NIS2 a architektura kybernetické bezpečnosti

Luděk Novák; ISACA CRC

7. února 2024

ISACA
Czech Republic Chapter

Obsah

ISACA Czech Republic Chapter

Terminologie informační a kybernetické bezpečnosti

ISO/IEC 27001 (2005, 2013, 2022)	ČSN ISO/IEC 27001:2006	ČSN ISO/IEC 27001:2014	ČSN ISO/IEC 27001:2023	VKB:2014	VKB:2018	Optimální způsob překladu
Information security	Bezpečnost informací	Bezpečnost informací	Informační bezpečnost	Bezpečnost informací	Bezpečnost informací	Informační bezpečnost
Information Security Management	Management bezpečnosti informací	Řízení bezpečnosti informací	Management informační bezpečnosti	Řízení bezpečnosti informací	Řízení bezpečnosti informací	Řízení informační bezpečnosti
Information Security Management System	Systém managementu bezpečnosti informací	Systém řízení bezpečnosti informací	Systém managementu informační bezpečnosti	Systém řízení bezpečnosti informací	Systém řízení bezpečnosti informací	Systém řízení informační bezpečnosti
N/A	N/A	N/A	N/A	Řízení kybernetické bezpečnosti	Řízení kybernetické bezpečnosti	Řízení kybernetické bezpečnosti
Risk Management	Management rizik	Řízení rizik	Management rizik	Řízení rizik	Řízení rizik	Řízení rizik
Information Security Risk Assessment	Hodnocení rizik (bezpečnosti informací)	Posuzování rizik bezpečnosti informací	Posouzení rizika informační bezpečnosti	Hodnocení rizik (bezpečnosti informací)	Hodnocení rizik (bezpečnosti informací)	Hodnocení rizik informační bezpečnosti
Information Security Risk Treatment	Zvládání rizik (bezpečnosti informací)	Ošetření rizik bezpečnosti informací	Ošetření rizika informační bezpečnosti	Zvládání rizik (bezpečnosti informací)	Zvládání rizik (bezpečnosti informací)	Zvládání rizik informační bezpečnosti
Risk Treatment Plan	Plán zvládání rizik (bezpečnosti informací)	Plán ošetření rizik bezpečnosti informací	Plán ošetření rizika informační bezpečnosti	Plán zvládání rizik (bezpečnosti informací)	Plán zvládání rizik (bezpečnosti informací)	Plán zvládání rizik informační bezpečnosti
Statement of applicability	Prohlášení o aplikovatelnosti	Prohlášení o aplikovatelnosti	Prohlášení o aplikovatelnosti	Prohlášení o aplikovatelnosti	Prohlášení o aplikovatelnosti	Prohlášení o aplikovatelnosti

Co víme? (1)

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti § 7:

Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla **zajištěna bezpečná architektura informačního a komunikačního systému**, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti

a) po dobu nejméně tří let, nebo

b) po dobu jednoho roku, pokud absolvovala studium na vysoké škole.

Vyhláška o kybernetické bezpečnosti (návrh) :

Architekt kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna **bezpečná architektura regulované služby**, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti

a) po dobu nejméně tří let, nebo

b) po dobu jednoho roku, pokud absolvovala studium na vysoké škole.

ISACA Czech Republic Chapter

Co víme? (2)

