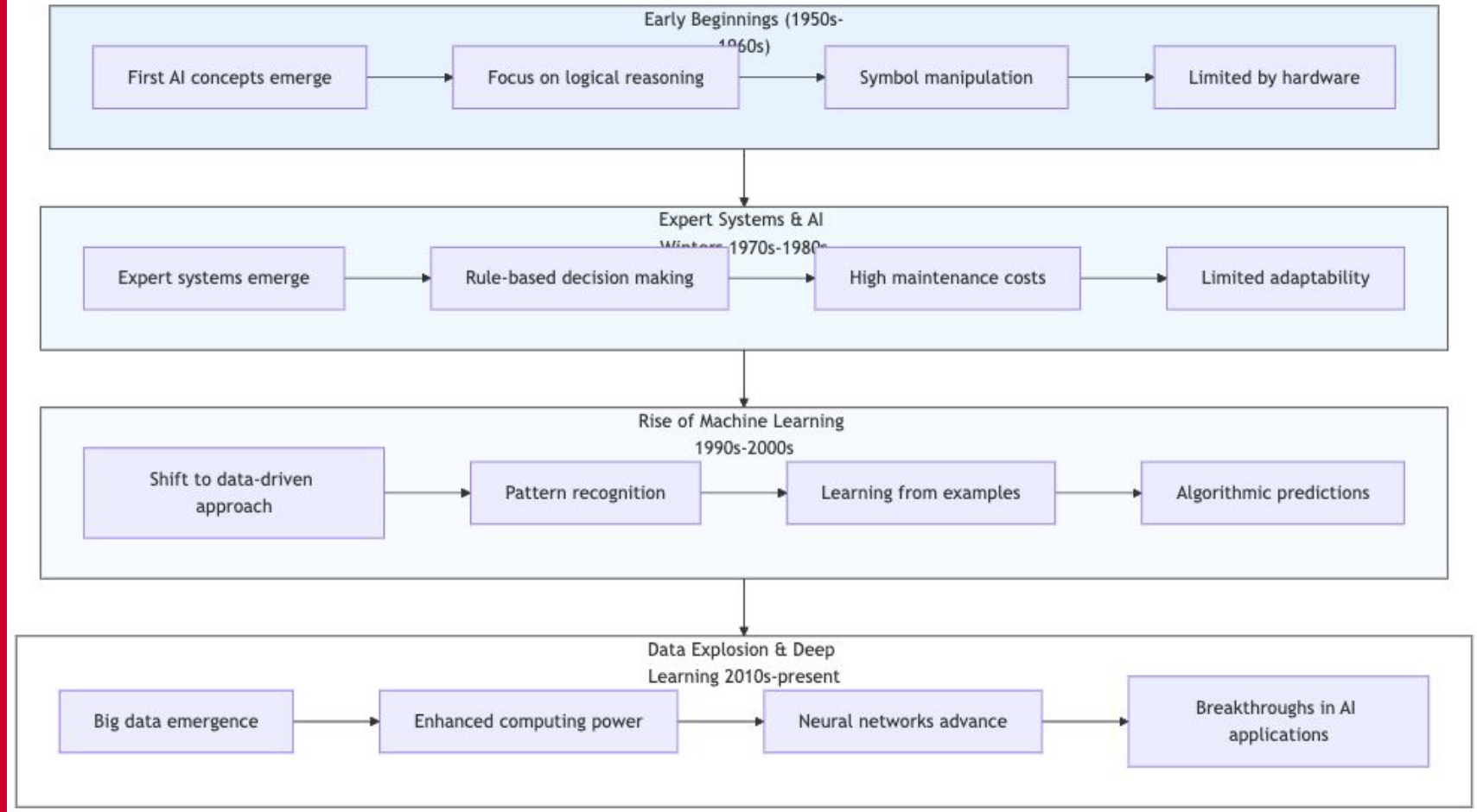
Vai MI padara mūsu drošību gudrāku: praktiski piemēri un “grābekļi” auditos

JURIS PŪCE
PEAK DEFENCE
Smart Strong Security³

v.1.1 2024.12.11

Mazi meli, Lieli Meli, Statistika..


Early Beginnings (1950s-1960s)
First AI concepts emerge
Focus on logical reasoning
Symbol manipulation
Limited by hardware
Expert Systems & AI Winters 1970s-1980s
Expert systems emerge
Rule-based decision making
High maintenance costs
Limited adaptability
Rise of Machine Learning 1990s-2000s
Shift to data-driven approach
Pattern recognition
Learning from examples
Algorithmic predictions
Data Explosion & Deep Learning 2010s-present
Big data emergence
Enhanced computing power
Neural networks advance
Breakthroughs in AI applications

Juris Pūce

PEAK DEFENCE (partner)
KleinTech Services (founder -> 2021)
Vidzemes Augstskola (digital law lecturer)
PECB (trainer since 2008)
Member of Advisory board for AI policy for NATO (2022)


IMPLEMENT
(IEVIEST)
OPERATE
(DARBINĀT)
ANALYSE
(ANALIZĒT)


EU
EU REGULATES,
U.S. INNOVATES..

LLM pielietošana “kāds tas ir”

[redacted]

to birojs

If you can't read this email, click here

Welcome!

