FINANŠU NOZARES ASOCIĀCIJA

MĀRCIS PELCIS

Finanšu nozares asociācijas Darbības atbilstības un kontroles komitejas Drošības apakškomitejas vadītājs

«Kiberšahs 2018» Rīga

KIBERDROŠĪBAS BRIEDUMA NOVĒRTĒJUMS BANKĀ

AKTUALITĀTE

- Informācijas tehnoloģiju attīstība.
- Jauni apdraudējumi.
- Bankas informācijas drošība un reputācija.
- Latvijas valsts finanšu sistēmas stabilitāte un drošība.

PROBLĒMAS

- Trūkst vienkopus pieejamas informācijas par banku sektora kiberdrošības briedumu, tā vēsturisko dinamiku un nepieciešamajiem attīstības virzieniem.
- Starp kiberdrošības ekspertiem un uzņēmumu vadītājiem, pastāv atšķirīga izpratne par kiberdrošības draudiem un uzņēmuma spējām, šo draudu pārvaldīšanā.

KĀPĒC VEIKT BRIEDUMA NOVĒRTĒJUMU JEB KO IEGŪST UZŅĒMUMS?

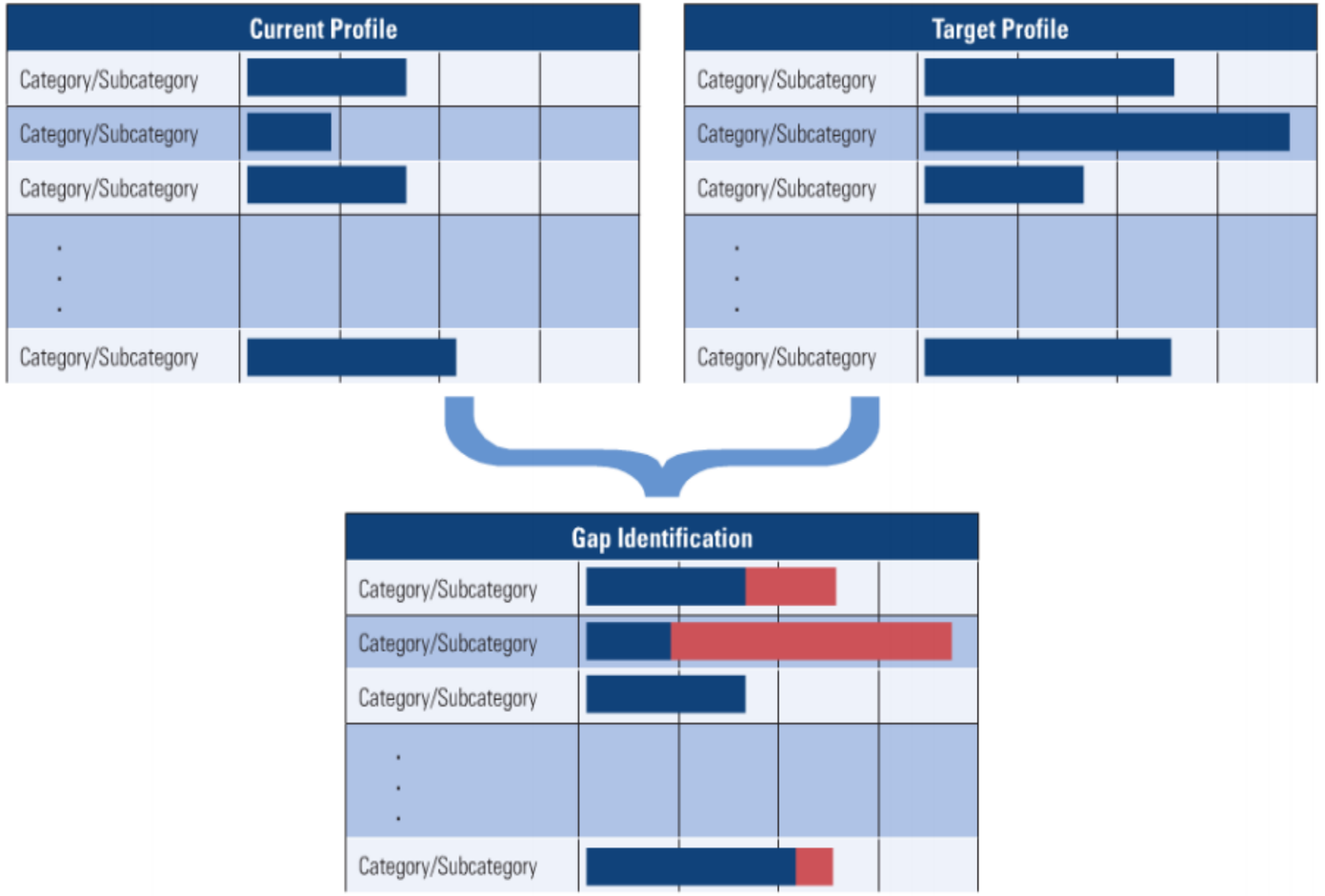
- Kādā stāvoklī ir uzņēmuma kiberdrošība šobrīd?
- Kādi ir nepieciešamie uzlabojumi un turpmākā attīstība?
- Vai kiberdrošības pārvaldībā notiek attīstība?
- Vai esošie kiberdrošības pārvaldības procesi nodrošina, drošības mērķu sasniegšanu?
- Iespēja sarunāties ar iekšējiem partneriem saprotamā valodā!
- Kāda ir uzņēmumā esošā kiberdrošības pārvaldība, salīdzinājumā ar konkurentiem?

NIST KIBERDROŠĪBAS IETVARS
(FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY)

