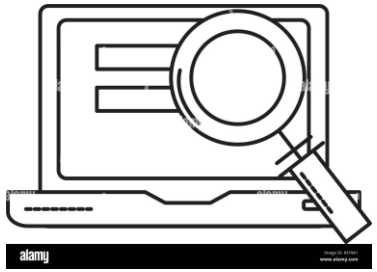
Finanšu ministrija

# IKT DROŠĪBAS AUDITS: *no dokumentiem līdz realitātei*

## Prioritārā audita starprezultātu prezentācija



**Dace Bērziņa-Ķule**
Iekšējā audita departamenta vecākā eksperte
Finanšu ministrija

2025.gada 10.decembrī

Finanšu ministrija

# KĀPĒC ŠIS AUDITS IR SVARĪGS?
## *(un ko realitāte saka priekšā jau šodien)*

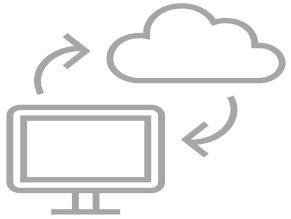
**📌 Audits kā prioritāte (2024–2025)**
• IKT drošības pārvaldības audits noteikts kā valsts pārvaldes prioritārs uzdevums, pamatojoties uz MK 20.03.2024. rīkojumu Nr. 188 "Par kopējām valsts pārvaldē auditējamām prioritātēm 2024. un 2025. gadam".
• Audits īstenots saskaņā ar "IKT drošības pārvaldības iekšējā audita veikšanas vadlīnijām", kas izstrādātas, balstoties uz minēto MK rīkojumu.
• Mērķis – iegūt reālu kopainu, nevis tikai dokumentos atspoguļoto situāciju.

**📘 Vadlīnijas un labā prakse**
• Finanšu ministrijas koordinētās vadlīnijas nosaka vienotu audita ietvaru.
• Novērtējums balstīts uz: spēkā esošiem normatīvajiem aktiem, labās prakses principiem (t.sk. ISO 27001), un topošajām Nacionālās kiberdrošības likuma prasībām.
• Vadlīnijas palīdz "vienā valodā" novērtēt 16 IKT drošības jomas.

**📚 Šobrīd – starprezultāti no 35 iestādēm (tendences, ne gala aina)**
• Galīgie rezultāti būs līdz 2026. gada 31. janvārim.
• Šobrīd analizēti 35 iestāžu starprezultāti, kas atklāj kopējo situāciju un risku tendences.
• Jau tagad redzamas skaidras likumsakarības un "kopīgās sāpes".

Finanšu ministrija

# KO AUDITS ATKLĀJA KOPSKATĀ?
## (*pirmās tendences no 35 iestādēm – pirms detalizētajām 16 jomām*)



*Dokumentos viss izskatās kārtībā – audits parāda, kā ir realitātē.*

🔍 **Prakse bieži atšķiras no dokumentiem.**
*Dokumentācija nereti ir sakārtota, bet īstenošana ikdienā – fragmentāra.*

🧭 **Drošības pārvaldība nav vienmērīga.**
*Atbildības sadalījums un procesu briedums būtiski svārstās starp iestādēm*

🔐 **Piekļuves un lietotāju kontrole ir vājākā joma.**
*MFA, paroļu politika un kontu pārskatīšana joprojām ir galvenie riski.*

📘 **Apmācību un zināšanu pārbaudes nav pietiekamas.**
*Kiberdrošības kultūra veidojas nevienmērīgi.*

🛠 **Infrastruktūra un IS dzīves cikla pārvaldība nav konsekventa.**
*Nav vienotu kārtību, dokumentācija nav pilnīga, MDM netiek plaši izmantots*

⚠️ **Noturība pret incidentiem un krīzēm – nepietiekama.**
*Procesi nav pilnībā definēti vai testēti.*

Finanšu ministrija

# DROŠĪBAS PĀRVALDĪBAS PAMATI

## *(no dokumentiem uz realitāti – ko audits parādīja?)*

*Papīros atbildīgie ir, bet audits parāda – vai viņi ir arī realitātē.*

### 🧭 Organizatoriskā vide

❗ Atbildības sadalījums nav viennozīmīgs; dokumentācija novecojusi.

✅ Sakārtotas lomas un aktualizēti pienākumi stiprina drošības kultūru.

### ⚙️ Vadības procesi

❗ Trūkst regulāru pārbaužu un risku novērtēšanas.

✅ Proaktīva uzraudzība ļauj savlaicīgi identificēt un mazināt riskus.

### 🎓 Apmācības un zināšanas

❗ Apmācības notiek neregulāri; nav zināšanu pārbaudēs balstītas kontroles.

✅ Regulāras apmācības veicina kiberdrošības briedumu un IKS efektivitāti.

❗ Galvenais novērojums ✅ Ieguvums

Finanšu ministrija

# RESURSU UN SISTĒMU PĀRVALDĪBA
## *(no sistēmām līdz cilvēkiem – kur slēpjas riski?)*

*Tīkls bez dokumentācijas ir kā ēka bez plāna – stāv, bet neviens nezina, kas īsti kur ved.*

### 🔄 Informācijas sistēmu dzīves cikls

❗ Nav vienotas kārtības izstrādei, uzturēšanai un izmaiņu veikšanai.

✅ Strukturēta kārtība nodrošina kvalitāti, ilgtspēju un risku kontroli.

