Informatikai kockázatkezelés energetikai vállalatcsoportban

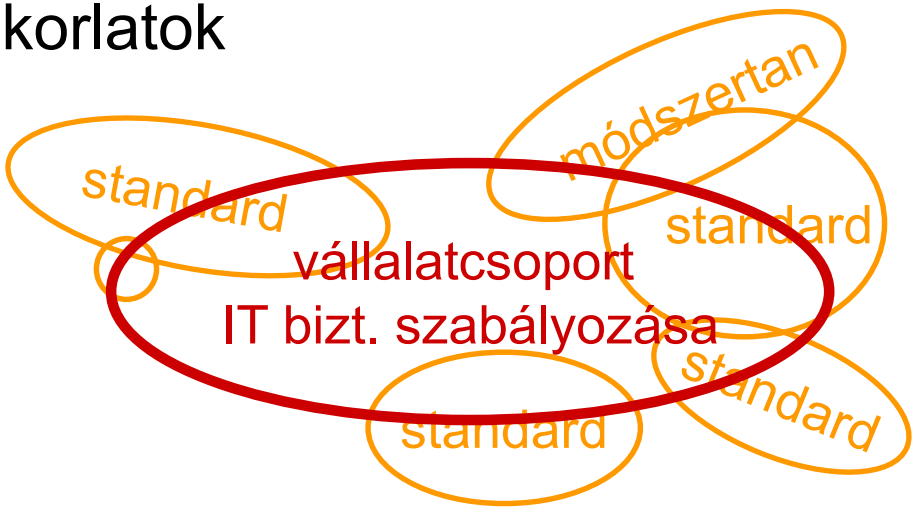
esettanulmány

Sipos János

partner, JaSipos IT biztonsági és audit Kft.

Előzmények, háttérinformáció

- 24 ország, 192 vállalat
- átgondolt, tudatos IT biztonsági szabályozási környezet
  - ISO 17799, ISO 27001 - 27004
  - COBIT 4.1
  - ITIL
  - Common Criteria (ISO 15408)
  - Orange Books
  - Közigazgatási Informatikai Tárcaközi Bizottság ajánlásai
  - legjobb gyakorlatok



Követelmények, célprogram

Célprogram

- kockázatok felmérése, értékelése
- stratégia készítése
- 5-10 éves fejlesztési terv készítése
- projektek definiálása

Elvárások

- áttekinthető, hatékony módszertan
- mérhetőség, megismételhetőség
- egzakt cselekvési terv
  - feladatterv
  - időterv
  - pénzügyi terv
- auditálhatóság, audit-állóság

Kockázatok felmérése

- vállalati bontásban
- 21 témakör 88 alfejezete alapján
- CMM (Capability Maturity Model) szerint értékelve (0-5 skálán)
- előre elkészített kérdőíveken
- felmérés előtt
  - felsővezetői támogatás elnyerésével
  - felmérést végzők oktatásával