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

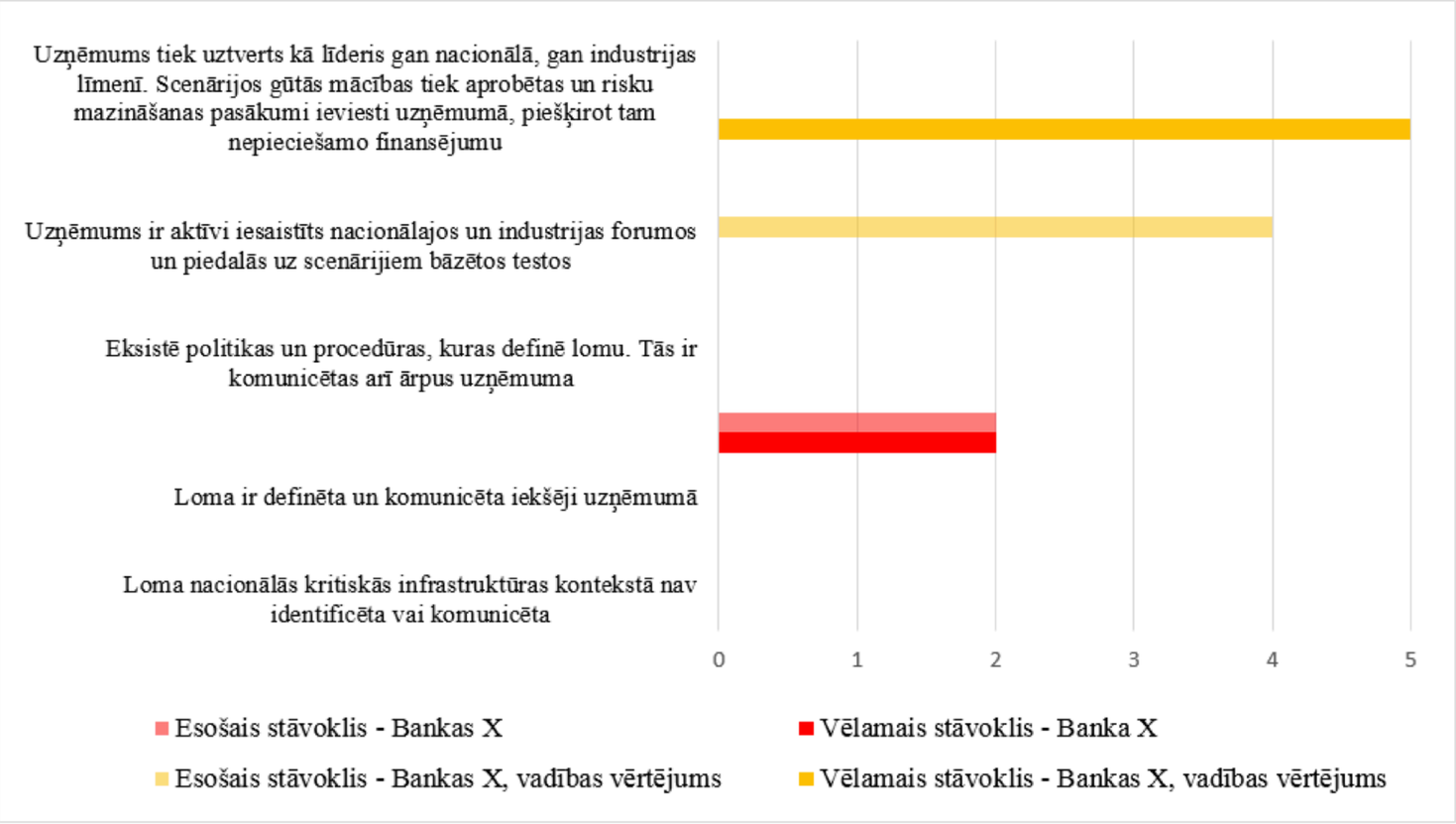
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

NIST KIBERDROŠĪBAS IETVARS
(FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY)



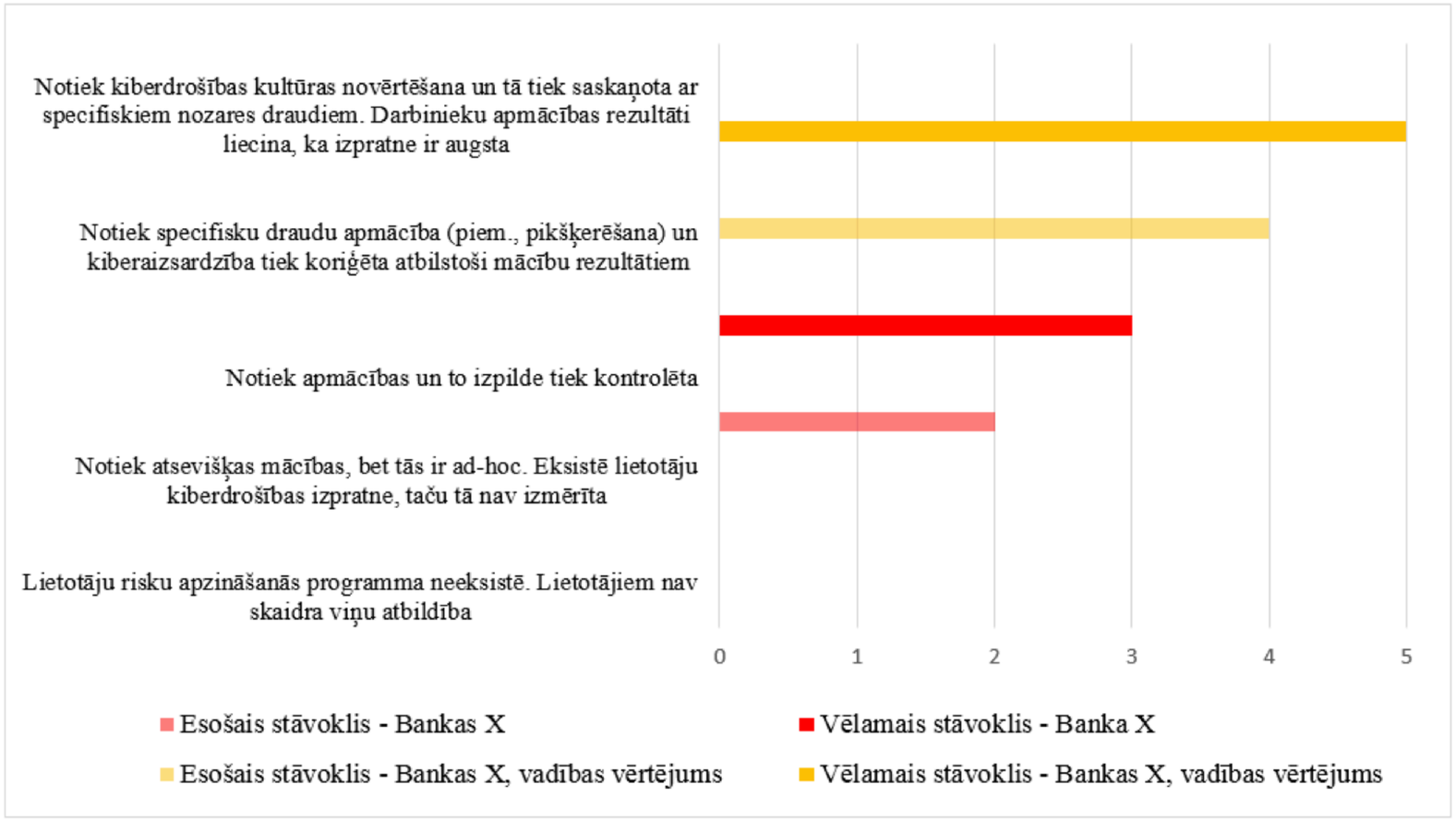
KIBERDROŠĪBAS EKSPERTIEM TRŪKST ZINĀŠANAS UN IZPRATNES PAR UZŅĒMUMA LOMU VALSTS KRITISKĀS INFRASTRUKTŪRAS UN FINANŠU STABILITĀTES NODROŠINĀŠANĀ