### 🧩 Lietotāju un piekļuves pārvaldība

❗ MFA netiek izmantota; paroles vājas; kontu pārskatīšana – neregulāra.

✅ Stingra piekļuves kontrole samazina nesankcionētas piekļuves riskus.

### 🖧 Tehniskā infrastruktūra

❗ Tīkla arhitektūras dokumentācija ir nepilnīga un nevienmērīga.

✅ Skaidra infrastruktūras pārvaldība uzlabo drošību un incidentu reakcijas ātrumu.

❗ Galvenais novērojums ✅ Ieguvums

Finanšu ministrija

# DATU DROŠĪBA UN PIEEJAMĪBA

## (*kur rodas vājās vietas, un kādi ir ieguvumi tās novēršot?*)

*Attālinātais darbs ir drošs tikai tad, ja drošība nav attālināta.*

### ☁️ Mākoņdatošana

❗ Nav noteiktu drošības prasību pakalpojumu sniedzējiem.

✅ Skaidri kritēriji nodrošina drošu un kontrolējamu ārpakalpojumu izmantošanu.

### 💻 Portatīvās iekārtas

❗ Nav MDM; datu šifrēšana nav obligāta.

✅ Centralizēta pārvaldība un šifrēšana aizsargā datus arī ārpus iestādes tīkla.

### 🏠 Attālinātais darbs

❗ MFA netiek izmantota; trūkst drošas darba vides prasību.

✅ Droša attālinātā piekļuve aizsargā datus un nodrošina elastīgu darbu.

### 🔧 Atjauninājumu vadība

❗ Nav vienotas, dokumentētas kārtības sistēmu atjaunināšanai.

✅ Regulāri atjauninājumi mazina ievainojamības un uzlabo stabilitāti

❗ Galvenais novērojums ✅ Ieguvums

Finanšu ministrija

# NOTURĪBA UN KRĪŽU VADĪBA
## *(kas notiek, kad notiek neparedzamais?)*

*Krīzes plāns, kas nav testēts, nav plāns – ir tikai optimisma vingrinājums.*

| Joma | ❗ Galvenais novērojums | ✅ Ieguvums |
|---|---|---|
| 🧠 **Ievainojamības pārvaldība** | Nav regulāru drošības testu, ievainojamību skenējumu vai izvērtējumu. | Savlaicīga risku identificēšana un mazāk "pārsteigumu". |
| 🚨 **Incidentu vadība** | Nav vienotas incidentu vadības kārtības; lomas un atbildības nav skaidri noteiktas. | Ātra, koordinēta reakcija un mazāks ietekmes apjoms. |
| 🔐 **Datu drošība** | Nav pilnīgas šifrēšanas un rezerves testu. | Uzticama datu aizsardzība. |
| ♻️ **Nepārtrauktība** | Plāni nav testēti, rezerves kopijas netiek regulāri pārbaudītas. | Stabilitāte un ātra atjaunošanās. |
| 🛡️ **Krīžu vadība** | Nav pārbaudītu scenāriju. | Gatavība un noturība krīzēs. |

Finanšu ministrija

# KO NOZĪMĒ ŠIE TRŪKUMI?
## *(kā lasīt audita rezultātus)*

*Iekšējais audits nav kontrole, bet ieguldījums – ceļš uz drošāku un pārdomātāku vidi.*

**Audits nav "atradumu saraksts" – tas ir rīcības ceļvedis.**
**Rezultāti atklāj sistēmiskas nepilnības, kas lielākoties ir risināmas ar pārvaldības izmaiņām, nevis ar dārgiem tehniskiem risinājumiem.**

**Trūkumi ir līdzīgi visās iestādēs.**

**Tie nav "nejauši gadījumi", bet norāda uz kopīgu pārvaldības brieduma līmeni.**

**Risinājumi ir zināmi un praktiski īstenojami.**

**Daudzi uzlabojumi balstās dokumentācijas sakārtošanā, procesu formalizēšanā un atbildību precizēšanā.**

**Mazas izmaiņas rada lielu efektu.**

**Vienots MFA, centralizēta MDM ieviešana, regulāras pārbaudes → būtisks drošības līmeņa lēciens.**

Finanšu ministrija

# KO DARĪT TĀLĀK?

*Trūkumi ir zināmi – un risinājumi ir vienkārši. Galvenais ir sākt ar pamatiem.*

## 1 Sakārtot drošības procesus

Atbildības, riska vadība, dokumentācijas aktualizēšana.
"Procesi vispirms – tehnoloģijas pēc tam."

## 2 Nostiprināt piekļuves un datu drošību

MFA, paroles, piekļuves pārskatīšana, šifrēšana, rezerves kopijas.

## 3 Regulāras apmācības un pārbaudes

Kiberdrošība nav vienreizēja aktivitāte – tā ir kultūra.

## 4 Testēt nepārtrauktību

"Krīzes plāns, kas nav testēts, ir tikai drukāts optimisms."

Finanšu ministrija

# Paldies par uzmanību!

***"Un atcerēsimies – drošība sākas ar izpratni.***
***Drošība nav projekts, tā ir disciplīna.***
***Audits palīdz to iegūt un nostiprināt."***

Dace Bērziņa-Ķule
FM iekšējā audita departaments
E-pasts: dace.berzina-kule@fm.gov.lv