

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

JURIS PŪCE
PEAK DEFENCE
Smart Strong Security³



Mazi meli, Lieli Meli, Statistika..

A dark-colored umbrella is shown against a black background. The letters 'A' and 'I' are printed in a large, white, sans-serif font across the center of the umbrella's canopy. The umbrella's ribs and central pole are visible. In the background, there are several out-of-focus light sources, including a bright one on the right and several smaller ones at the bottom, suggesting an outdoor night setting.

AI

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, ~~X~~
U.S. INNOVATES...



LLM pielietošana
“kāds tas ir”



to birojs ▾

[Redacted]



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:

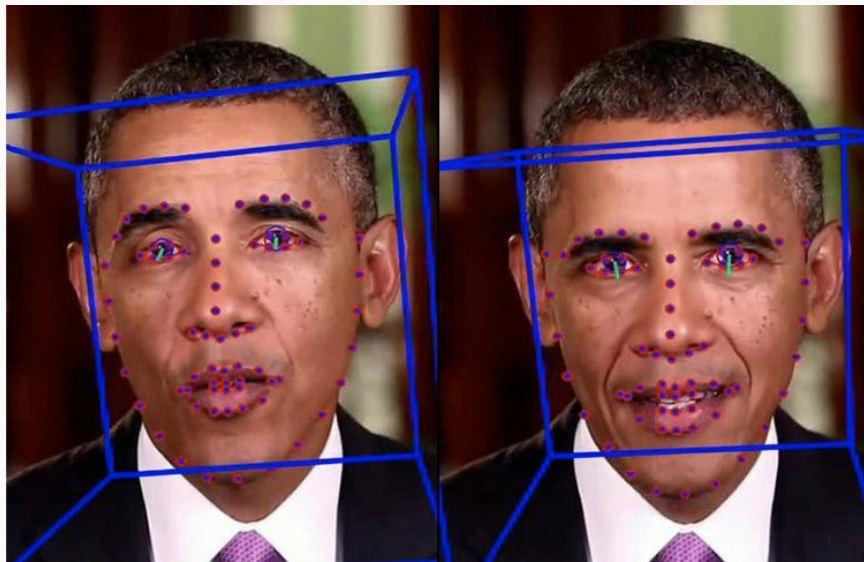
- **Entrepreneurs Competence Center: assistant and advisor to Latvian entrepreneurs**
- **Your company's financial advisor [Redacted] - get professional reporting of Your finances!**

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

Your [Redacted]

F: [Redacted]

E: [Redacted]



🗨️ 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

PEAKDEFENCE CS Sign out (→)

PEAK DEFENCE

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

🏠 > Requirements + New Requirement

Requirements 🗑 Clear

Title ↑↓	Type ↑↓	Sources ↑↓
Article 20, P.1 Management bodies must approve the cybersecurity risk-management measures	Legal Obligations	NIS 2
Article 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

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)

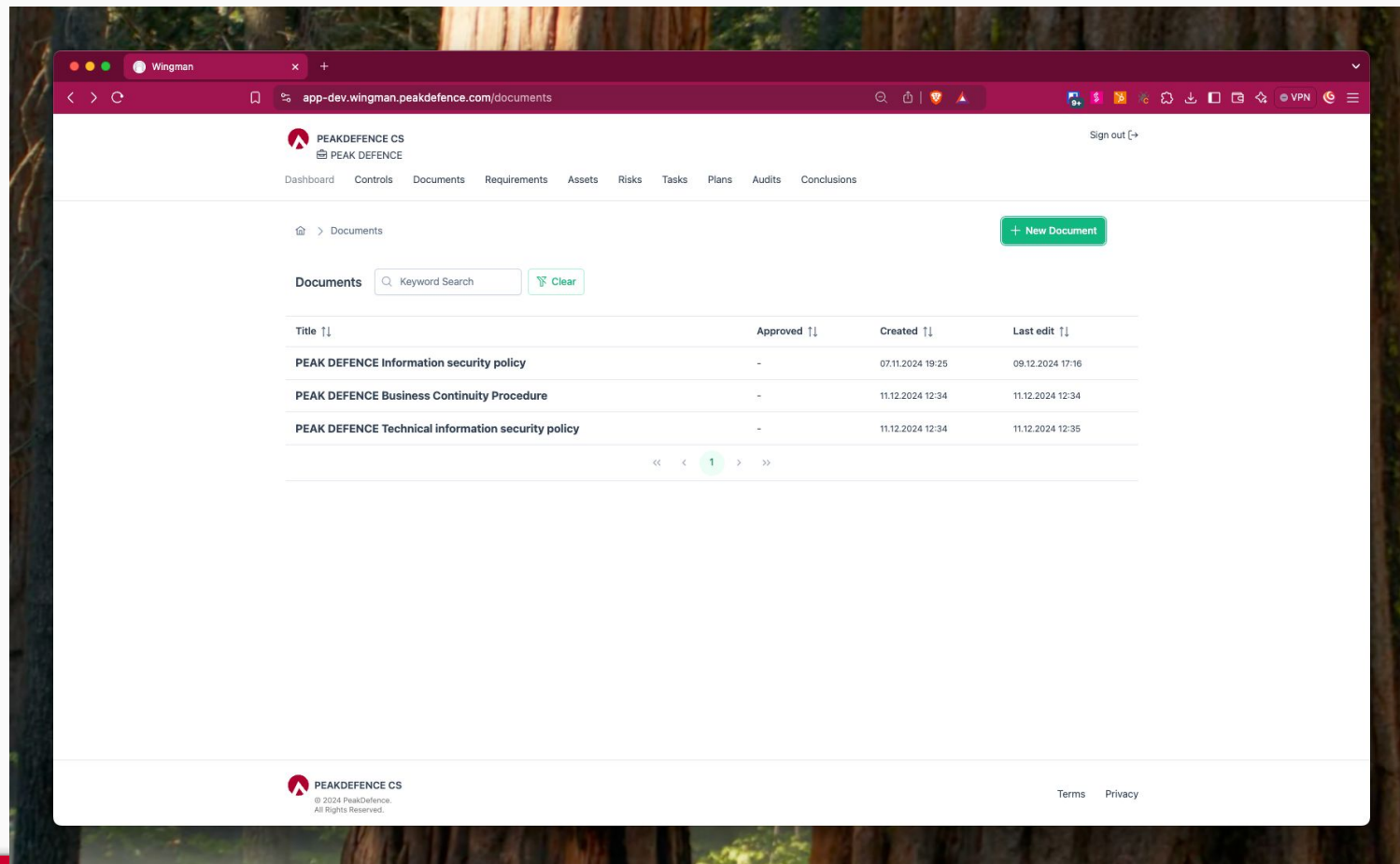
- Audita process / Esošās gatavības novērtējums
- Ja mēs gribētu / mums vajag ATBILST...
 - NIS 2, DORA...



