" Louis, I think this is the beginning of a beautiful friendship."

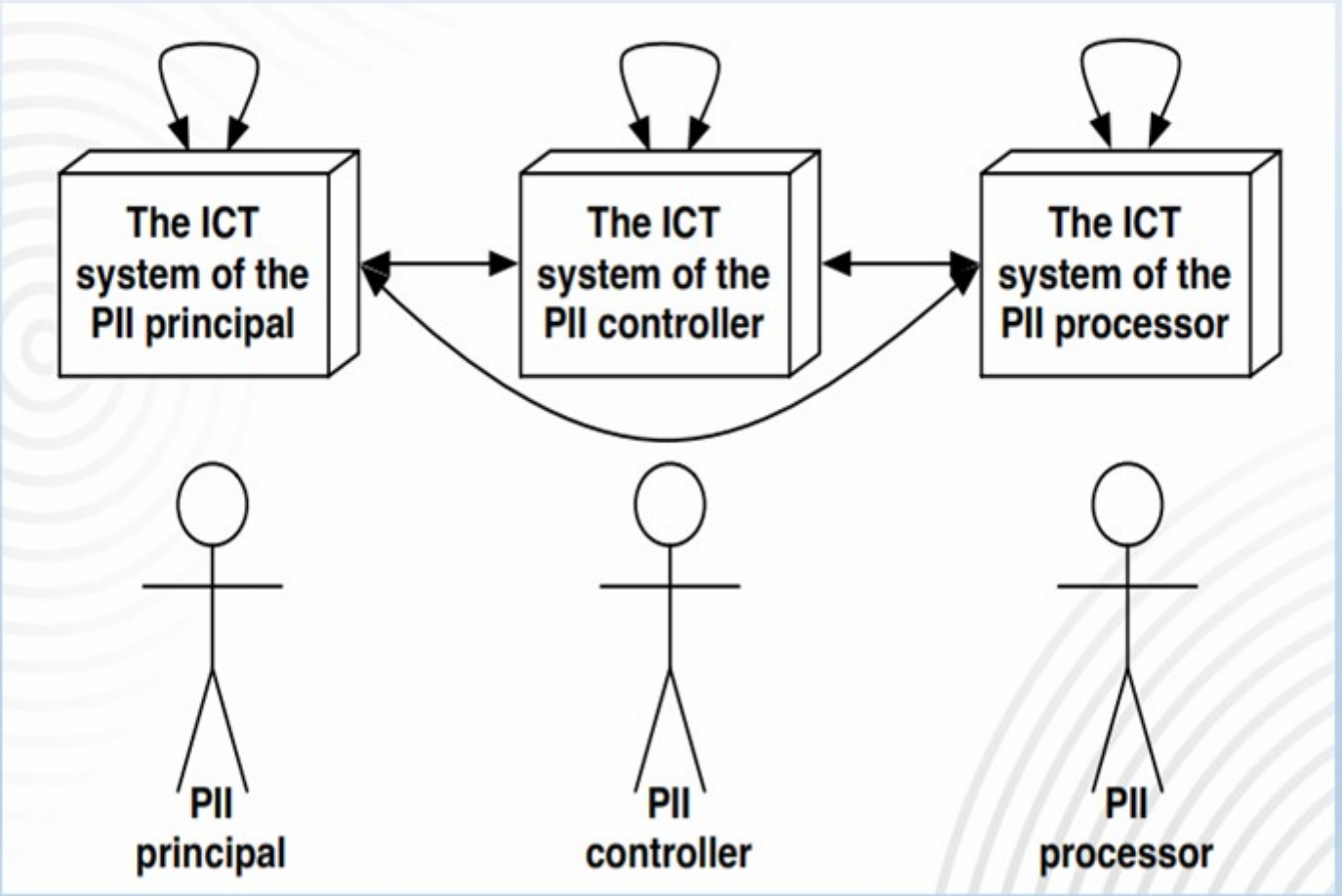
(Rick)

avagy

Szinergiák az adatvédelmi- és az információbiztonsági szabványokban.

