CYBERDAY

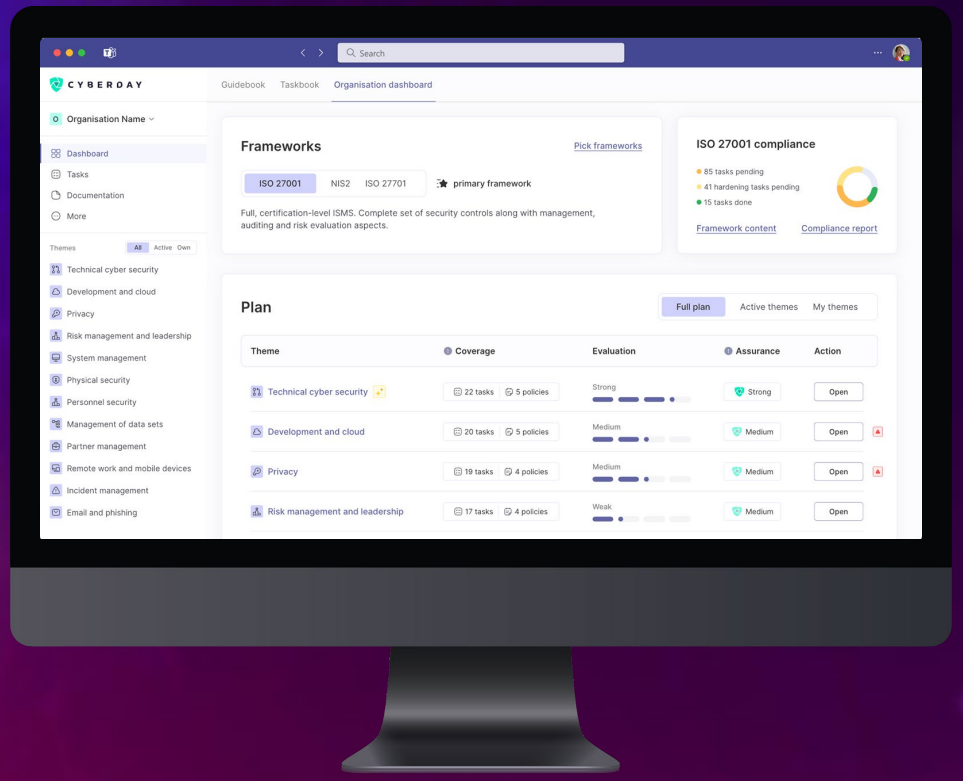
Kohti ISO 27001 -sertifiontia

Mitä olisin halunnut tietää ennen ISO 27001 -projektia?

Aleksi Pulkkanen

COO, Cyberday / Agendium Ltd

Cyberday Oy lyhyesti



1

Cyberday Oy

- Ohjelmisto - ja tietoturvayritys, fokus tietoturvan johtaminen ja compliance
- HQ Tamperella
- Perustettu 2014
- 600+ asiakasta 20+ EU-maasta ja kaikilta toimialoilta ja kokoluokista

2

Digiturvamalli

- ISMS-työkalu suoraan MS Teamsin sisällä
- Selkeyttää matkaa kohti omia compliance-tavoitteita
- Kaikki matkalla tarvitut työkalut, yhdellä selkeällä hinnalla

kiwa certified
ISO/IEC 27001
Inspecta Sertifiointi Oy

OULU · ecraft · KUNTALIITTO · KiiLTO · KREATE THE FUTURE IS BUILT TODAY · Saariomen · WIHURI · SARKANIEMI · DELETE WORKING FOR THE FUTURE


ISO 27001:2022
ISO 27001:2013
ISO 27017
ISO 27018
ISO 27701
ISO 13485:2016
ISO 9001:2015
ISO 22301:2019
SOC 2
NIST
C2M2
CYBER ESSENTIALS
GDPR
NIS2
DORA
CIS
CIS 18
CYBER FUNDAMENTALS
Cyberday content library
DORA RMF
Kokonaiskuva
Julkri: TL IV-I
Katakri
Katakri (2020)
NIS2 Lithuania
NIS2 Finland
NIS2 Belgium
NIST 2.0
NSM ICT
NIS2 Latvia
TiHL
TISAX
NIS2 Croatia
TiHL TT
Omavalvonta
THL TTsuun
IEC 62443
PCI DSS
HIPAA

Älä tee tuplatyötä. Tee asiat hallitusti kerran, näytä compliance moneen suuntaan.