- **Architektura**: Struktura systému nebo služby IT zahrnující vzájemné vztahy mezi komponentami a prostředím, ve kterém se nacházejí. Architektura také obsahuje normy/standardy a směrnice, které usměrňují návrh a rozvoj systému. (ITIL v3, Slovníček termínů, definic a zkratek, itSMF Czech Republic, o.s.)
- **Architektura podniku / úřadu**: Úroveň detailu popisu architektury úřadu jako celku, dílčí schopnosti nebo odpovídajícího funkčního celku, zaměřená na to, jaké prvky a proč v této architektuře existují.
- **Architektura úřadu**: Architektura úřadu jako manažerská metoda je prostředkem celostního poznávání organizace na podporu rozhodování, zejména při plánování strategických změn, ale také na podporu řízení výkonnosti, kvality a zodpovědnosti.
- **Architektura řešení**: Úroveň detailu popisu architektury dílčí schopnosti úřadu nebo odpovídajícího funkčního celku, zaměřená na to, jak prvky architektury fungují nebo mají fungovat.
- **Architektura (systému)**: Struktura komponent / prvků, jejich vzájemných vazeb a principů a návodů řídících jejich návrh a vývoj v čase.
- **Architektura veřejné správy**: Architektura veřejné správy jako socio-ekonomicko-technického systému je souborem prvků, které tvoří strukturu systému, jejich vzájemných vazeb, jejich chování (fungování) a principů a pravidel jejich vzniku a vývoje v průběhu času.
- **Architektura rizik a bezpečnosti**: postihuje specifické bezpečnostní aspekty napříč doménami

Zdroj: https://archi.gov.cz/slovnik_egov

ISACA Czech Republic Chapter

Co nevíme? (1)

Co má činit architekt kybernetické bezpečnosti?

Vyhláška č. 82/2018, § 7, Bezpečnostní role

(1) **Manažer kybernetické bezpečnosti**

a) je bezpečnostní role odpovědná za systém řízení bezpečnosti informací, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením kybernetické bezpečnosti nebo s řízením bezpečnosti informací

1. po dobu nejméně tří let, nebo

2. po dobu jednoho roku, pokud absolvovala studium na vysoké škole,

b) odpovídá za pravidelné informování vrcholového vedení o

1. činnostech vyplývajících z rozsahu jeho odpovědnosti a

2. stavu systému řízení bezpečnosti informací a

c) nesmí být pověřen výkonem rolí odpovědných za provoz informačního a komunikačního systému.

(2) **Architekt kybernetické bezpečnosti** je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla **zajištěna bezpečná architektura** informačního a komunikačního systému, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti

a) po dobu nejméně tří let, nebo

b) po dobu jednoho roku, pokud absolvovala studium na vysoké škole.

ISACA Czech Republic Chapter

Co nevíme? (2)

Co je to architektura kybernetické bezpečnosti?

- Architektura rizik a bezpečnosti (DIA)

- Bezpečná architektura informačního a komunikačního systému (VKB)
- Architektura bezpečnosti (VKB)
- Bezpečnostní architektura (VKB)
- Topologie infrastruktury (VKB)
- Segmentace infrastruktury (VKB)

- Bezpečná architektura regulované služby (nVKB)
- Architektura bezpečnosti (nVKB)
- Bezpečnostní architektura (nVKB)

- Architektury systému regulované služby (nVKB)
- *Architektura systému (nVKB)*
- *Architektura informačního a komunikačního systému (nVKB)*
- Topologie infrastruktury (nVKB)
- Segmentace infrastruktury (nVKB)

ISACA Czech Republic Chapter

Architektura kybernetické bezpečnosti

Významná nejasnost současné regulace KB:

- Existuje Architekt Kybernetické bezpečnosti, ale v podstatě nemá žádné regulované úkoly ani výstupy

Vazby a souvislosti je nezbytné systematicky řešit

Architektura kybernetické bezpečnosti (obrázek) usnadňuje pochopení problematiky (významně jednodušeji než většina rizikových analýz)

Vhodným využitím „architektury kybernetické bezpečnosti“ získává řada regulačních požadavků vyšší kvalitu a vyzrálost

- Vazby mezi aktivy, závislosti na dodavatelích apod.

ISACA Czech Republic Chapter

Proč architektura kybernetické bezpečnosti?