If you want to expand Your circle of contacts, as well as develop the business, join [redacted] web for companies - Business Network! It is a unique platform that has just launched, but has already registered more than 700 companies - Your potential customers and partners.

Find out more about the opportunities in the latest edition of "Your Business" here.

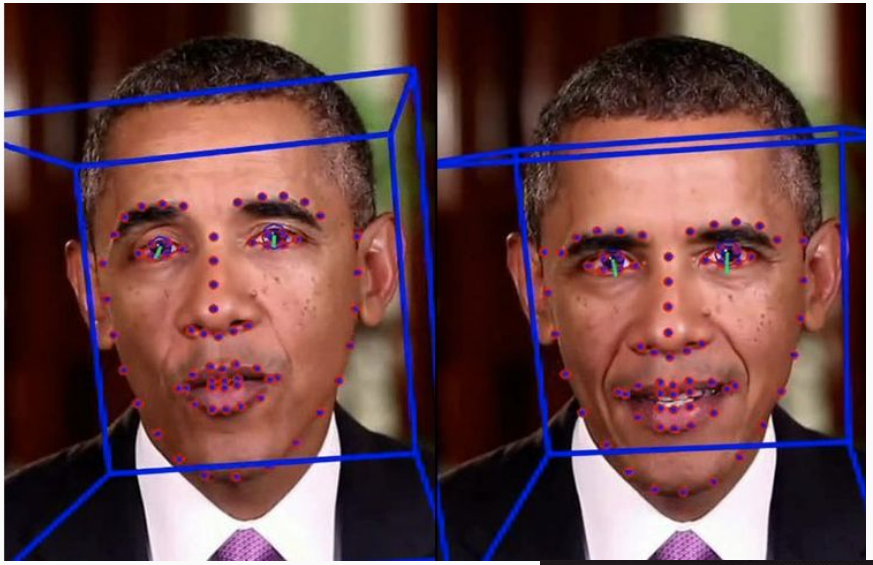
Some more topics in the issue:

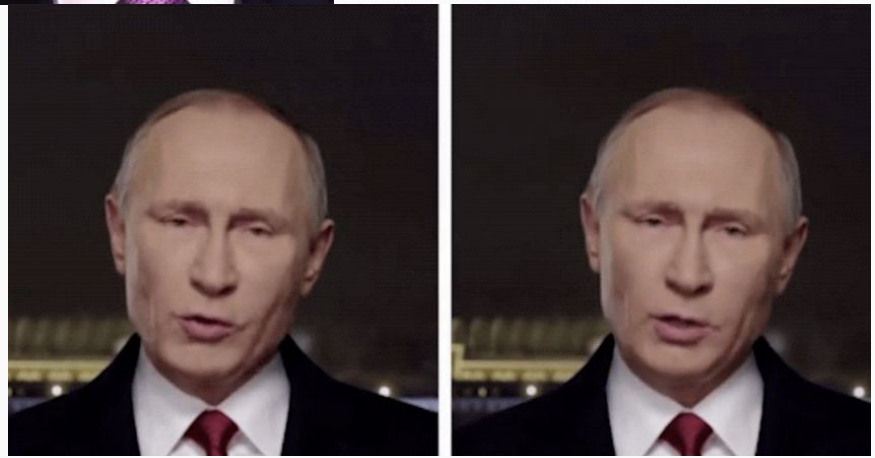
- **Entrepreneurs Competence Center: assistant and advisor to Latvian entrepreneurs**
- **Your company's financial advisor [redacted] - get professional reporting of Your finances!**

We hope you find this edition really useful for the development of Your company!

Your [redacted]

[redacted]