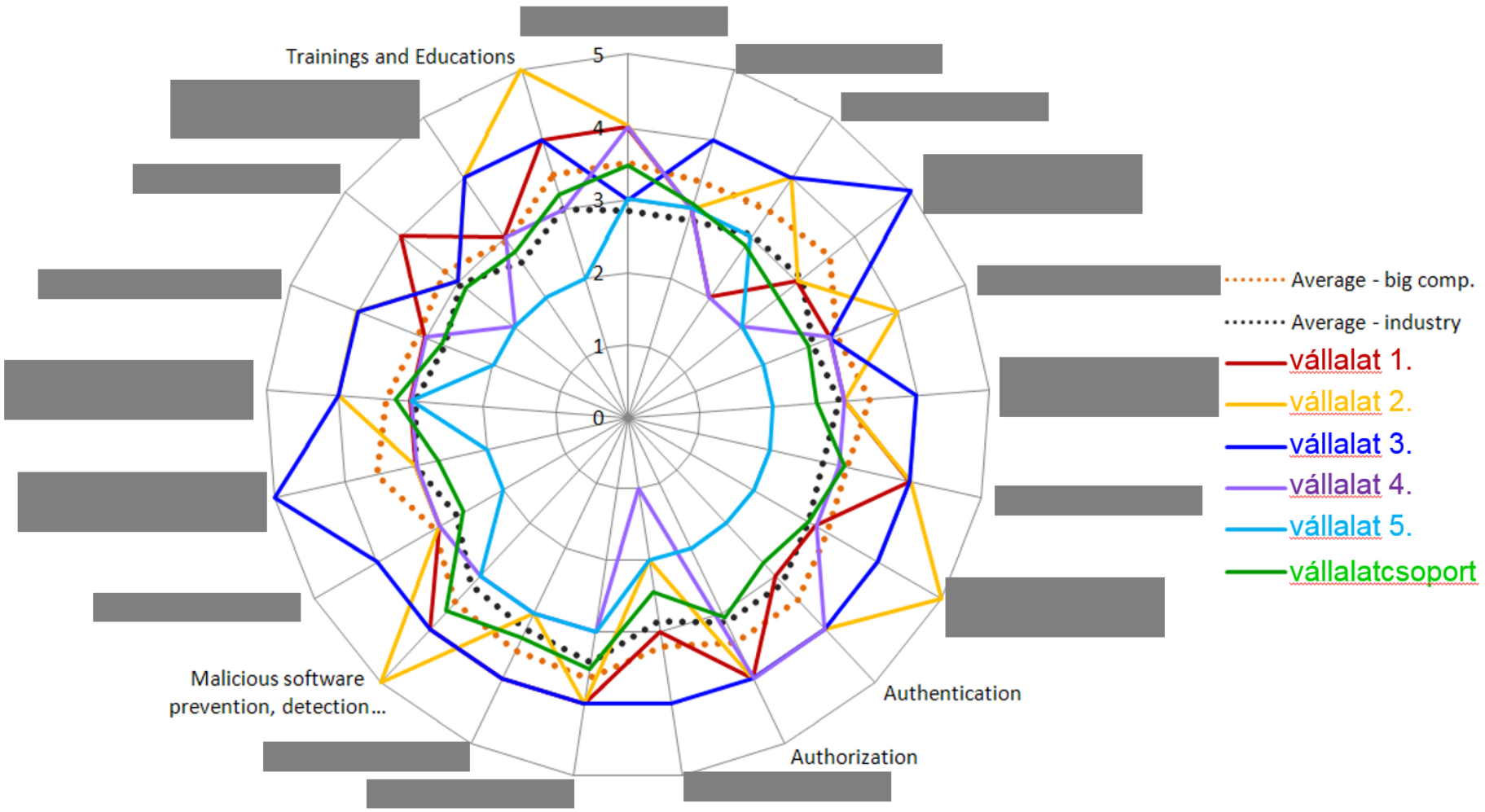
Relevant chapter within the (...) regulation	No.	Questions	Evaluation criterias - expected answers	Rating
2.2.9. Authentication	1	Please describe authentication process to domain. What kind of authentication is used, how is it regulated, is it for all users, what are the settings?	Windows autentication system. Settings: min psw length characters, expiration 3 months, last 3 psws has to be diferent.	
2.2.9. Authentication	2	Please describe authentication process to ERP system and main applications. What kind of authentication is used, how is it regulated, is it for all users, what are settings?	PSW autentication is used. Min psw length 7, has to be complex, last 6 psws has to be different.	
2.2.9. Authentication	3	Do ERP system and other applications support rules for length, composition of passwords and restriction on using previous passwords?	ERP does.	