Dr. Farkas Tamás
adatvédelmi szakjogász

Adatvédelmi szerepkörök



ISO/IEC 29100:2011 alapelvei I.

- **Hozzájárulás és önkéntesség** (5.2 Consent and choice)
- **Célhoz kötöttség és jogalapok** (5.3 Purpose legitimacy and specification)
- **Az adatkezelés korlátozása** (5.4 Collection limitation)
- **Adatminimalizálás** (5.5 Data minimalization)
- **Felhasználás, megőrzés és a hozzáférés korlátozása** (5.6 Use, retention and disclosure limitation)

ISO/IEC 29100:2011 alapelvei II.

- **Pontosság és minőség** (5.7 Accuracy and quality)
- **Nyitottság, átláthatóság és tájékoztatás** (5.8 Openness, transparency and notice)
- **Az egyéni részvétel és hozzáférés** (5.9 Individual participation and acess)
- **Számonkérhetőség** (5.10 Accountability)
- **Az információbiztonság** (5.11 Information security)
- **Adatvédelmi rendelkezések betartása** (5.12 Privacy compliance)

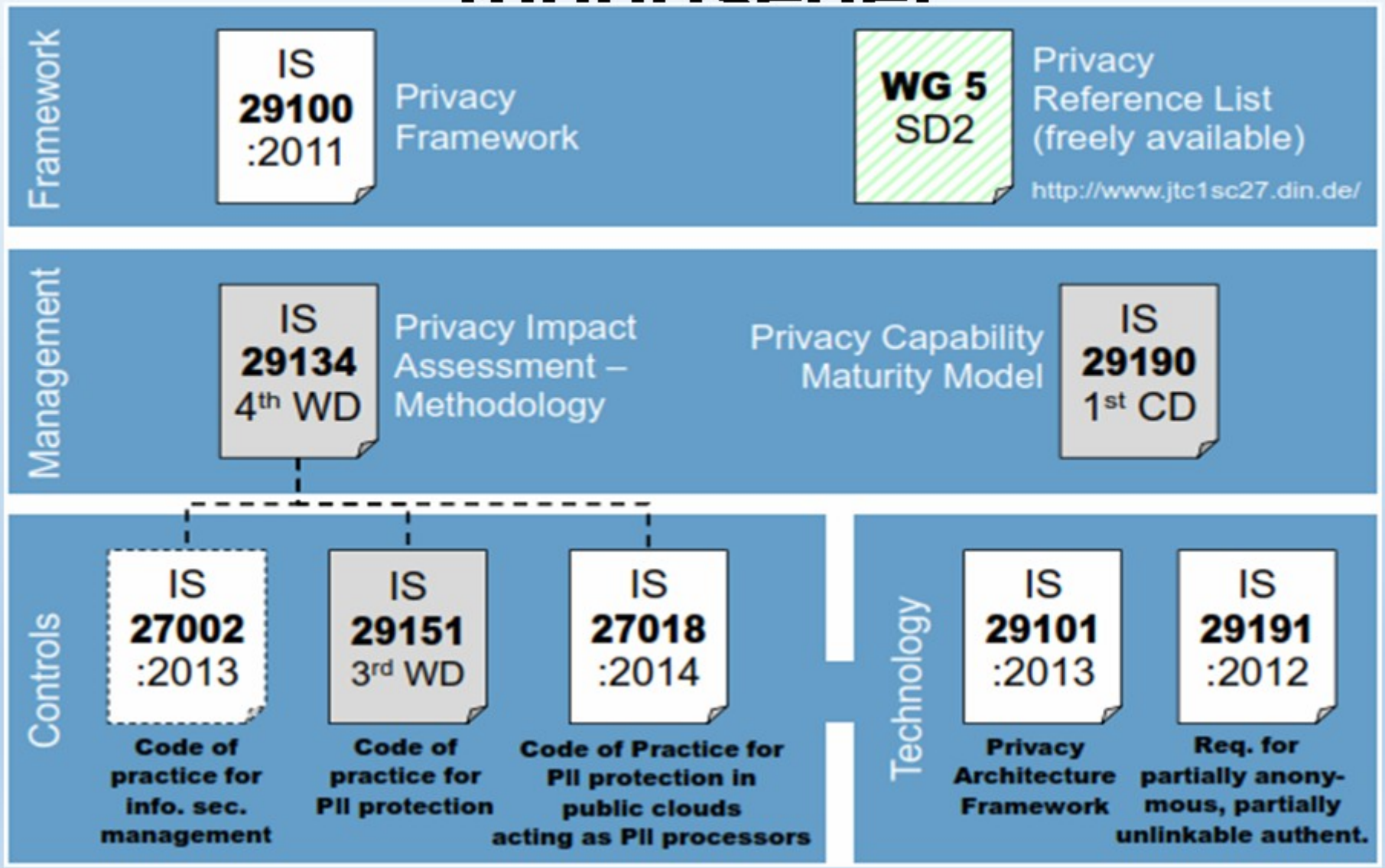
Alapfogalmak összevetése

ISO 29100 család	ISO 27000 család
Privacy stakeholder (PII principal, controller, processor)	Stakeholder
PII (Personaly Identified Information)	Information asset
Privacy breach	Information securíty incident
Privacy control	Control
Privacy risk	Risk
Privacy risk management	Risk manegement
Privacy safeguarding requirements	Control objectives

Közös felületek

ISO 29100	ISO 27001
Hozzáférés korlátozása	Bizalmasság
Megőrzés	Sértetlenség, Rendelkezésre állás
Pontosság, minőség	Sértetlenség, Rendelkezésre állás
Számonkérhetőség	Számonkérhetőség
Információbiztonság	Minden IBIR alapelv
Átláthatóság	Hitelesség, letagadhatatlanság