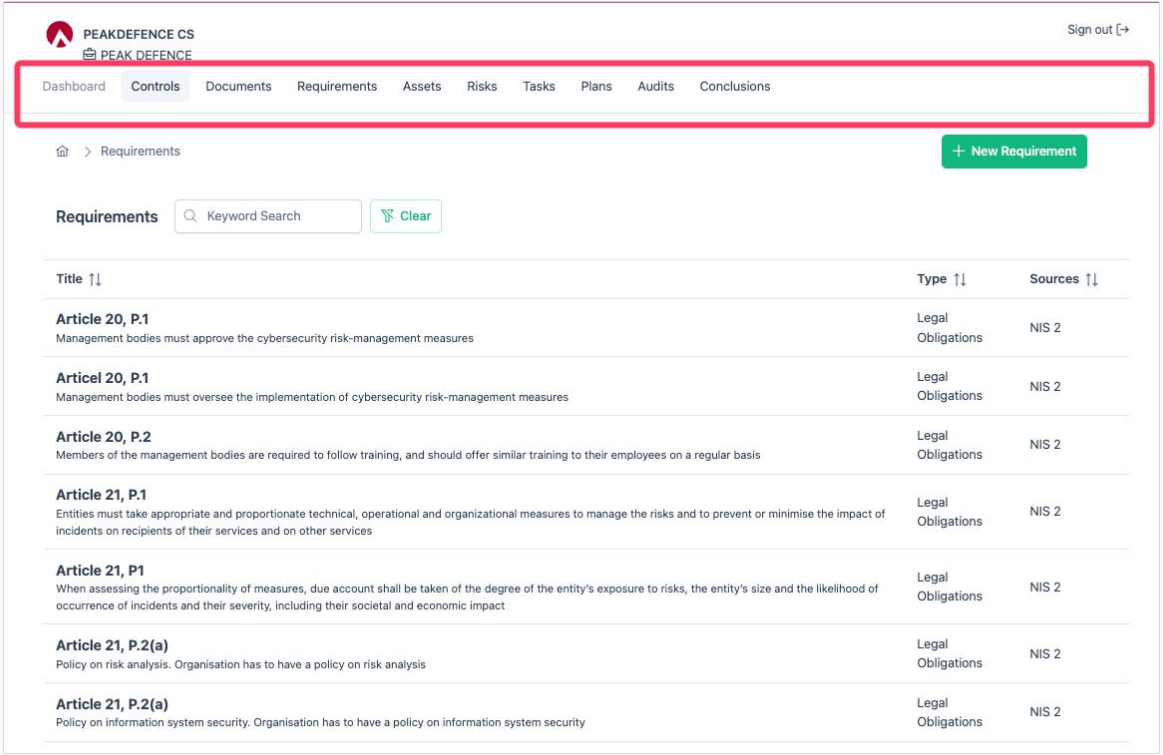

Claude
Untitled
Izveido man informācijas drošības politiku, kas atbilst NIS 2 direktīvas prasībām?

Secinājumi

- LLM ir lielisks, lai “mācītos” kādu tēmu
- Noteiktās jomās mēs šīs izmaiņas neapturēsim
- Tomēr esošie pielietojumi maz saprot “kontekstu” un nevajag tos pārvērtēt
- Drošībā “pareizie dokumenti” ir 10%

PRAKSE…

KIBERDROŠĪBAS DATU MODELIS



IMPLEMENT (IEVIEST)

- Sākotnējais gatavības novērtējums (NIS 2, DORA, ISO 27001, SOC 2...)

- DOKUMENTU IZVEIDE
- UZDEVUMI
- AWARENESS (INFORMĒTĪBA)

OPERATE (DARBINĀT)

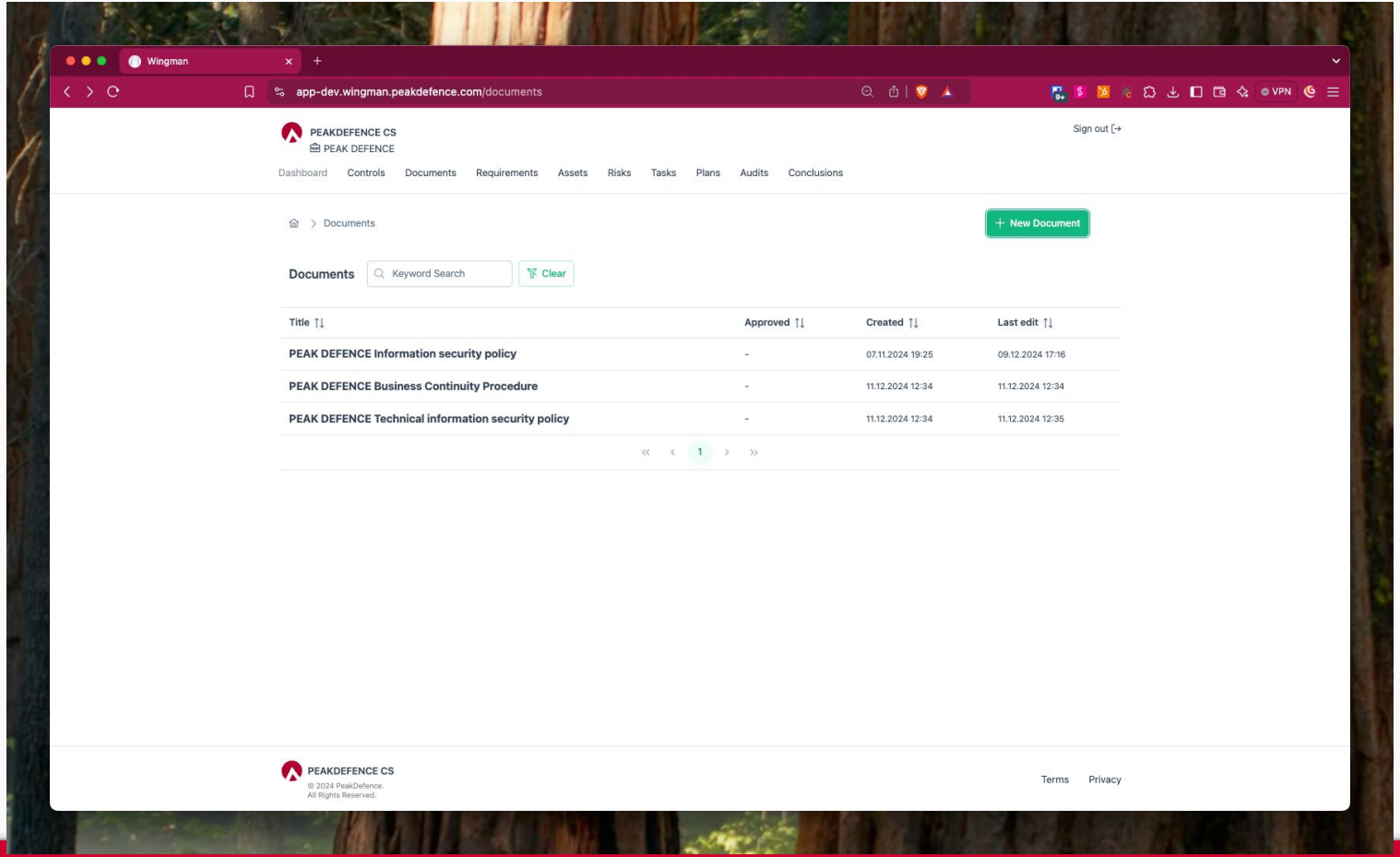
- Jautājumu apstrāde (Teams, Slack, u.c.)
- Piltuve un Prioritizācija
  - Drošības notikumi
  - Ievainojamību ziņojumi
  - Apdraudējumu ziņojumi
  - “Near miss”
  - Incidenti
- Izmaiņas kontrolēs
- Regulārie uzdevumi
  - Resursu reģistrs
  - Risku reģistrs
  - Piekļuves kontroles...