Hiányzó adatok kezelése

Kockázatok bemutatása

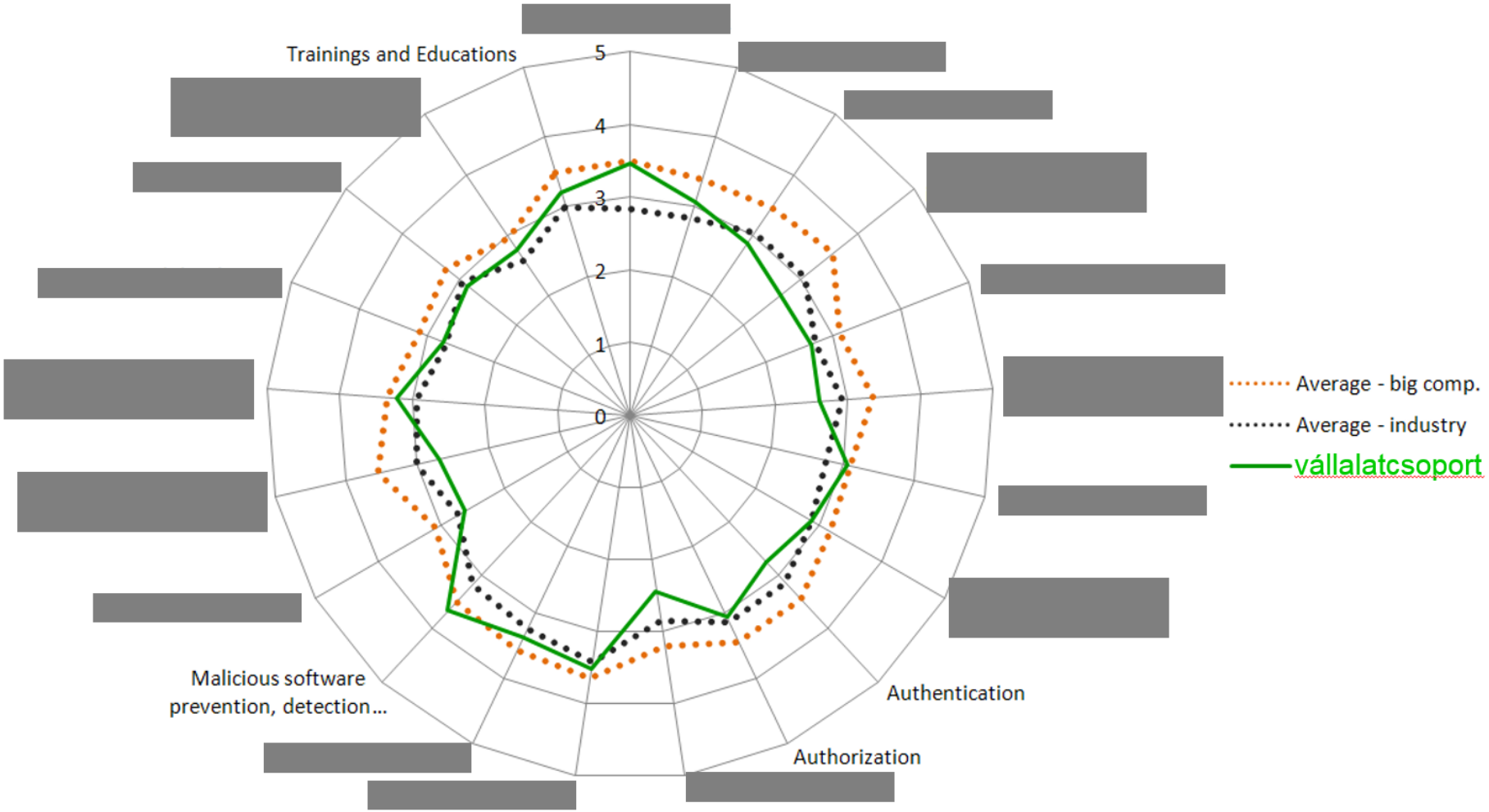
- **Szabályozásnak megfelelő bontásban**
  - 21 témakörben
- **Súlyozva**
  - vállalatméret alapján
- **Szemléletesen**
  - vállalati bontásban
  - vállalati átlaghoz viszonyítva
  - hasonló méretű vállalatokhoz viszonyítva
  - hasonló tevékenységű vállalatokhoz viszonyítva
  - célhoz viszonyítva
- **Konvertálás: ISO27001 vs. vállalati szabályozás**
  - vállalati szabályozás és ISO 27001 felépítése részben eltérő