A szabványok kölcsönös függőségei



Adatvédelmi hatásvizsgálat

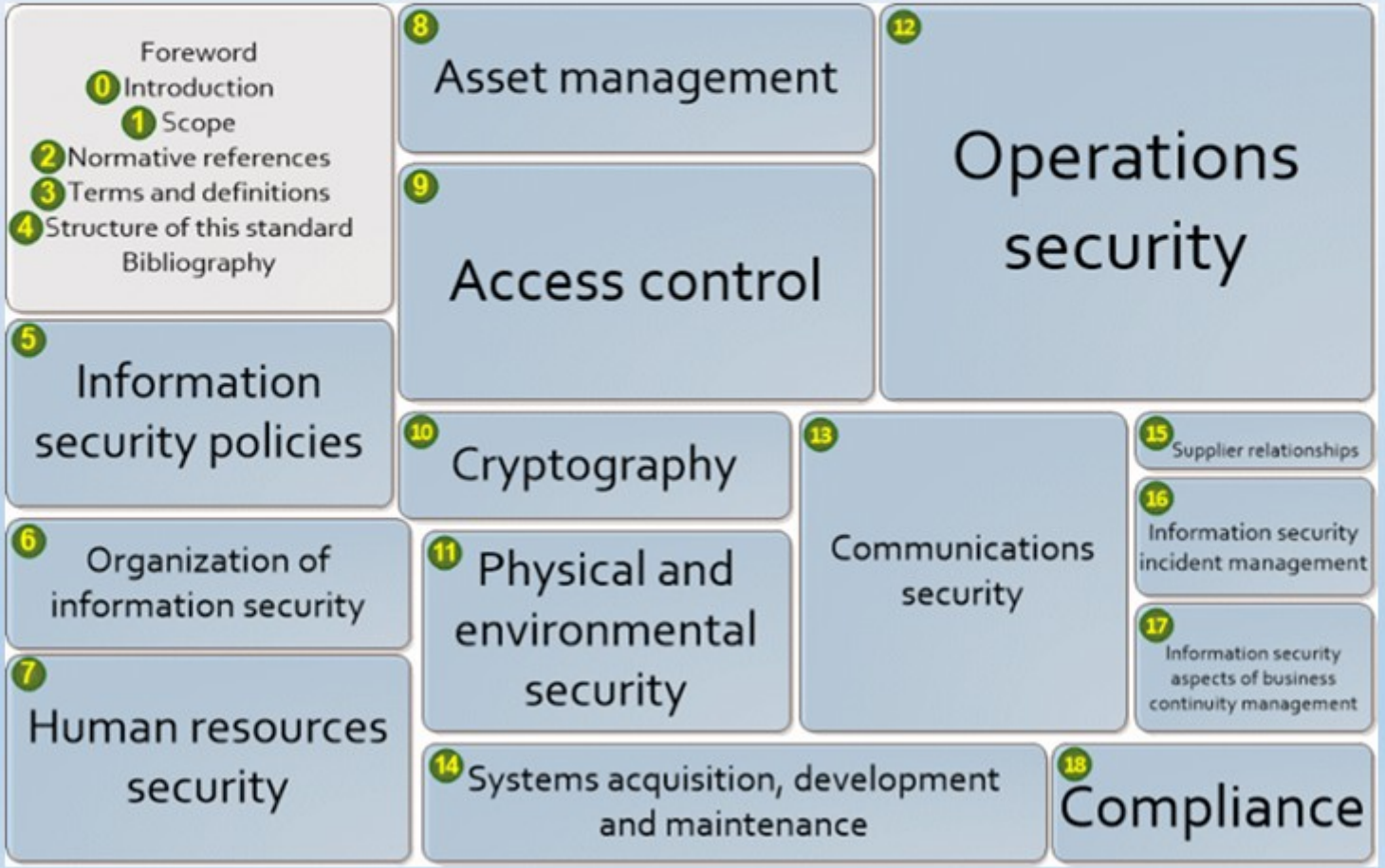
(Privacy Impact Assessment IS 29134 4th WD)

Adatvédelmi kockázatok azonosítása(6.2.3.1)