ANALYSE (ANALIZĒT)

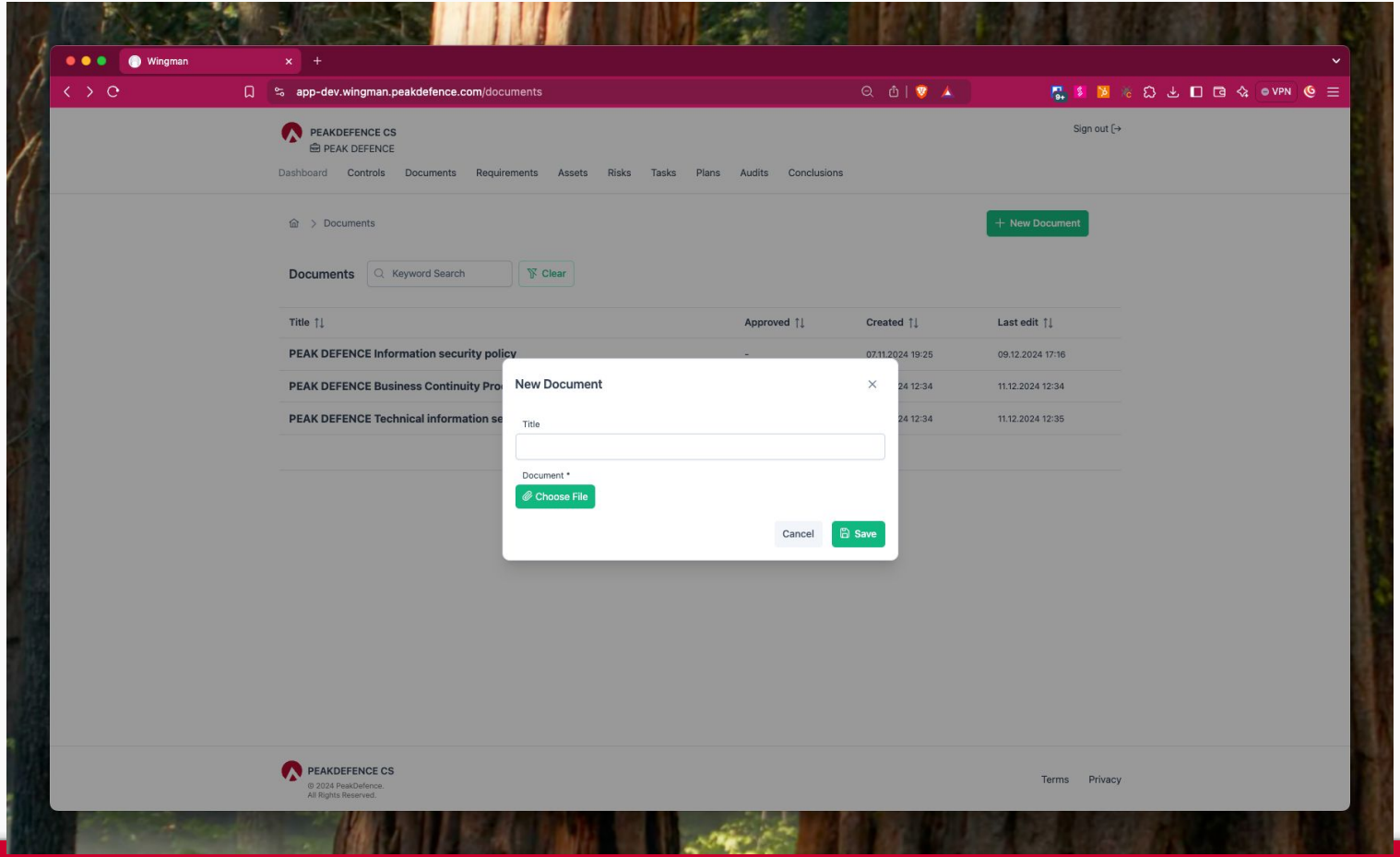
- Audita process / Esošās gatavības novērtējums
- Ja mēs gribētu / mums vajag ATBILST...
  - NIS 2, DORA...