Uzņēmuma loma kritiskajā infrastruktūrā ir identificēta un komunicēta:

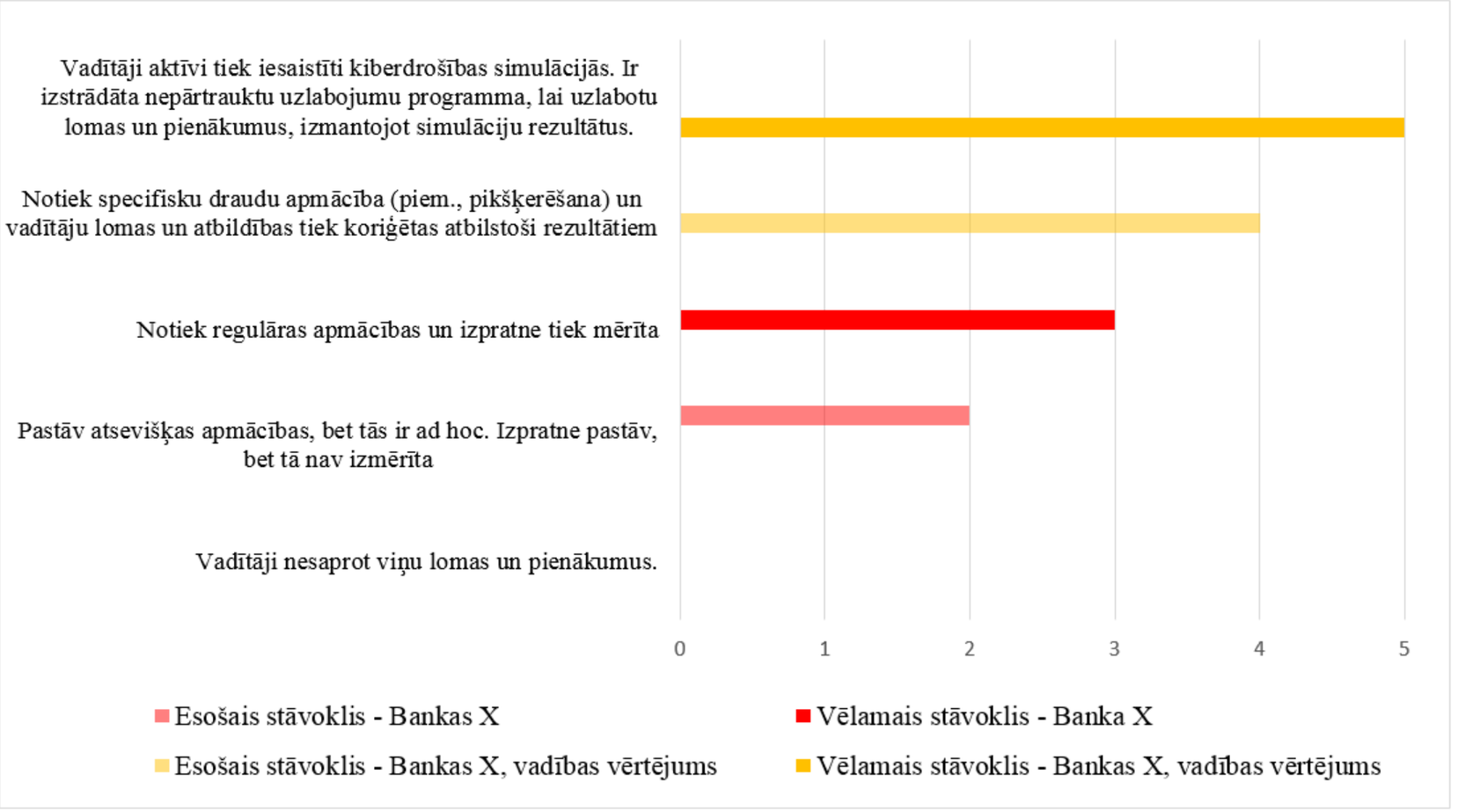


KIBERDROŠĪBAS EKSPERTU UN UZŅĒMUMA VADĪBAS VĒRTĒJUMOS IR BŪTISKAS ATŠĶIRĪBAS UN PRETRUNAS, KURAS LIECINA PAR SAVSTARPĒJU KOMUNIKĀCIJAS TRŪKUMU

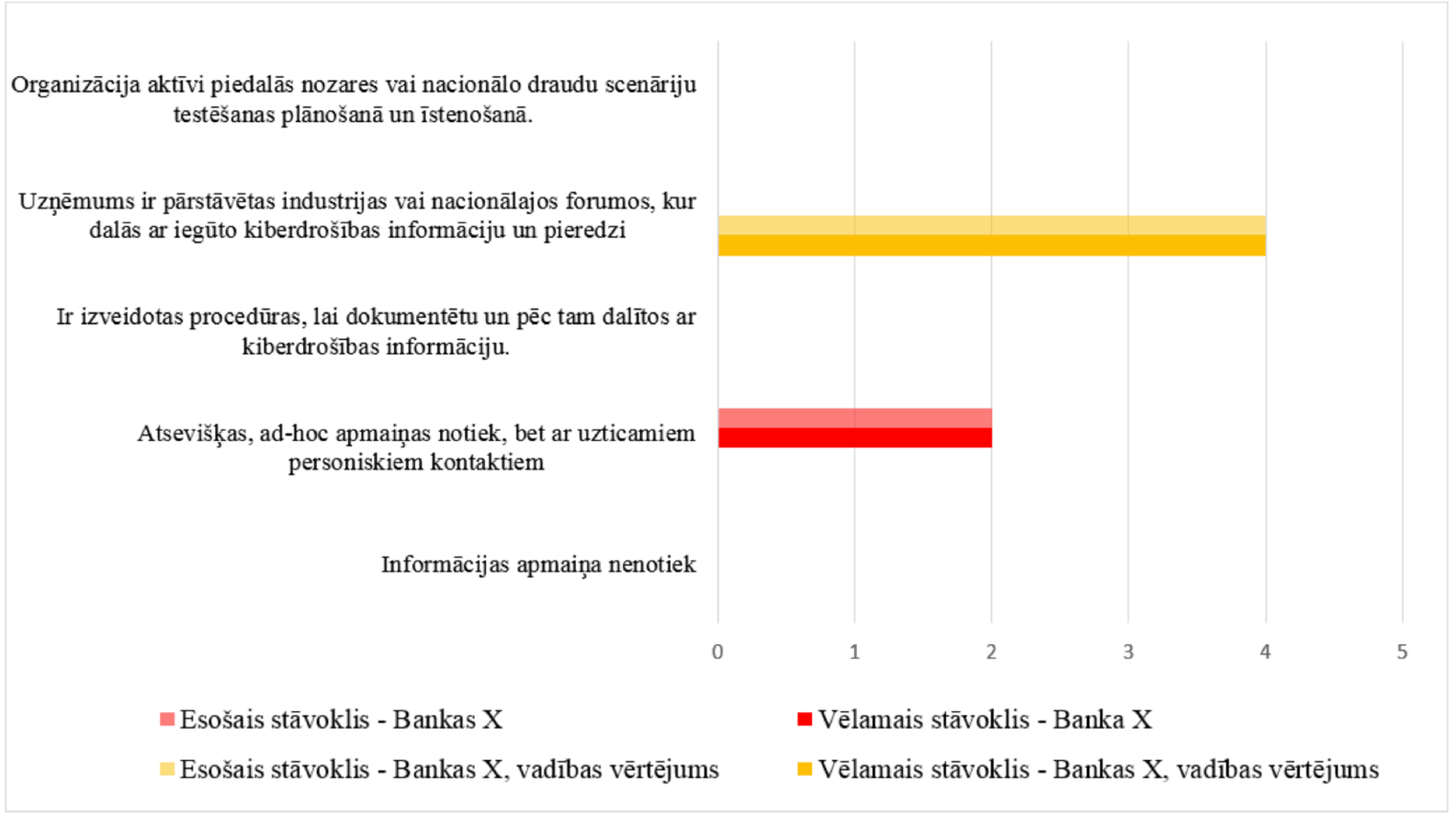
Visi lietotāji ir informēti un apmācīti:



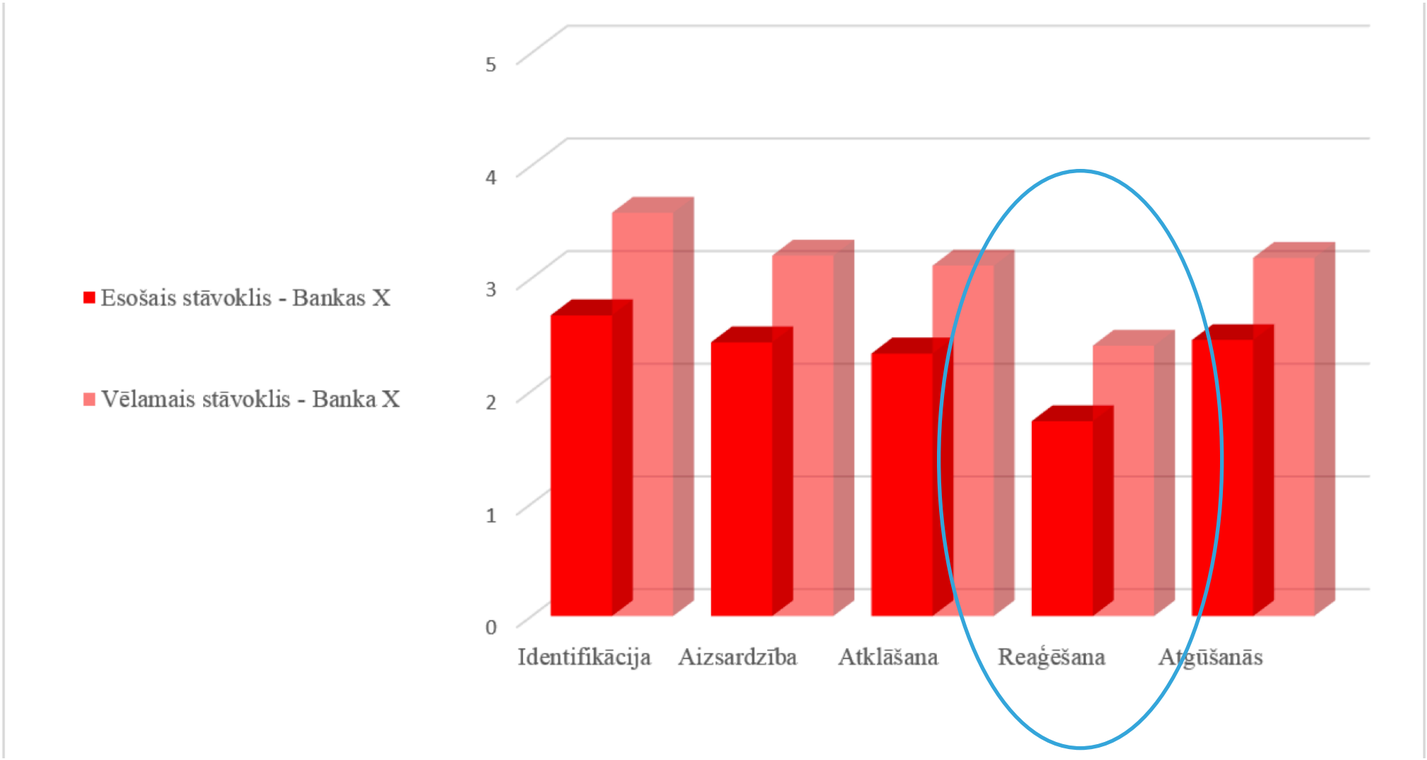
Uzņēmuma vadība saprot lomas un pienākumus:



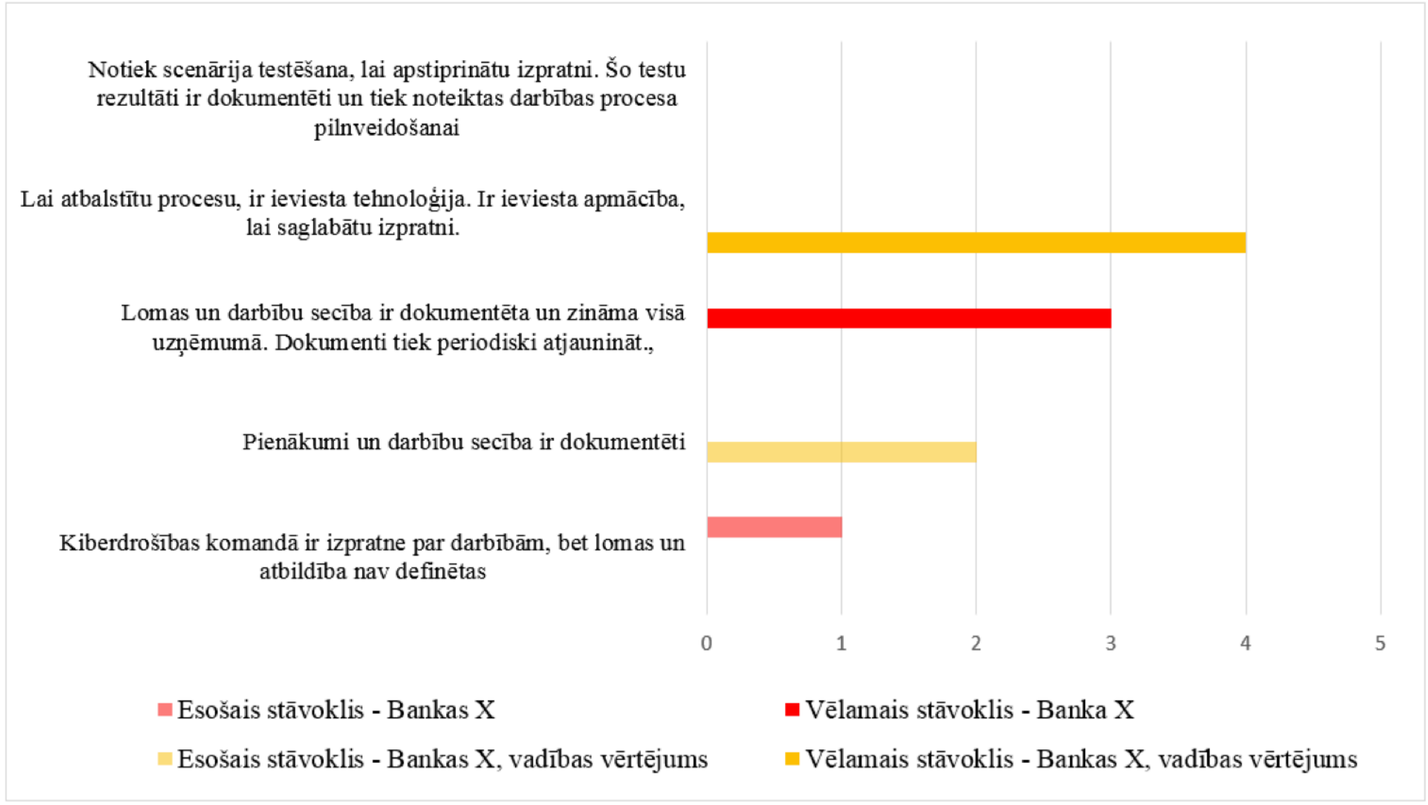
Notiek brīvprātīga informācijas apmaiņa ar ārējām ieinteresētajām personām:



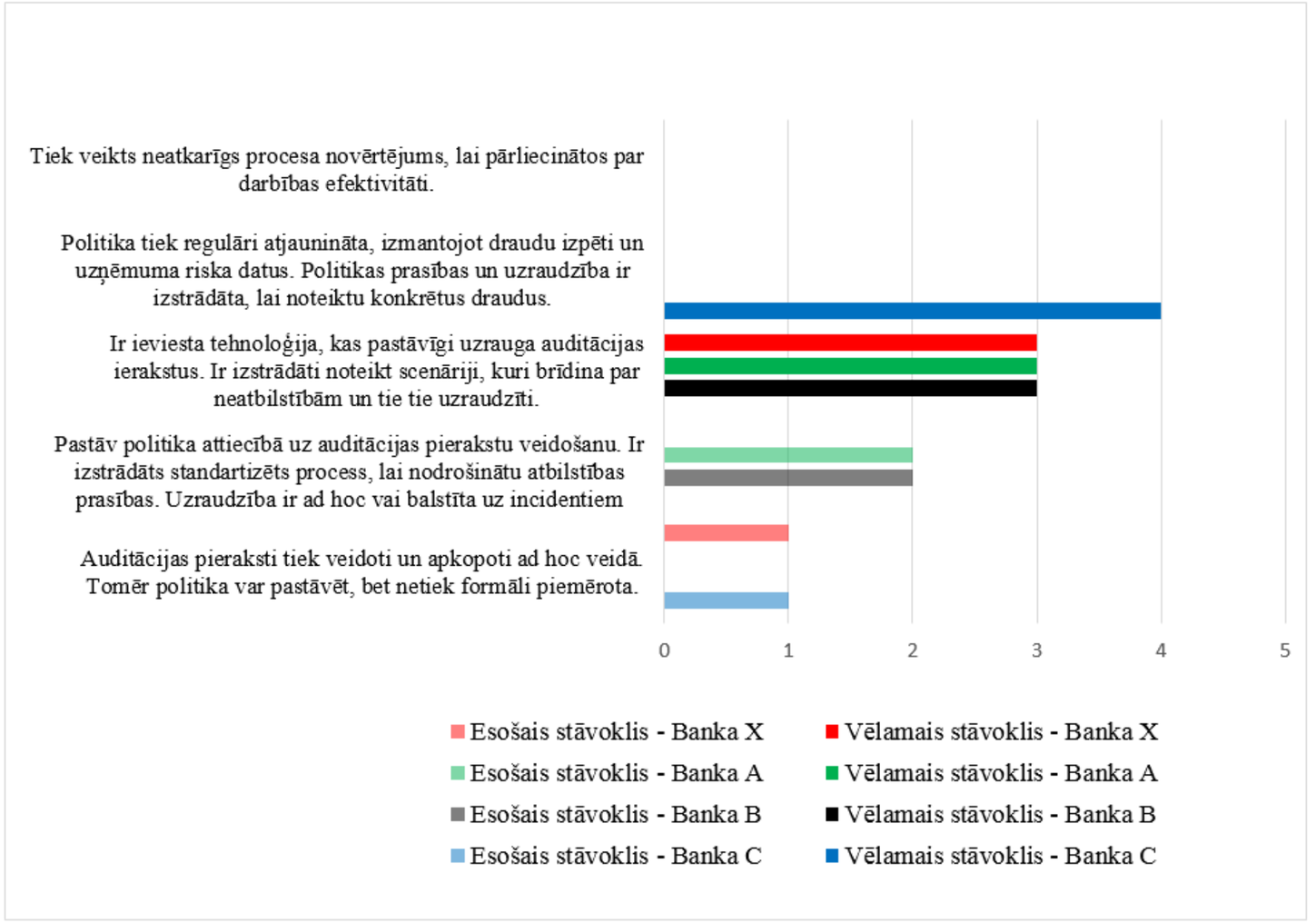
REAĢĒŠANAS FUNKCIJAS ZEMAIS NOVĒRTĒJUMS, LIECINA PAR NEPIETIEKAMU UN ATBILSTOŠU REAĢĒŠANAS SPĒJU TRŪKUMU