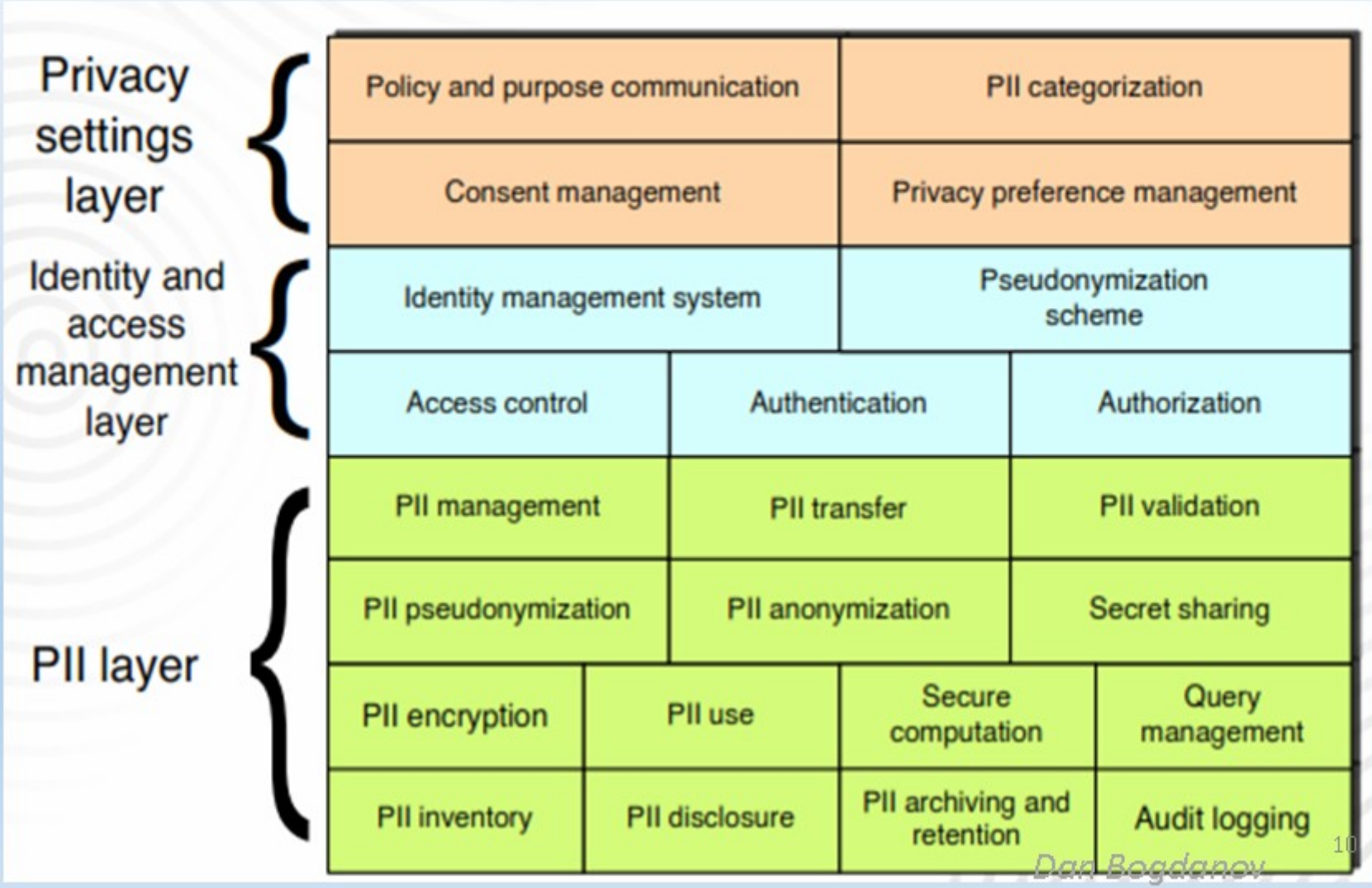
- Jogosulatlan személy hozzáférése a PII-hoz (bizalmasság elvesztése); IBIR
- PII adatvesztés módosítás miatt (sértetlenség); IBIR
- PII-adatvesztés eltűnés miatt (rendelkezésre állás); IBIR
- PII jogellenes összekapcsolása (az adatok érintetthez rendelhetővé válása);
- Az adatkezelésre vonatkozó információk visszatartása PII-vesztés (átláthatóság);
- Jogalap és célhoz kötöttség nélküli adatgyűjtés (irányítás elvesztése)

Az adatkezelő és az adatfeldolgozó vonatkozásában is!

ISO/IEC 27002:2013 szabályozási területei



Az adatvédelemi rétegek ISO/IEC 29101:2013



Dan Bogdanov

Jogi vonzatok

Adatvédelem

- 95/46 EK EU irányelv
- 2011. CXII. Tv. Infotv.
- Ágazati törvények: Ehtv, Grt, Ekert, Dmt, Eüaktv
- 29. WP, NAIH vélemények, ajánlások, határozatok

Információbiztonság

- 2013. L. tv. Ibtv
- Végrehajtási rendeletek

Javaslatok

- Követelmények naprakész ismerete!
- A folyamatokat és a támogató szakemberek megnyerése!
- A szükséges intézkedések megtervezése!
- Szabályozási környezet kialakítása!
- A célok és a szabályok kommunikálása!
- Az érdekeltek tájékoztatása, képezése és oktatása!
- A szabályok betartásának, betarthatóságának ismerete!
- A változások követése!

Nyitott kérdések

- Hogy kezeljük a fenntartásokat?
- Mi tehető mindenki számára megismerhetővé?
- Hogy kezeljük az IB és az AV ütközéseit? (biztonsági mentések, zárolás)
- ?
- ?
- ?

Köszönöm a figyelmet!