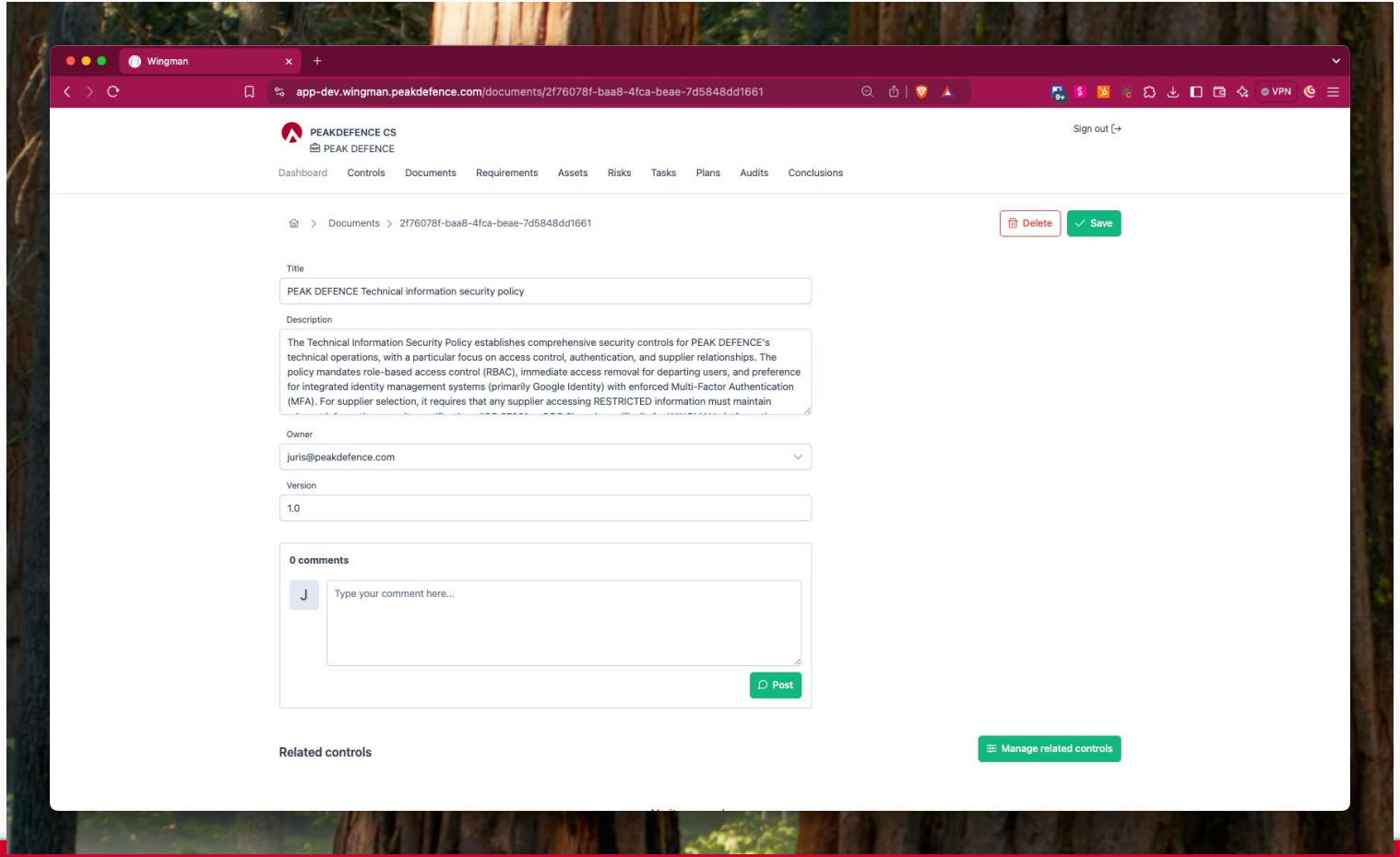
Vai Jūs “Sakāt ko darāt?”*

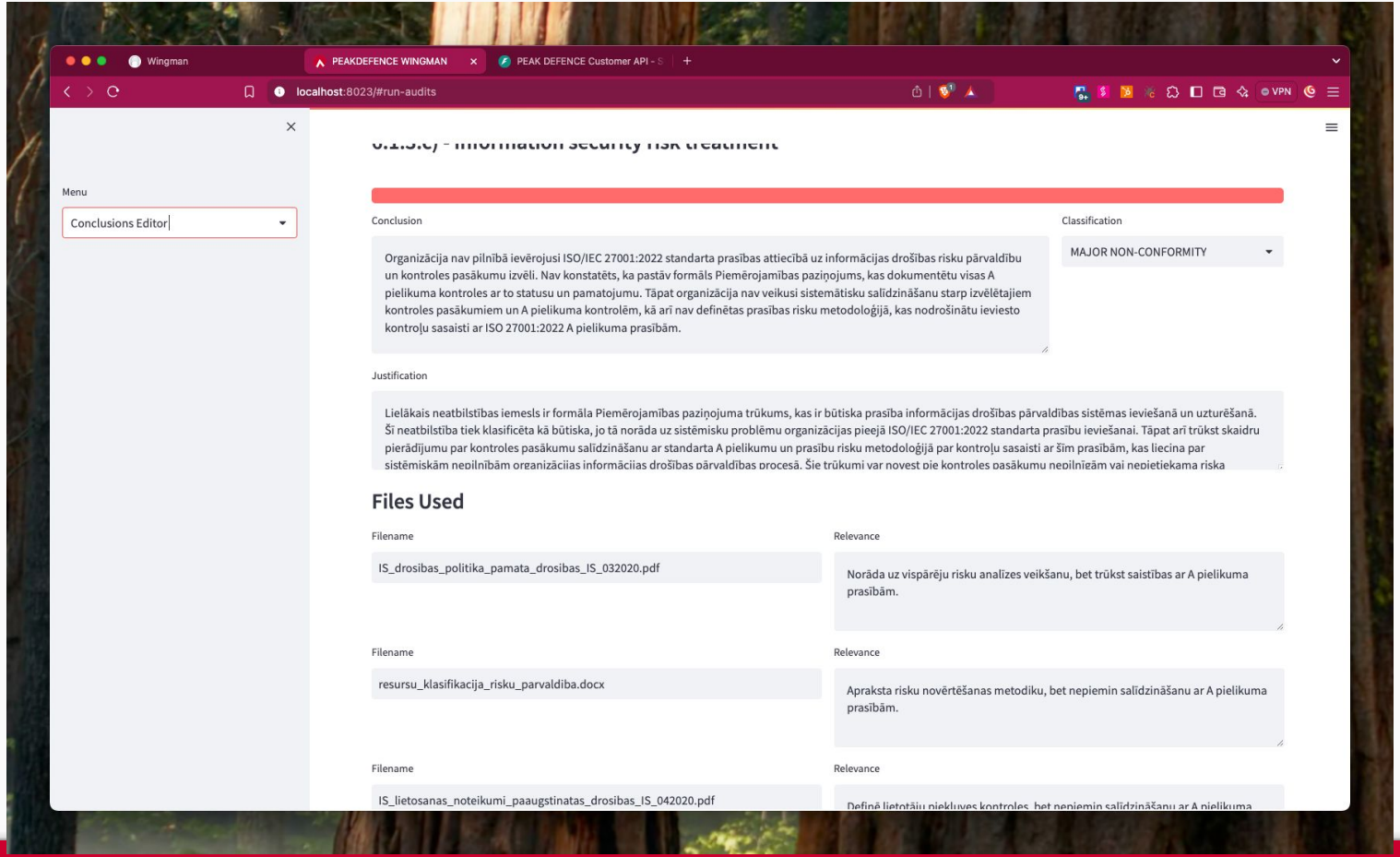
DO YOU SAY WHAT YOU DO?
1.fāzes audits



Dokumentu pievienošana


Wingman
app-dev.wingman.peakdefence.com/documents
VPN
PEAKDEFENCE CS
PEAK DEFENCE
Sign out
Dashboard
Controls
Documents
Requirements
Assets
Risks
Tasks
Plans
Audits
Conclusions
Documents
New Document
Documents
Keyword Search
Clear
Title
Approved
Created
Last edit
PEAK DEFENCE Information security policy
07.11.2024 19:25
09.12.2024 17:16
PEAK DEFENCE Business Continuity Pro
24 12:34
11.12.2024 12:34
PEAK DEFENCE Technical information se
24 12:34
11.12.2024 12:35
New Document
Title
Document *
Choose File
Cancel
Save
PEAKDEFENCE CS
© 2024 PeakDefence.
All Rights Reserved.
Terms
Privacy