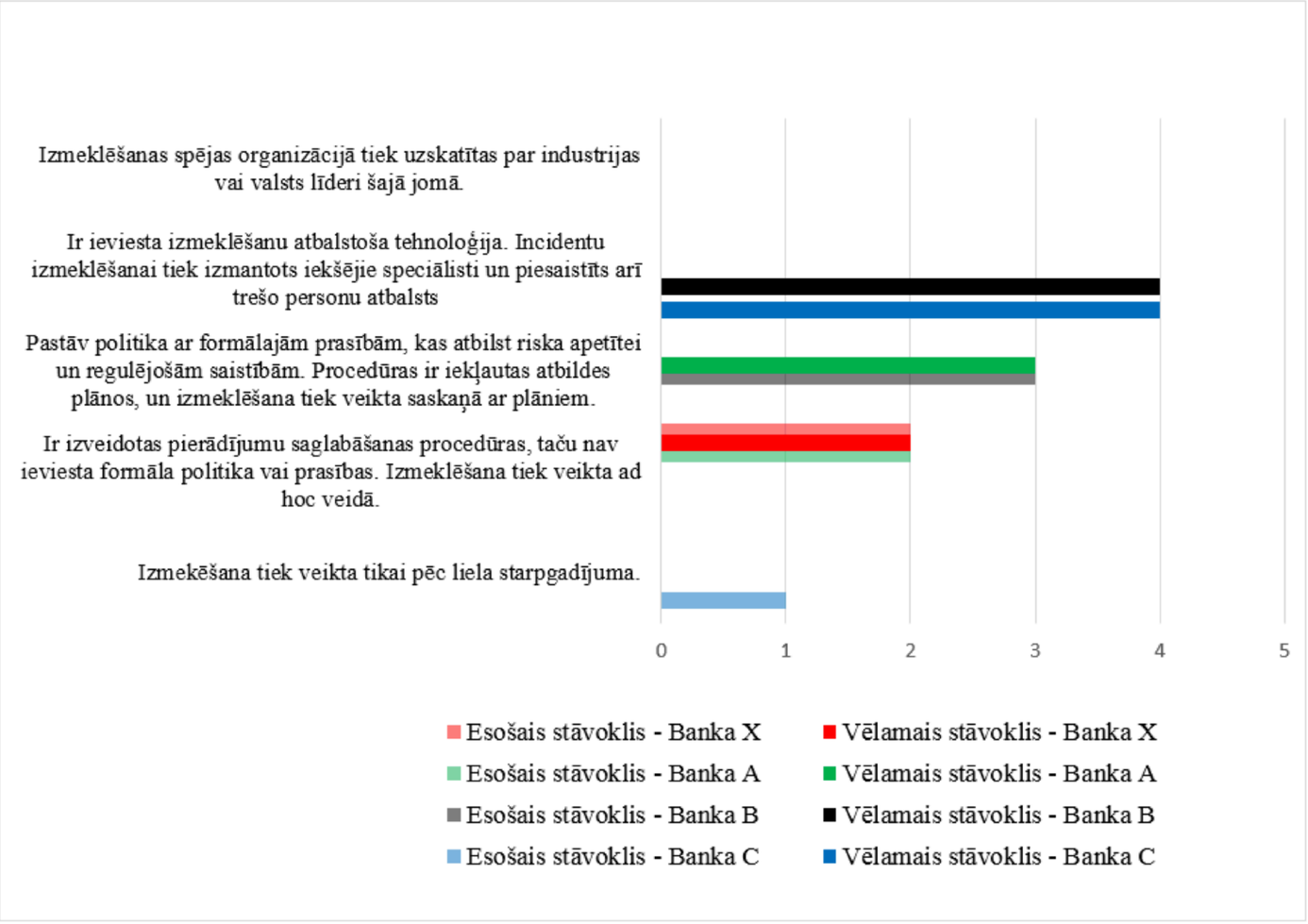
Personāls zina savu lomu un darbības, ja nepieciešams veikt reaģēšanas vai atbildes darbības:



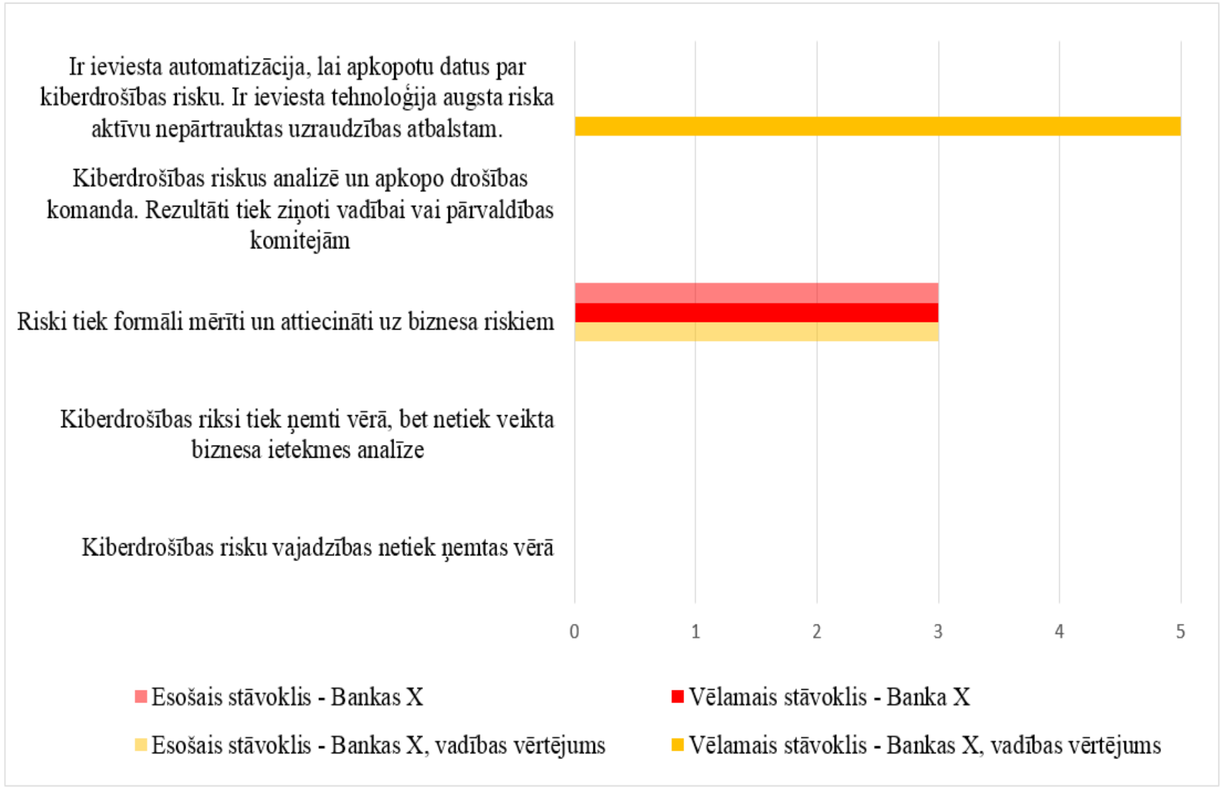
Auditācijas žurnāla ieraksti ir noteikti, dokumentēti, īstenoti un pārskatīti saskaņā ar politiku

