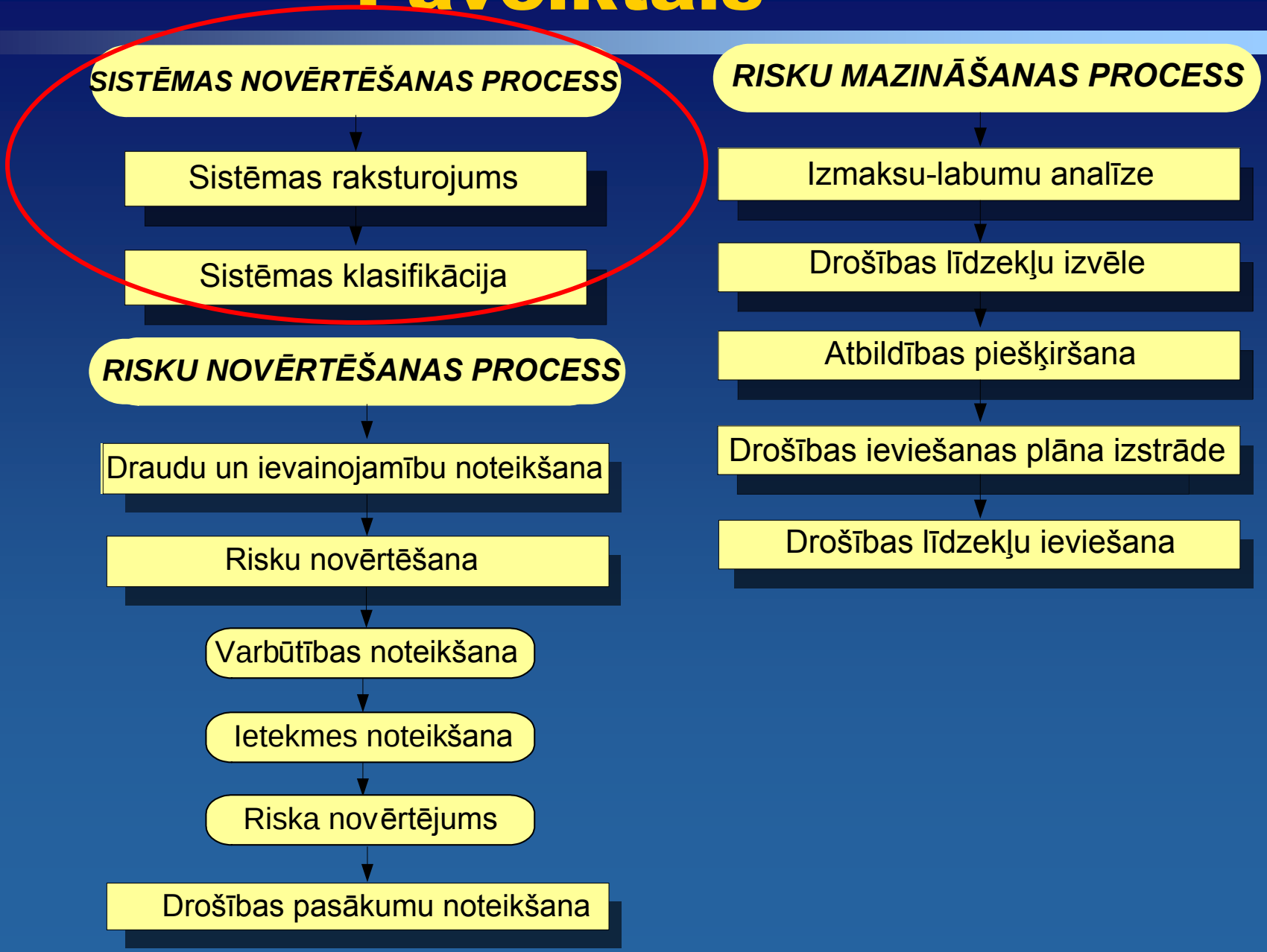
- Pirms risku analīzes vēlams veikt informācijas klasificēšanu pēc divām pazīmēm – vērtības un konfidencialitātes.
- **Vērtības noteikšanai**, novērtē IS zaudējuma ietekmi.
- Zaudējumus var vērtēt pēc šādas skalas:
  - A – organizācijas darbība ir apdraudēta,
  - B – nopietni zaudējumi,
  - C – jūtami zaudējumi,
  - D – nebūtiski zaudējumi,
  - E – nav zaudējumu.
- Piemēram, ja grāmatvedības sistēmas dati par pēdējo pusgadu tiek sabojāti, tas var radīt jūtamus zaudējumus (C).
- **Otrkārt**, novērtē informācijas **slepenības pakāpi**.

Kritiskais laika intervāls

- Kritiskais laika intervāls – laika intervāls, kuru pārsniedzot nav iespējama organizācijas apmierinoša darbība, ja sistēma nav lietojama.
- Kritisko laika intervālu nosaka, izvēloties to laika intervālu, virs kura informācijas resursu nepieejamība var radīto zaudējumu ietekmi paaugstināt no C uz B līmeni.
- Piemērs.