Tietoturvakehikot jakavat yhteisen ytimen – riskienhallinta, varmuuskopiot, haittaohjelmat, henkilöstön osaaminen, pääsyn hallinta…

Digiturvamalli kohdistaa vaatimukset yleisiin tehtäviin – yksi suunnitelma josta syntyy compliance nyt ja jatkossa

ISO 27001

NIS2

GDPR

Mitä olisin halunnut tietää ennen omaa ISO 27001 -sertifiointiprojektia?

CYBERDAY

1. ISO 27001 on projekti, siinä missä muutkin

- **Projektin avainaskeleet**
  - Ymmärrä, mitä tarvitaan
  - Toteuta ne asiat
- **ISO 27001: 22 vaatimusta, 93 kontrollia**
  - Älä ulkoista standardin ymmärtämistä
  - Saatte enemmän hyötyä + löydätte teille relevantin tason
- **ISMS adminin tärkeä rooli**
  - Pidä kunnianhimo tarpeeksi korkealla
  - …mutta varmista kokoajan tarkoituksenmukaisuus

CYBERDAY

2. Ensin kukaan ei tiedä, kuinka kauan teillä kestää

- **Kesto vaihtelee**
  - 2 viikkoa, 2 kuukautta, 2 vuotta, ei koskaan?
  - Riippuu toiminnan laajuudesta, nykyisestä tietoturvatasosta, resursseista ja käytetyistä työkaluista
- **Ei oikoteitä**
  - Fiksulla aloituksella voit pian arvioida, kuinka paljon teillä on tekemistä
- **Standardia voi aluksi hyödyntää monin tavoin**
  - Benchmark
  - Nykytason arviointi
  - Compliance … ja sitten sertifiointi

CYBERDAY

3. Ei kannata ohittaa tavoitteiden määrittelyä

- **Mitä tavoittelemme ISO 27001 -sertifioinnilla?**
  - Parantunut tietoturva ja jatkuvuus
  - Tietoturva - / asiakasvaatimusten täyttäminen
  - Kilpailukyky… vai kaikki ylläolevat?
- **Isot tavoitteet, vastaava sitoutuminen tekemiseen**
  - ISO 27001 on hankalaa, jos sen odotettiin olevan helppoa
- **Johdon sitoutuminen = onnistumisen varmistaja**
  - Ilman tätä projekti voi menettää momentuminsa

CYBERDAY

4. Teillä voi olla 3 tai 30 politiikkaa – te päätätte.

- Dokumentaatiota tarvitaan
  - Jotkin dokumentit ovat pakollisiakin, mutta niitä on vähän
  - Yleensä asiat toteutuvat paremmin, jos ne kirjoitetaan ylös
- Jokaisen asian ei tarvitse olla 10 -sivuinen politiikka
  - Ketterämmät muodot helpottavat ylläpitoa
  - Vaikealukuiset politiikat lannistavat osallistumista
- ISMS adminin rooli
  - Pysy kriittisenä ja huolehdi dokumentaation sopivuudesta

CYBERDAY

5. Kukaan ei palkitse kontrollien täydellisestä toteuttamisesta

- **Suurin osa kontrolleista on relevantteja**
  - Mutta kontrollien toteutuksissa on monia syvyyksiä
  - Löydätte parannuksia luonnostaan työn ohessa
- **Ei liian herkästi ”ei soveltuvaksi"**
  - Perustelujen oltava selkeät, jos kontrolli jätetään pois
    - Riskilähtöinen kevyempi toteutus voi olla helpompi perustella

CYBERDAY

6. ISMS-pääkäyttäjän työ voi olla yksinäistä

- **Selkeät roolit, liittyvät vastuut ja liittyvät osaamiset auttavat paljon**
  - CISO, HR, riskienhallinta, tekninen tietoturva, fyysinen tietoturva…
- **Johdon on osallistuttava aktiivisesti (vaatimus 5)**
  - Johdon katselmukset, tavoitteiden asettaminen, resurssien määrittely…
- **ISO 27001 rakentaa tietoturvakulttuuria koko organisaatioon**
  - Kulttuuri alkaa ihmisistä (relevanssi)
  - Ei ole ”IT-asia”