Kockázatok bemutatása –vállalati bontásban

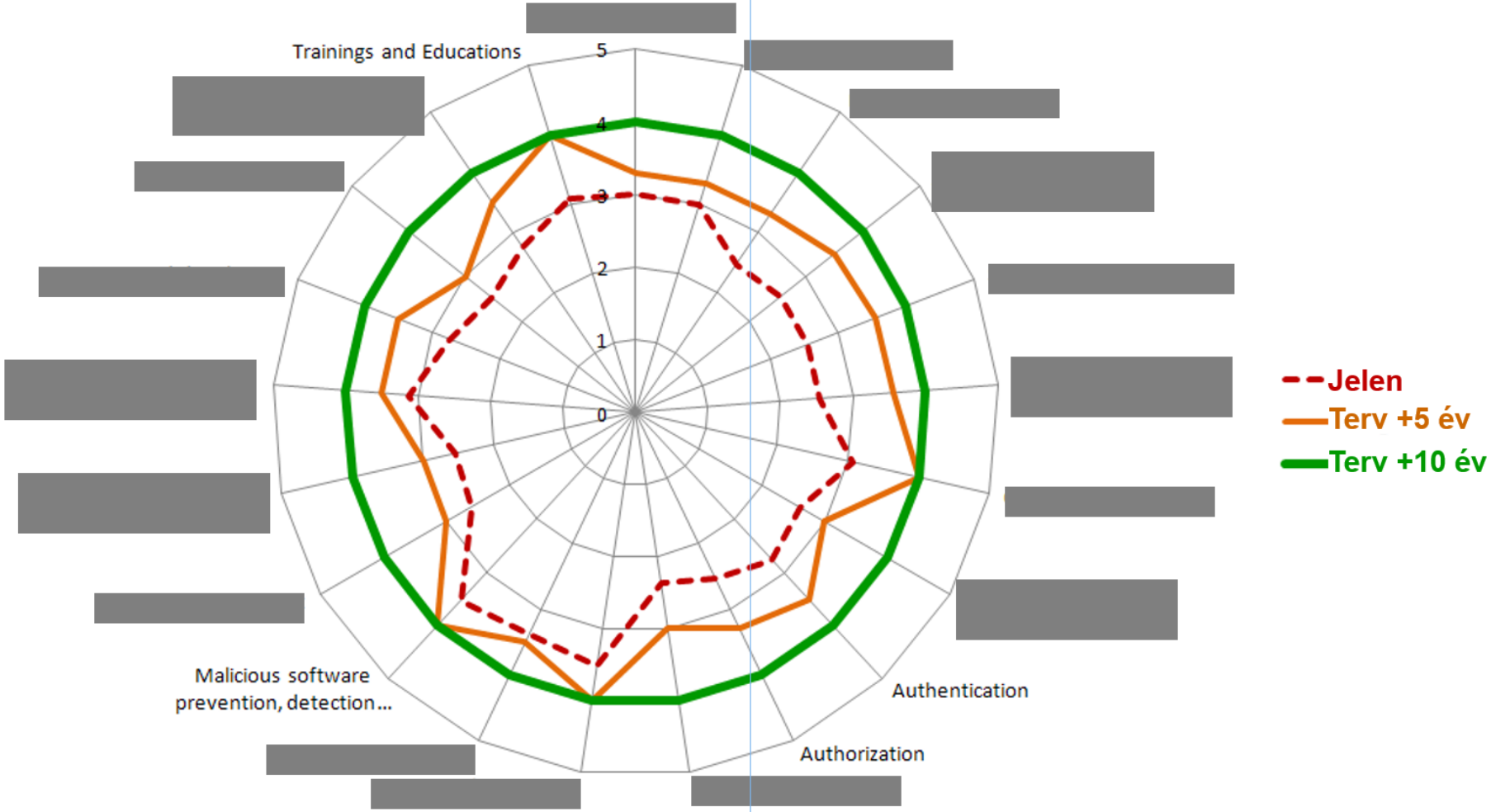


JaSipos IT BIZTONSÁGI & AUDIT KFT

Kockázatok bemutatása – csoportszinten

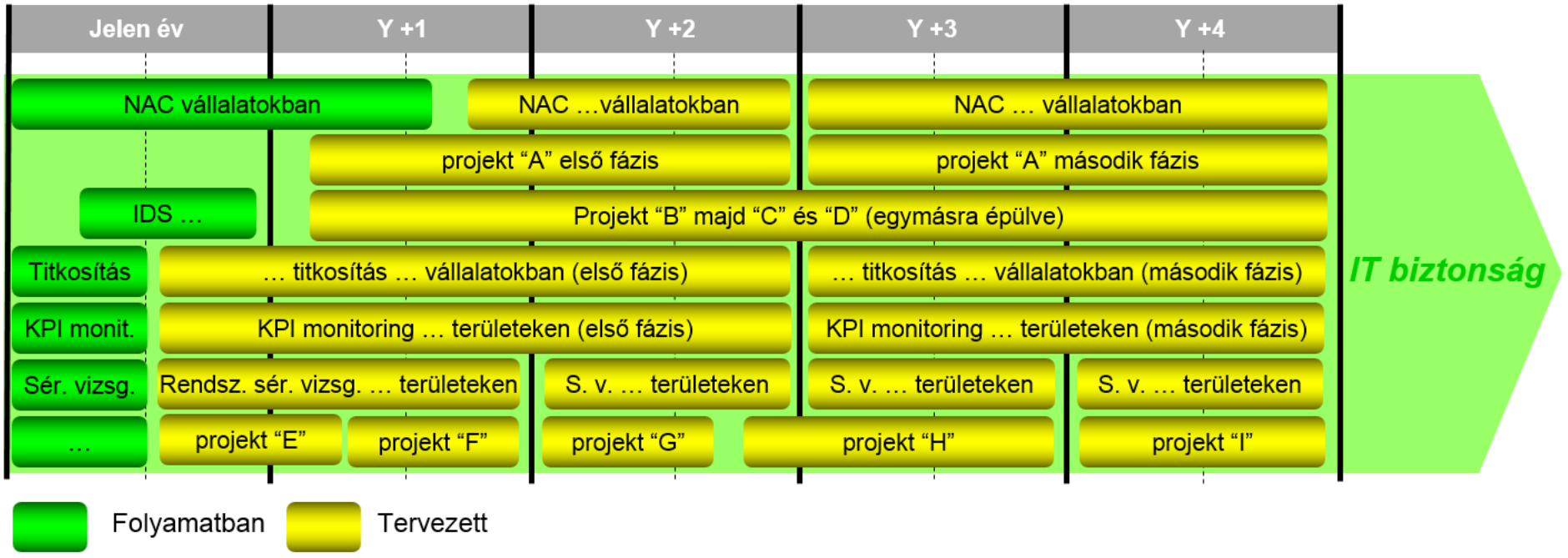


Biztonsági szint vs. elérendő cél



Célhoz vezető út: projektek

- **Projektek indoklása**
  - jelen helyzetből a tervezett állapotba
  - mely vállalatban, miért indokolt
  - priorizálás: elmaradás a tervezett állapottól stb.



Összefoglalás

Kiinduló állapot

- **Kockázatfelmérés**
  - **Kockázatértékelés, értelmezés**
    - **Cél meghatározása**
      - **Cselekvési terv**
        - ***Megvalósítás***
          - ***Visszamérés***

(Jelenleg nem került bemutatásra)

Munkatársaink szakmai tapasztalata

- Auditált ügyfél támogatása - több, mint **200** esetben
- Audit elvégzése - több, mint **90** esetben
- Elvárásoknak megfelelés (compliance) – közel **200** esetben
- Kockázatkezelés – több iparágban
- Információ biztonság – több, mint **200** ügyfélnél
- Információ biztonsági felelős – több ügyfélnél
- Visszaélések kivizsgálása – több, mint **75 M Euro** összértékben
- Tanácsadás – több, mint **150** sikeres projekt **11** országban

Önnek miben segíthetünk?

Lépjünk kapcsolatba most!

www.jasipos.com