PIEEJAMĪBAS ZAUDĒJUMS UZ:					
Vienu stundu	A	B	C	D	E
Vienu dienu	A	B	C	D	E
Vienu nedēļu	A	B	C	D	E
Divām nedēļām	A	B	C	D	E
Vienu mēnesi	A	B	C	D	E
KRITISKAIS LAIKA INTERVĀLS – Divas nedēļas					

Paveiktais


SISTĒMAS NOVĒRTĒŠANAS PROCESS
Sistēmas raksturojums
Sistēmas klasifikācija
RISKU NOVĒRTĒŠANAS PROCESS
Draudu un ievainojamību noteikšana
Risku novērtēšana
Varbūtības noteikšana
Ietekmes noteikšana
Riska novērtējums
Drošības pasākumu noteikšana
RISKU MAZINĀŠANAS PROCESS
Izmaksu-labumu analīze
Drošības līdzekļu izvēle
Atbildības piešķiršana
Drošības ieviešanas plāna izstrāde
Drošības līdzekļu ieviešana

Risku novērtēšana

IS resursa nosaukums:	
RISKA NOVĒRTĒŠANAS FORMA NR.	A1
Drauds	Servera aparatūras ekspluatācijas vides traucējumi
Riska apraksts	Servera aparatūras ekspluatācijas vides traucējumu rezultātā tiek sabojāta aparatūra un zaudēti sistēmas dati
Vidējais biežums	
Zaudējumu vēsture	

Ievainojamības	
	Servera aparatūra nav pasargāta no elektroenerģijas padeves pārtraukumiem
	Servera aparatūra netiek ekspluatēta atbilstoši ražotāju prasībām (temperatūras režīms, u.c.)
	Pieslēgums elektrotīklam un datortīklam nav iekārtots atbilstoši tehniskajiem noteikumiem (piemēram, tiek lietoti pagarinātāji, iekārtas nav pieslēgtas pie zemējuma kontūra atbilstoši tehniskiem noteikumiem, u.tml.)
	Nav instrukcijas par rīcības plānu elektroenerģijas padeves pārtraukumu gadījumā
	Ventilācijas atveres (logi, u.tml.) un ventilācijas sistēma nav aizsargātas pret svešķermeņu iekļūšanu, gaisa piesārņojumu, radiācijas iekļūšanu telpā un tiešu saules staru iedarbību
	Telpās, kurās uzstādīti serveri un rezerves kopēšanas iekārtas, atļauts smēķēt
	Telpas, kurās uzstādīti serveri un rezerves kopēšanas iekārtas, var applūst no gruntsūdeņiem vai ūdenstilpnēm

Drauda iestāšanās varbūtība	neiespējams	maz ticams	iespējams	ļoti iespējams	noteikti iestāsies
Ietekme uz iestādi	nav zaudējumu	nebūtiski zaudējumi	jūtami zaudējumi	nopietni zaudējumi	darbība ir apdraudēta

Nepieciešamie drošības pasākumi	Eksistē	Ir ieplānots	Vajadzīgs
Uzstādīt nepārtrauktās barošanas iekārtas			
Izstrādāt aparatūras izmantošanas un drošības noteikumus			
Izstrādāt elektrotīkla un datortīkla izmantošanas un drošības noteikumus			
Ierīkot piespiedu ventilāciju			
Izstrādāt instrukciju par rīcības plānu elektroenerģijas padeves pārtraukumu gadījumā			
Aizsargāt ventilācijas atveres pret svešķermeņu iekļūšanu			
Aizliegt darbiniekiem pīpēt telpās, kurās uzstādīta datortehnika			
Uzstādīt dīzeļģeneratoru elektroenerģijas nodrošināšanai			
Veikt regulāru UPS sistēmas darbības parametru pārbaudi			