CYBERDAY

7. Auditoijatkin ovat (kiireisiä) ihmisiä

- **Jos sertifiointi kiinnostaa, hankkiudu kalenteriin ajoissa**
  - Isot auditoinnit kestävät ja kalenterit voivat olla täynnä useita kuukausia
- **Auditoinnissa ei kannata esittää täydellistä**
  - Pyri läpinäkyvään, selkeään ja todenmukaiseen viestintään
  - Tavoite auditoinneissa = parantaa
- **Ulkoiset ja sisäiset auditoinnit ovat parhaimmillaan erittäin hyödyllisiä työkaluja / tapahtumia**

CYBERDAY

8. Pahinta on käyttää energiaa asiaan, jota ei olisi pitänyt tehdä ollenkaan

- **Panostakaa selkeään riskienhallinnan toimintamalliin**
  - Ei liikaa hienostelua, mutta ei yleisiä riskilistojakaan
- **Riskienhallinnassa on kyse tietoturva -ajattelusta, priorisoinnista ja jatkuvasta parantamisesta**
  - Tarkoitus ei ole kiirehtiä kirjaamaan excelissa riskejä käsitellyiksi
- **Riskienhallinta kehittyy hallintajärjestelmän mukana**
  - Aloita selkeyttä korostaen
  - Paranna syvyyttä ajan myötä

CYBERDAY

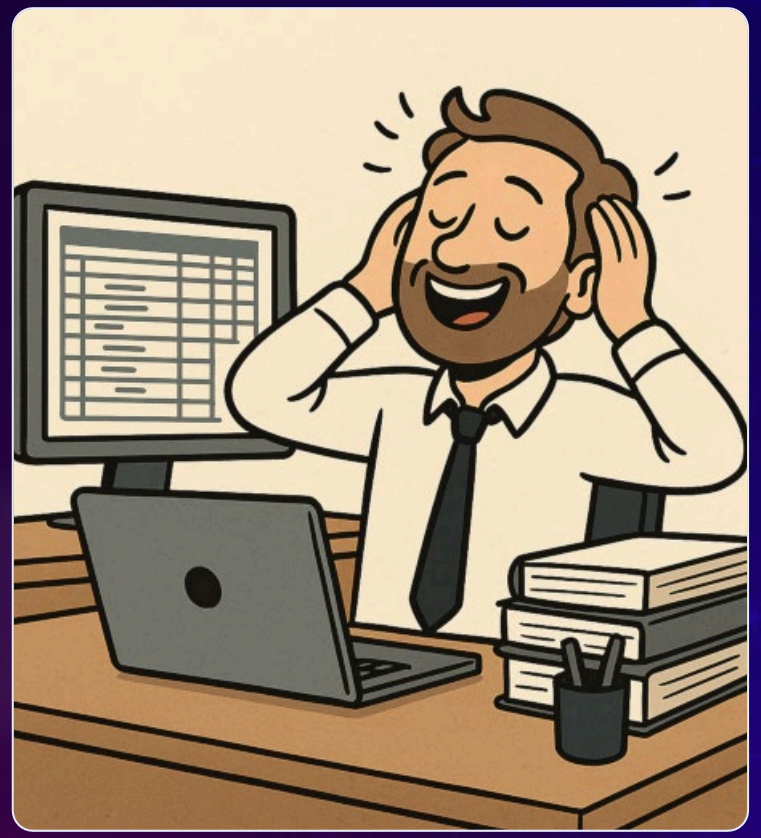
9. Täydellisyyttä ei vaadita. Mutta parantamista vaaditaan – joka vuosi.

- **Hallintajärjestelmän varsinainen pyörittäminen vasta alkaa sertifioinnin jälkeen**
  - Jatkuva parantaminen, riskien hallinta…
  - Tarkistukset, katselmukset, auditoinnit, koulutus…
- **Parhaassa tapauksessa ISMS on tärkeä osa organisaatiotanne**
  - Tuottaa kypsää tietoturvatekemistä – ei vain compliancea
- **Muista jatkossakin ISO 27001 pääkohdat 4 - 10**
  - Auditoija katsoo niitä aina eniten ja haluaa nähdä kehitystä

CYBERDAY

10. Työkalu voi säästää järkeäsi

- Manual ISO 27001 = pain
- Työkaluilla monia hyötyjä
  - Ymmärrä vaaditut asiat ja delegoi toteutus
  - Muodosta dokumentaatio puoliautomatisoidusti
  - Näytä auditoijalle, että teillä on ylläpidettävä toimintatapa
- Pysy kriittisenä. Pidä ISMS relevanttina.
  - Tehtäväsi myös työkaluja hyödynnettäessä.