Vai Jūs "Sakāt
ko darāt?"*

DO YOU SAY WHAT YOU DO?

1.fāzes audits



Dokumentu pievienošana

Wingman

app-dev.wingman.peakdefence.com/documents

PEAKDEFENCE CS
PEAK DEFENCE

Sign out →

Dashboard Controls Documents Requirements Assets Risks Tasks Plans Audits Conclusions

Documents + New Document

Documents

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 *

PEAKDEFENCE CS
© 2024 PeakDefence.
All Rights Reserved.

Terms Privacy

Wingman

app-dev.wingman.peakdefence.com/documents/2f76078f-baa8-4fca-beae-7d5848dd1661

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

0.1.3.0 - Information Security Risk Treatment

Conclusion

Classification: MAJOR NON-CONFORMITY

Organizācija nav pilnībā ievērojusi ISO/IEC 27001:2022 standarta prasības attiecībā uz informācijas drošības risku pārvaldību un kontroles pasākumu izvēli. Nav konstatēts, ka pastāv formāls Piemērojamības paziņojums, kas dokumentētu visas A pielikuma kontroles ar to statusu un pamatojumu. Tāpat organizācija nav veikusi sistemātisku salīdzināšanu starp izvēlētajiem kontroles pasākumiem un A pielikuma kontrolēm, kā arī nav definētas prasības risku metodoloģijā, kas nodrošinātu ieviesto kontroļu saistīti ar ISO 27001:2022 A pielikuma prasībām.

Justification

Lielākais neatbilstības iemesls ir formāla Piemērojamības paziņojuma trūkums, kas ir būtiska prasība informācijas drošības pārvaldības sistēmas ieviešanā un uzturēšanā. Šī neatbilstība tiek klasificēta kā būtiska, jo tā norāda uz sistēmisku problēmu organizācijas pieejā ISO/IEC 27001:2022 standarta prasību ieviešanai. Tāpat arī trūkst skaidru pierādījumu par kontroles pasākumu salīdzināšanu ar standarta A pielikumu un prasību risku metodoloģijā par kontroļu saistīti ar šīm prasībām, kas liecina par sistēmiskām neilnībām oranzāciias informācijas drošības pārvaldības procesā. Šie trūkumi var novest die kontroles osākumu neilnīeām vai neopietiekama riska

Files Used

Filename	Relevance
IS_drosibas_politika_pamata_drosibas_IS_032020.pdf	Norāda uz vispārēju risku analīzes veikšanu, bet trūkst saistības ar A pielikuma prasībām.
resursu_klasifikacija_risku_parvaldiba.docx	Apraksta risku novērtēšanas metodiku, bet nepiemin salīdzināšanu ar A pielikuma prasībām.
IS_lietosanas_noteikumi_paaugstinatas_drosibas_IS_042020.pdf	Definē lietotāju nielkūves kontroles, bet nepiemin salīdzināšanu ar A nielkūma