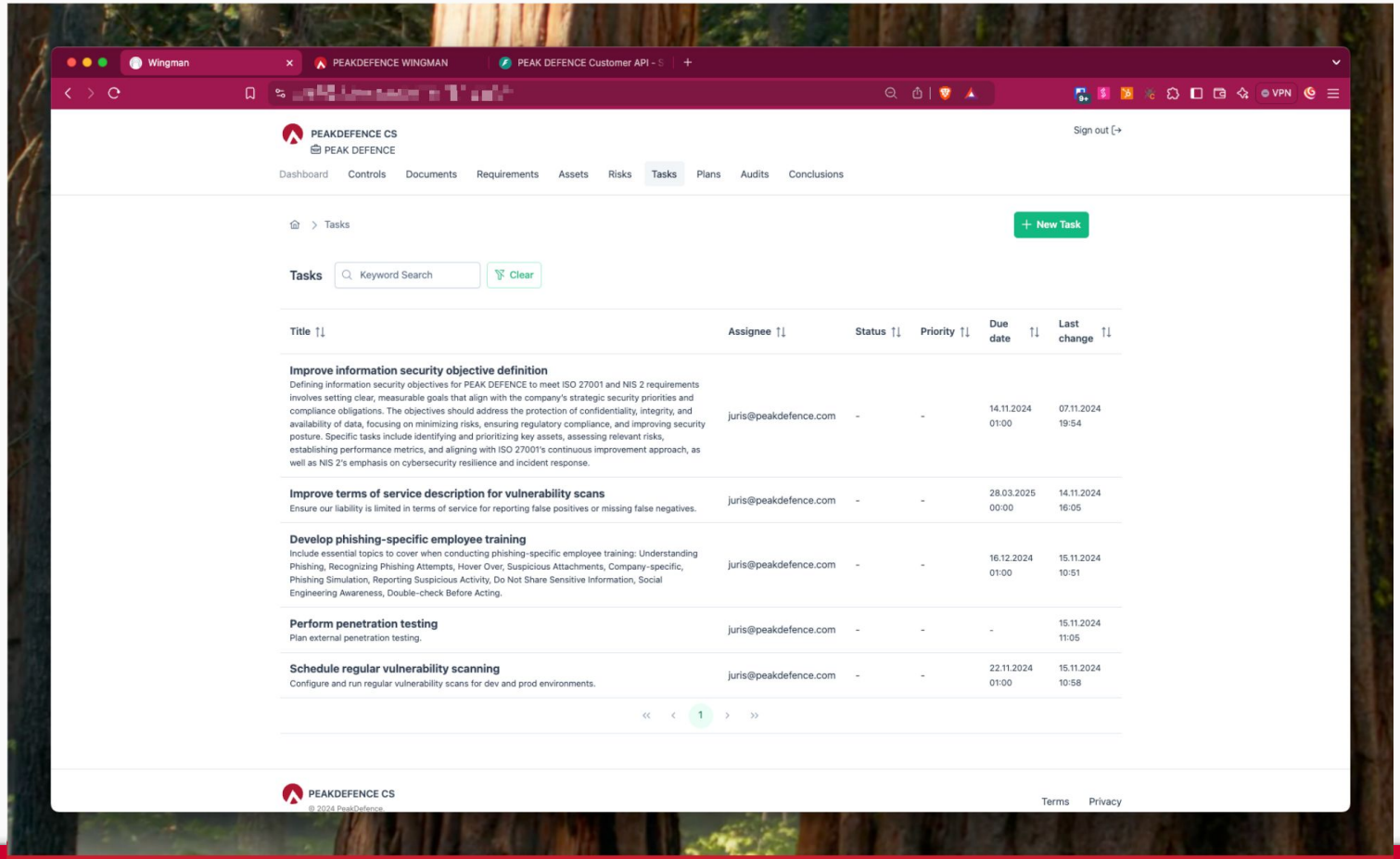

Wingman
app-dev.wingman.peakdefence.com/documents/2f76078f-baa8-4fca-beae-7d5848dd1661
VPN
PEAKDEFENCE CS
PEAK DEFENCE
Sign out
Dashboard
Controls
Documents
Requirements
Assets
Risks
Tasks
Plans
Audits
Conclusions
Documents
2f76078f-baa8-4fca-beae-7d5848dd1661
Delete
Save
Title
PEAK DEFENCE Technical information security policy
Description
The Technical Information Security Policy establishes comprehensive security controls for PEAK DEFENCE's technical operations, with a particular focus on access control, authentication, and supplier relationships. The policy mandates role-based access control (RBAC), immediate access removal for departing users, and preference for integrated identity management systems (primarily Google Identity) with enforced Multi-Factor Authentication (MFA). For supplier selection, it requires that any supplier accessing RESTRICTED information must maintain
Owner
juris@peakdefence.com
Version
1.0
0 comments
J
Type your comment here...
Post
Related controls
Manage related controls



Pielāgojas organizācijai

2. Audita posms (“DO WHAT YOU SAY”)

KONTROĻU IEVIEŠANA vai UZLABOŠANA



Izrietošie darba uzdevumi

“Aiz priekškara”

PEAKDEFENCE CS

PEAK DEFENCE

Sign out

Dashboard | Controls | Documents | Requirements | Assets | Risks | Tasks | Plans | Audits | Conclusions