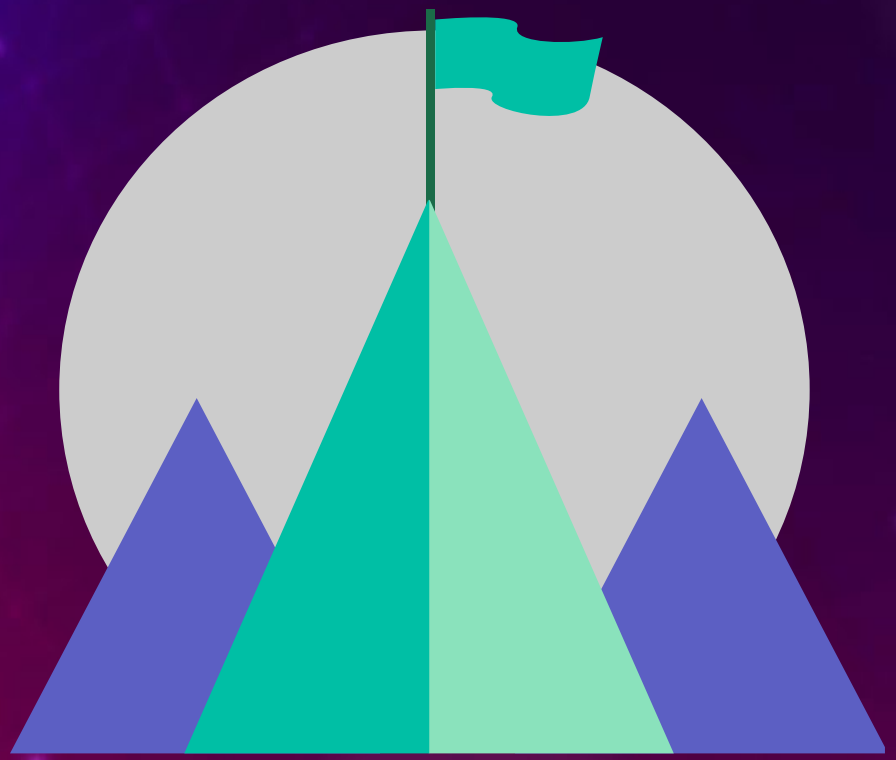
CYBERDAY

Mitä olisin halunnut tietää?

1. ISO 27001 on projekti, siinä missä muutkin
2. Ensin kukaan ei tiedä, kuinka kauan teillä kestää
3. Ei kannata ohittaa tavoitteiden määrittelyä
4. Teillä voi olla 3 tai 30 politiikkaa – te päätätte.
5. Kukaan ei palkitse kontrollien täydellisestä toteuttamisesta
6. ISMS-pääkäyttäjän työ voi olla yksinäistä
7. Auditoijat ovat (kiireisiä) ihmisiä
8. Pahinta on käyttää energiaa asiaan, jota ei olisi pitänyt tehdä ollenkaan
9. Täydellisyyttä ei vaadita. Mutta parantamista vaaditaan – joka vuosi.
10. Työkalu voi säästää järkeäsi

https://www.cyberday.ai/blog/iso-27001-compliance-and-certification-checklist

Toimivan hallintajärjestelmän hyödyt



01 **Parantunut tietoturva**

Suojaudu kyberhyökkäyksiltä ja vähennä riskejä selkeällä tietoturvatyöllä.

02 **Tehokas compliance**

Toteutatte asiat kerran, mutta olette valmiina raportoimaan nykyisiä ja tulevia vaatimuksia kohden (30+ vaatimuskehikkoa tuettuna).

03 **Myynti - ja maine -hyödyt**

Helpota myyntiä näyttämällä, että tietoturva otetaan vakavasti ja parhaat käytännöt ovat käytössä.

04 **Vältä sakkoja ja ongelmia**

Näytä vahvojen todisteiden avulla, että tietoturva oli otettu vakavasti ja työtä oli tehty.