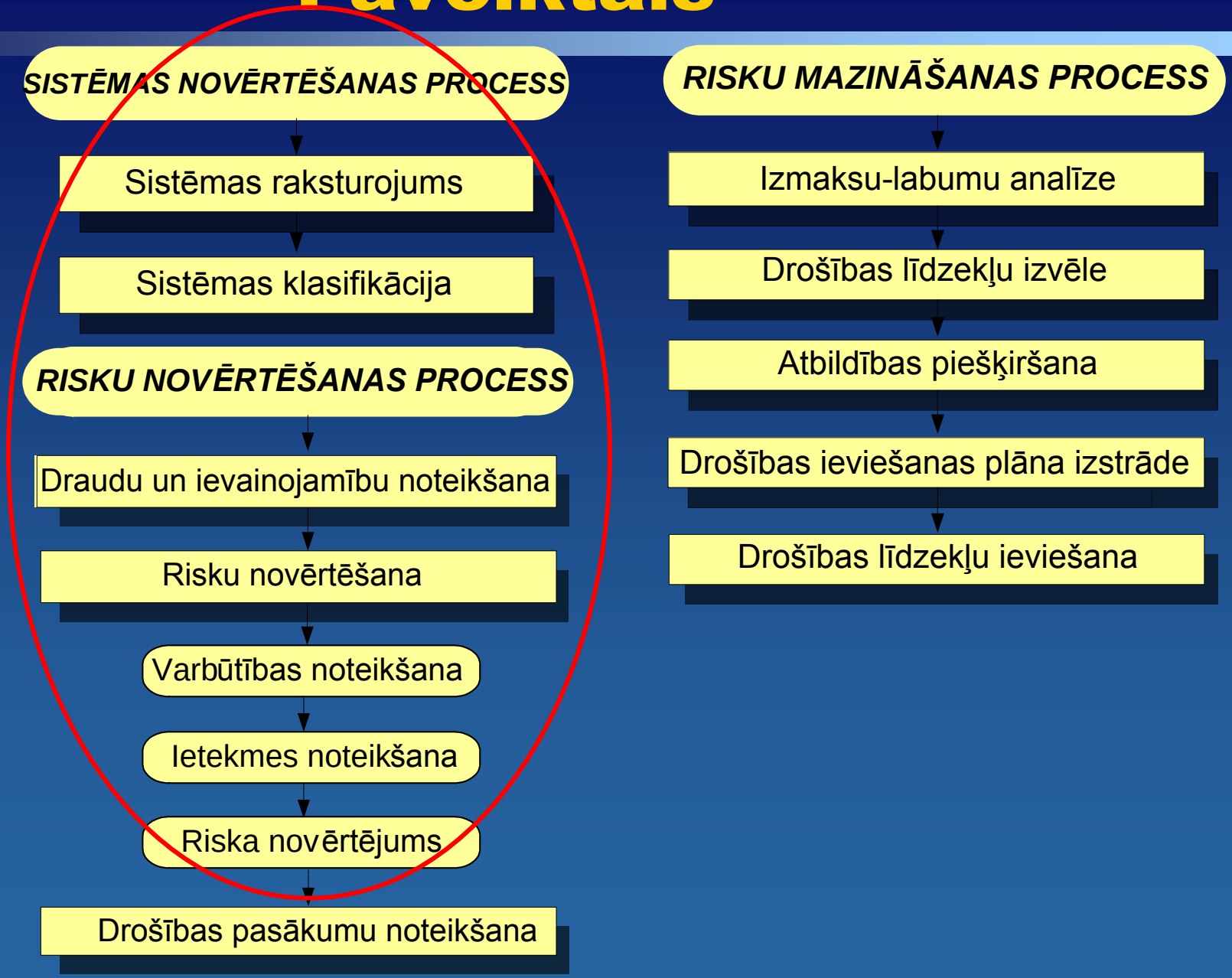
Riska novērtējums

Riska iestāšanās varbūtība	neiespējams	maz ticams	iespējams	ļoti iespējams	varbūtējs
Ietekme	niecīga ietekme	nebūtiska ietekme	nozīmīgi zaudējumi	nopietni zaudējumi	Firmas darbība ir apdraudēta
Riska klasifikācija	ļoti zems	zems	vidējs	augsts	ļoti augsts

RISKS = VARBŪTĪBA x IETEKME

Varbūtība	Ietekme				
	Nav zaudējumu	Nebūtiski zaudējumi	Jūtami zaudējumi	Nopietni zaudējumi	Firmas darbība ir apdraudēta
Noteikti iestāsies	Ļoti zems	Zems	Vidējs	Augsts	Ļoti augsts
Ļoti iespējams	Ļoti zems	Zems	Vidējs	Augsts	Augsts
Iespējams	Ļoti zems	Zems	Vidējs	Vidējs	Vidējs
Maz ticams	Ļoti zems	Zems	Zems	Zems	Zems
Neiespējams	Ļoti zems	Ļoti zems	Ļoti zems	Ļoti zems	Ļoti zems

Paveiktais


SISTĒMAS NOVĒRTĒŠANAS PROCESS
Sistēmas raksturojums
Sistēmas klasifikācija
RISKU NOVĒRTĒŠANAS PROCESS
Draudu un ievainojamību noteikšana
Risku novērtēšana
Varbūtības noteikšana
Ietekmes noteikšana
Riska novērtējums
Drošības pasākumu noteikšana
RISKU MAZINĀŠANAS PROCESS
Izmaksu-labumu analīze
Drošības līdzekļu izvēle
Atbildības piešķiršana
Drošības ieviešanas plāna izstrāde
Drošības līdzekļu ieviešana

Riska mazināšanas darbības

Riska līmenis	Nepieciešamas darbības
Ļoti augsts	Sistēmas darbību nevar turpināt. Drošības pasākumi jāveic nekavējoties, jāizstrādā plāns un tas jāīsteno, cik ātri vien iespējams.
Augsts	Ir neatliekama nepieciešamība pēc drošības pasākumiem. To ieviešanas plāns ir jāizstrādā un jāīsteno nekavējoties.
Vidējs	Papildu drošības pasākumi ir nepieciešami un plāns to realizācijai jāizstrādā un jāīsteno saprātīgā laikā.
Zems	Jaunu drošības pasākumu ieviešana nav kritiska. Izstrādājot sistēmas uzlabošanas plānu, ir jāizvērtē papildu drošības pasākumu nepieciešamība.
Ļoti zems	Drošības pasākumu ieviešana nav obligāta.