Requirements

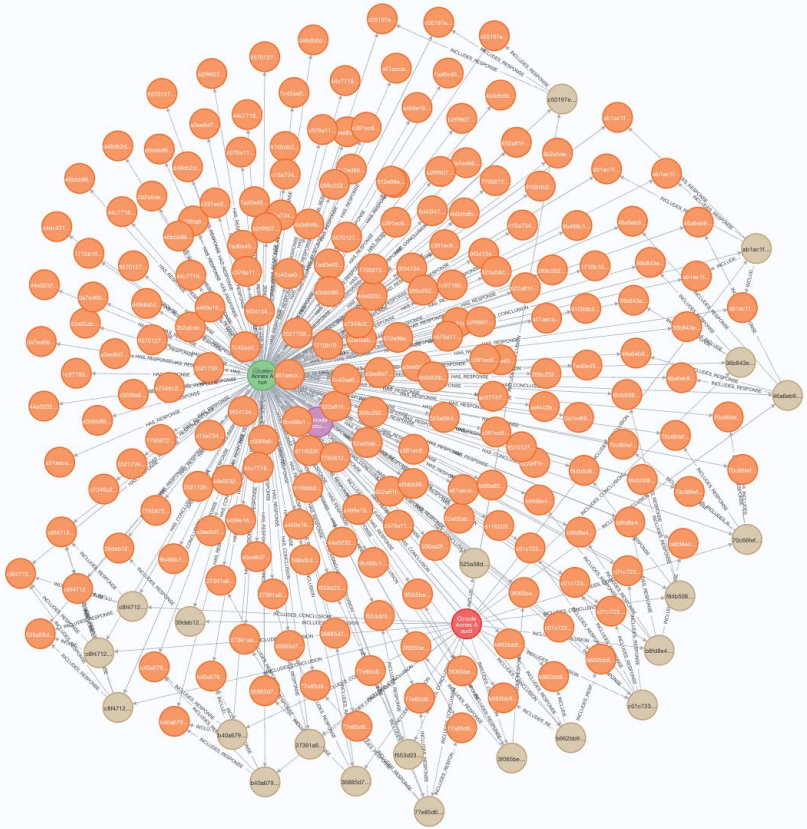
+ New Requirement

Requirements

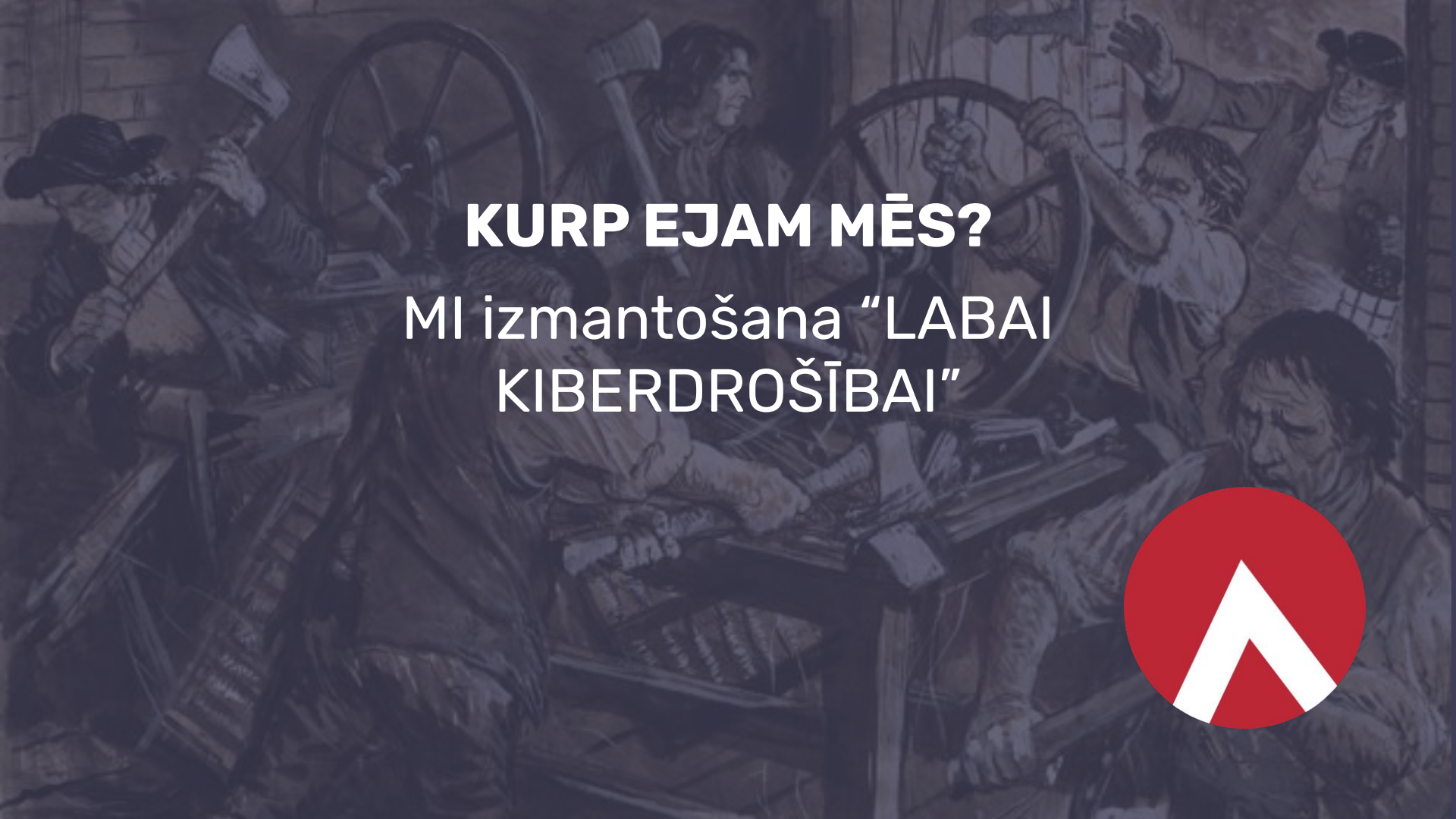
Keyword Search | Clear

Title	Type	Sources
Article 20, P.1 Management bodies must approve the cybersecurity risk-management measures	Legal Obligations	NIS 2
Articel 20, P.1 Management bodies must oversee the implementation of cybersecurity risk-management measures	Legal Obligations	NIS 2
Article 20, P.2 Members of the management bodies are required to follow training, and should offer similar training to their employees on a regular basis	Legal Obligations	NIS 2
Article 21, P.1 Entities must take appropriate and proportionate technical, operational and organizational measures to manage the risks and to prevent or minimise the impact of incidents on recipients of their services and on other services	Legal Obligations	NIS 2
Article 21, P1 When assessing the proportionality of measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact	Legal Obligations	NIS 2
Article 21, P.2(a) Policy on risk analysis. Organisation has to have a policy on risk analysis	Legal Obligations	NIS 2
Article 21, P.2(a) Policy on information system security. Organisation has to have a policy on information system security	Legal Obligations	NIS 2
	Legal	

...peakdefence.com/.../fd7eacd2-6d76-43b4-bb39-a0d...



Mūsu “iegūtās mācības”



KURP EJAM MĒS?

MI izmantošana “LABAI KIBERDROŠĪBAI”

Juris Puce

Making cybersecurity and information security implementers and auditors redundant with contextual...