Askeleet kohti ISO 27001 -sertifiointia

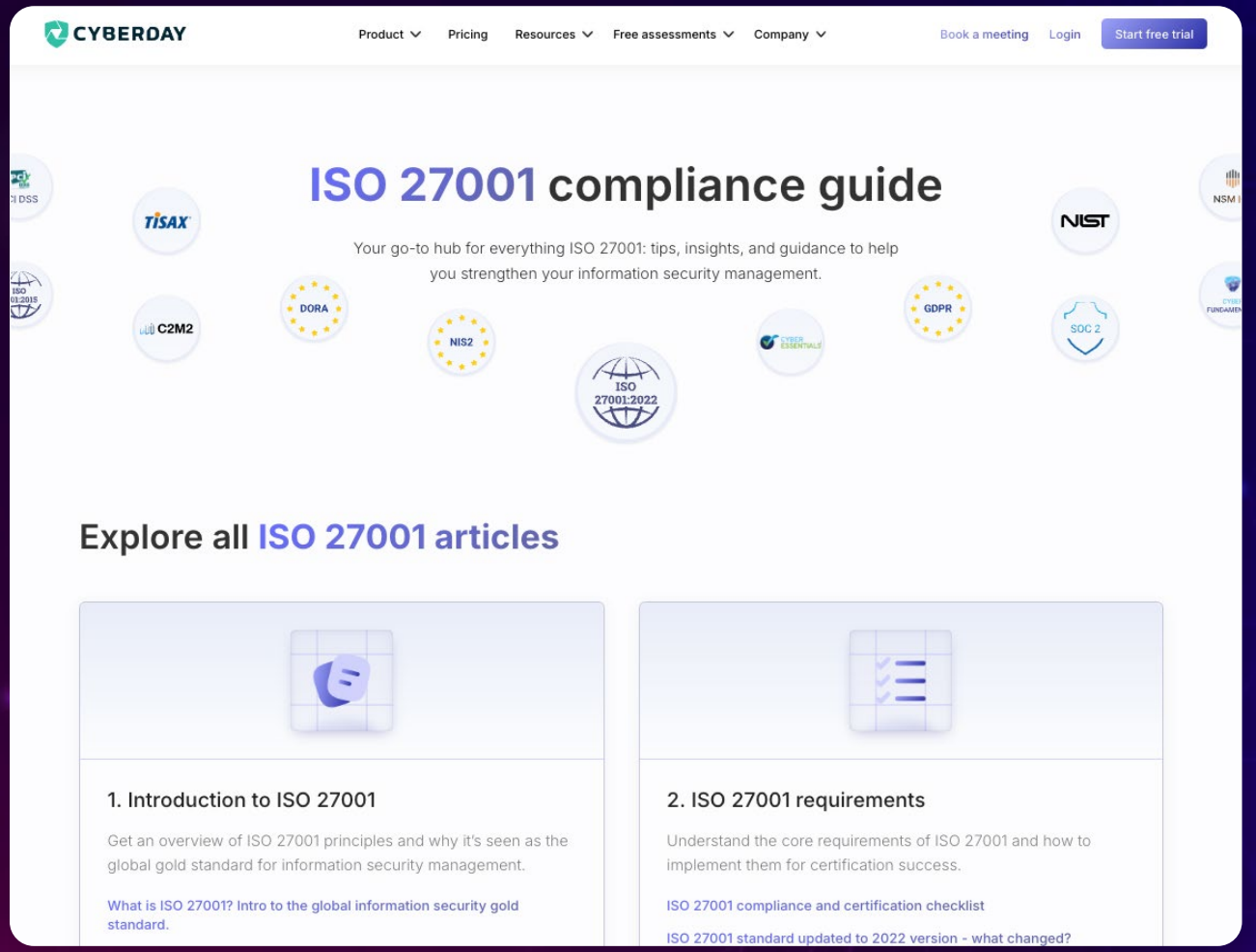
1. Ymmärrä ISO 27001:n perusteet
2. Määrittele hallintajärjestelmän scope
3. Valitse tapa ISMS:n rakentamiseen
4. Perusta ISMS-tiimi ja nimeä roolit
5. Arvio tietoturvan lähtötasonne
6. Luo ja vastuuta suojattavan omaisuuden luettelo
7. Luo henkilöstön ohjeistukset
8. Aloita työ tietoturvariskien hallinnassa
9. Tarkenna soveltuvuuslausuntoa (SoA)
10. Luo ja katselmoi halutut dokumentit / politiikat / raportit
11. Järjestä ensimmäinen johdon katselmus
12. Suorita ISO 27001:n sisäinen auditointi
13. Toteuta ulkoinen ISO 27001 – sertifiointiauditointi ja hanki sertifikaatti
14. Suunnittele ISMS:n jatkuva pyörittäminen, valvonta ja seuraavat auditoinnit

https://www.digiturvamalli.fi/blogi/iso-27001--vaatimustenmukaisuus-ja-sertifioinnin-muistilista