2. Audita posms (“DO WHAT YOU SAY”)

KONTROĻU IEVIEŠANA vai
UZLABOŠANA

Wingman x PEAKDEFENCE WINGMAN PEAK DEFENCE Customer API - 5 +

PEAKDEFENCE CS
PEAK DEFENCE

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

Tasks

[+ New Task](#)

Title ↑↓	Assignee ↑↓	Status ↑↓	Priority ↑↓	Due date ↑↓	Last change ↑↓
Improve information security objective definition Defining information security objectives for PEAK DEFENCE to meet ISO 27001 and NIS 2 requirements involves setting clear, measurable goals that align with the company's strategic security priorities and compliance obligations. The objectives should address the protection of confidentiality, integrity, and availability of data, focusing on minimizing risks, ensuring regulatory compliance, and improving security posture. Specific tasks include identifying and prioritizing key assets, assessing relevant risks, establishing performance metrics, and aligning with ISO 27001's continuous improvement approach, as well as NIS 2's emphasis on cybersecurity resilience and incident response.	juris@peakdefence.com	-	-	14.11.2024 01:00	07.11.2024 19:54
Improve terms of service description for vulnerability scans Ensure our liability is limited in terms of service for reporting false positives or missing false negatives.	juris@peakdefence.com	-	-	28.03.2025 00:00	14.11.2024 16:05
Develop phishing-specific employee training Include essential topics to cover when conducting phishing-specific employee training: Understanding Phishing, Recognizing Phishing Attempts, Hover Over, Suspicious Attachments, Company-specific, Phishing Simulation, Reporting Suspicious Activity, Do Not Share Sensitive Information, Social Engineering Awareness, Double-check Before Acting.	juris@peakdefence.com	-	-	16.12.2024 01:00	15.11.2024 10:51
Perform penetration testing Plan external penetration testing.	juris@peakdefence.com	-	-	-	15.11.2024 11:05
Schedule regular vulnerability scanning Configure and run regular vulnerability scans for dev and prod environments.	juris@peakdefence.com	-	-	22.11.2024 01:00	15.11.2024 10:58

« < 1 > »

PEAKDEFENCE CS
© 2024 PeakDefence

Terms Privacy

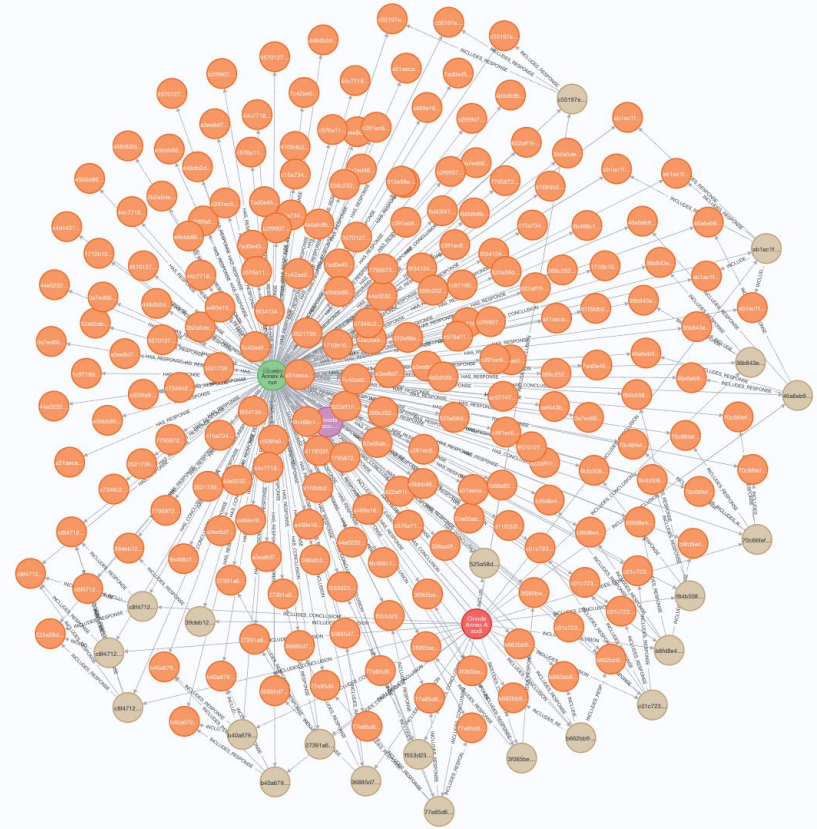
Izrietošie darba uzdevumi

“Aiz priekškara”

+ New Requirement

Requirements

Title [v]	Type [v]	Sources [v]
Article 20, P.1 Management bodies must approve the cybersecurity risk-management measures	Legal Obligations	NIS 2
Article 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
...peakdefence.com/.../id7eacd2-6d76-43b4-bb39-a0d...	Legal	NIS 2





Mūsu "iegūtās mācības"



KURP EJAM MĒS?

MI izmantošana "LABAI
KIBERDROŠĪBAI"





Juris Puce

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