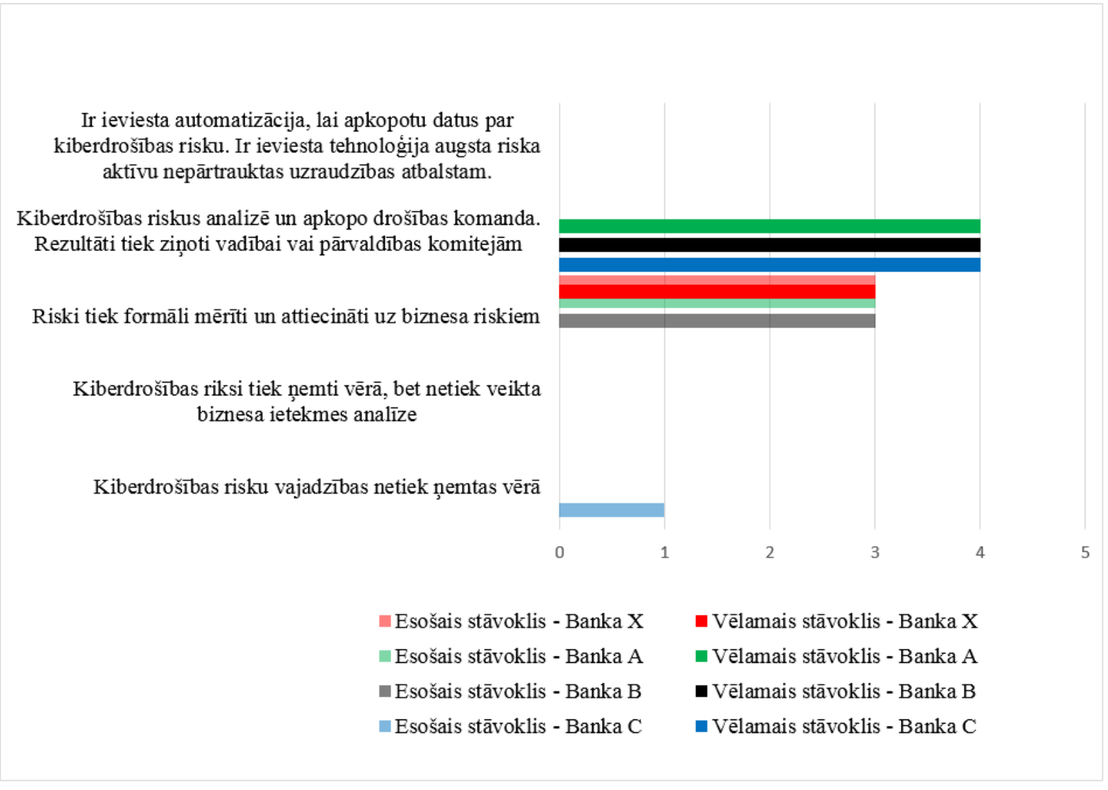


Tiek veikta incidenta izmeklēšana (ekspertīze):

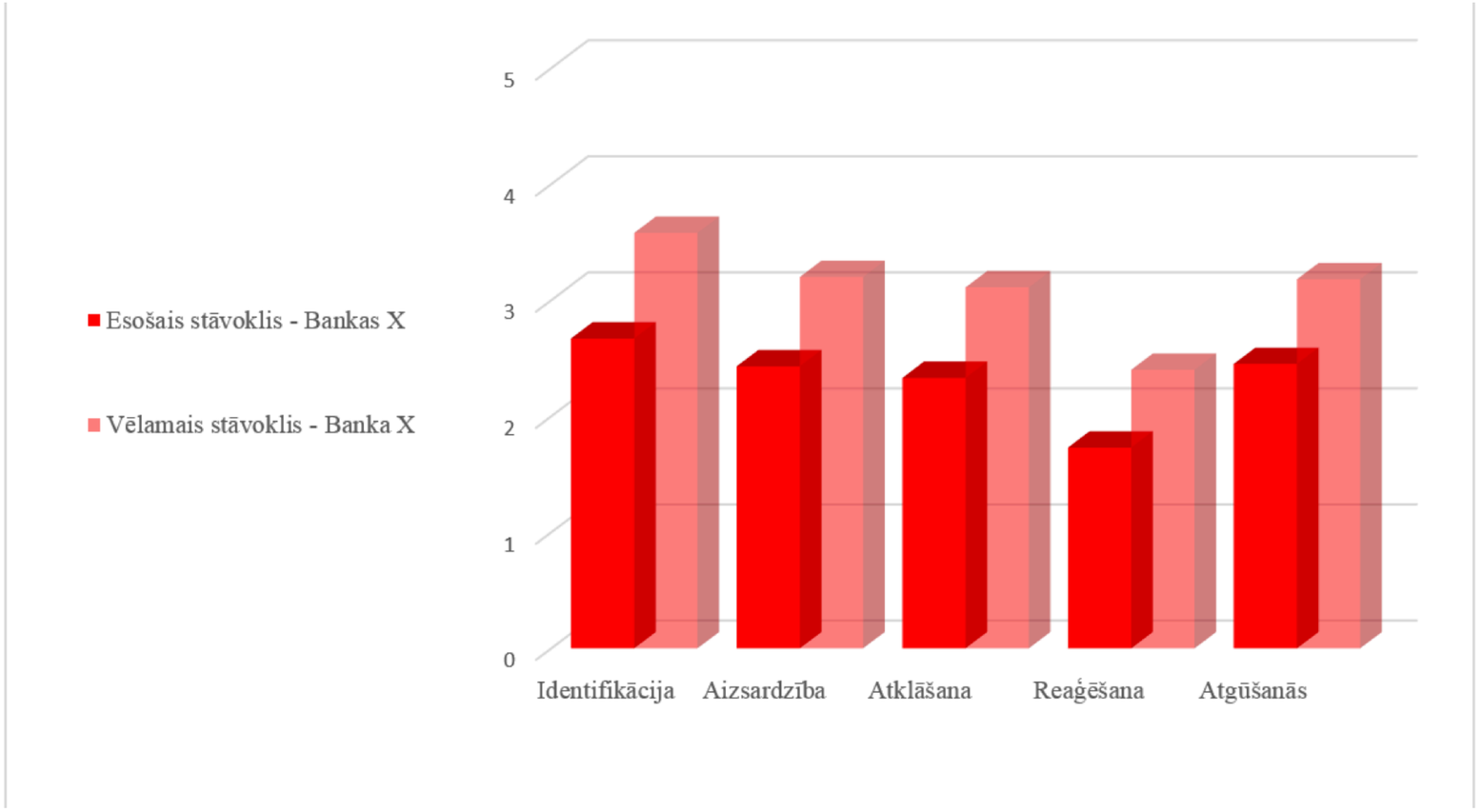


Risku vadības procesā tiek apzinātas un atbalstītas kiberdrošības risku vajadzības:

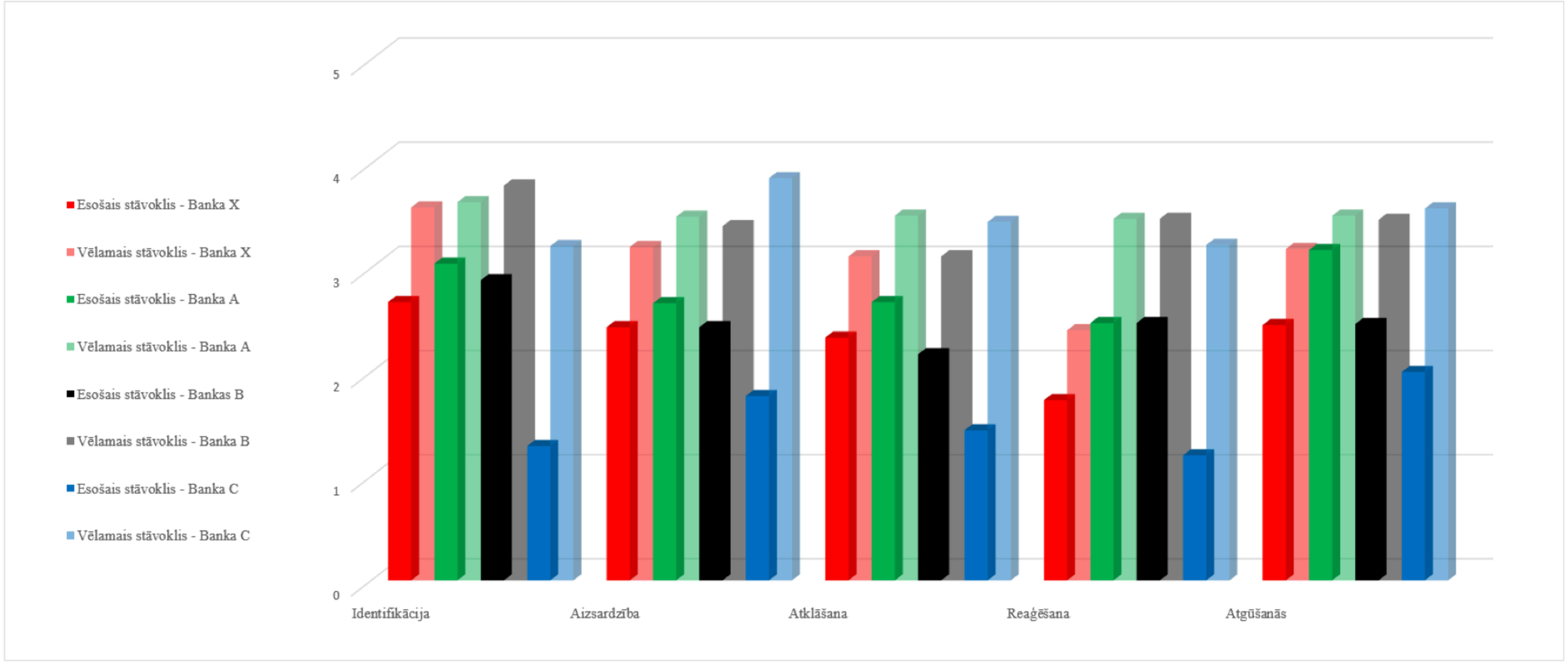




NELIELĀS ATŠĶIRĪBAS STARP ESOŠO UN VĒLAMO BRIEDUMA STĀVOKLI, LIECINA PAR DISKUSIJAS TRŪKUMU UN KONCENTRĒŠANOS UZ ATBILSTĪBAS PRASĪBU NODROŠINĀŠANU



KIBERDROŠĪBAS BRIEDUMS BANKĀS “X”, “A”, “B”, “C” UN IESPĒJAMS VISĀ SEKTORĀ, IR LĪDZĪGS



NEPIECIEŠAMIE ATTĪSTĪBAS VIRZIENI

- Jāpilnveido sadarbība starp banku kiberdrošības ekspertiem, uzņēmuma vadību un biznesa procesu veidotājiem.
- Jāuzlabo Bankas reaģēšanas spējas, izstrādājot un attīstot atbildes darbību plānu, kā arī definējot darbinieku lomas un pienākumus.
- Bankām nepieciešams definēt kiberdrošības vietu un lomu to uzņēmējdarbībā, skaidri nosakot, vai mērķis ir atbilstība regulējošajām prasībām, vai sistemātiska un efektīva kiberdrošības risku pārvaldība.
- Kiberdrošības izpratnes, apzināšanās un brieduma veicināšanai, ir nepieciešams veikt regulāras, uz nozares specifiskiem riskiem balstītas apmācības, turklāt to rezultātus ne tikai izmantojot aizsardzības koriģēšanai, bet arī komunikācijai darbiniekiem.
- Kiberdrošības brieduma diskusiju nepieciešams attīstīt ne tikai atsevišķas bankas iekšienē, bet valsts un sektora līmenī, veicinot izpratni par sektora lomu valsts kritiskās infrastruktūras un finanšu sistēmas stabilitātes kontekstā.
- Kiberdrošības brieduma novērtējumu, nepieciešams veikt ar noteiktu regularitāti, tādējādi iegūstot kvalitatīvus un salīdzināmus datus, objektīvai esošā stāvokļa, sasniegtā progresa un veicamo korekciju novērtēšanai.
- Kiberdrošības brieduma novērtēšanas procesā ir jāpiedalās ne tikai kiberdrošības ekspertiem, bet arī uzņēmuma vadībai, biznesa procesu īpašniekiem, personāla vadītājiem un komunikācijas speciālistiem.

FINANŠU NOZARES ASOCIĀCIJA

PALDIES!

JAUTĀJUMI?

ATSAUCES

- Mustard S.(2014), “NIST Cybersecurity Framework Aims to Improve Critical Infrastructure”, pieejams: http://www.powermag.com/nist-cybersecurity-framework-aims-to-improve-critical-infrastructure/?pagenum=1

- NIST (2018), Version 1.1. “Framework for Improving Critical Infrastructure Cybersecurity”, pieejams: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- https://nistmaturity.com/