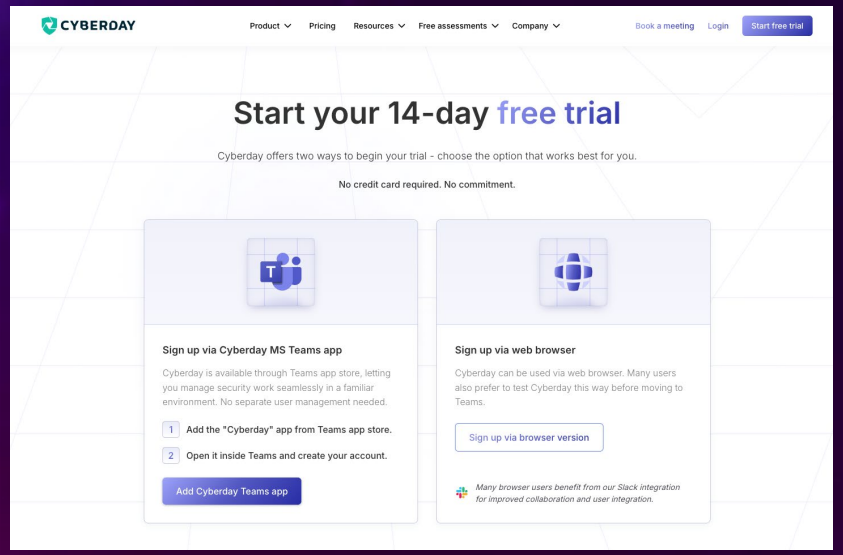
Haluatteko oppia lisää ISO 27001:stä?

Digiturvamalli.fi sivustolla tarjolla laaja kokoelma ISO 27001 -sisältöä

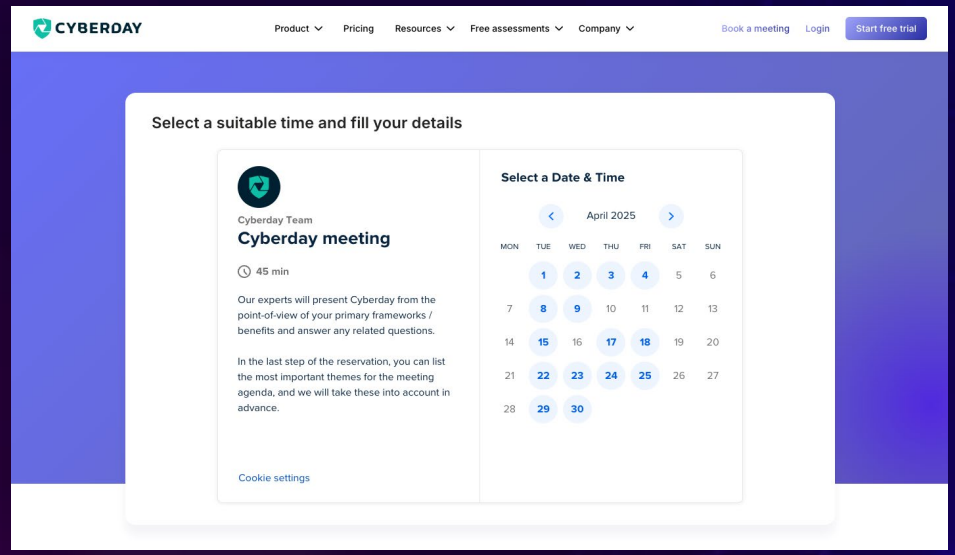
digiturvamalli.fi/kokoelma/iso-27001



Haluatteko keskustella lisää kanssamme?



tai



Kokeilkaa itse

Ilmainen 14 päivän kokeilu tarjolla
digiturvamalli.fi/kokeile

Varaa palaveri kanssamme

Valitse teille toimiva aika osoitteesta
digiturvamalli.fi/palaveri

Kiitokset mielenkiinnosta!

Aleksi Pulkkanen

COO, Agendium Oy, CIPP/E

+358 44 3581 817

aleksi.pulkkanen@agendium.com