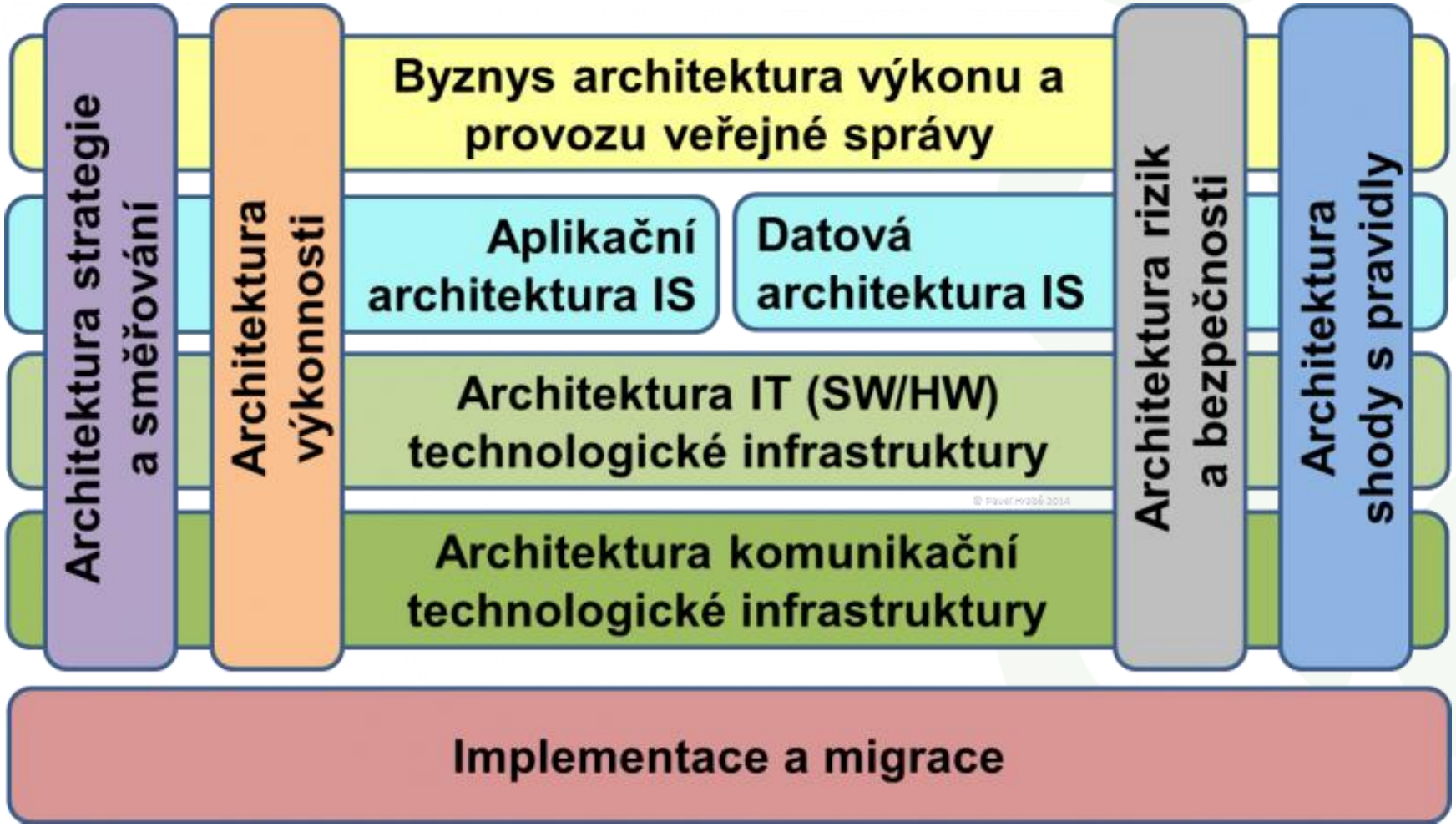
Střední škola: obrázek je lepší než několik stran popisu

Zkušenost z auditu: máme obrázky, ale nikdo je neukazuje

Potřebujeme užitečné „obrázky“ pro řízení informační a kybernetické bezpečnosti!

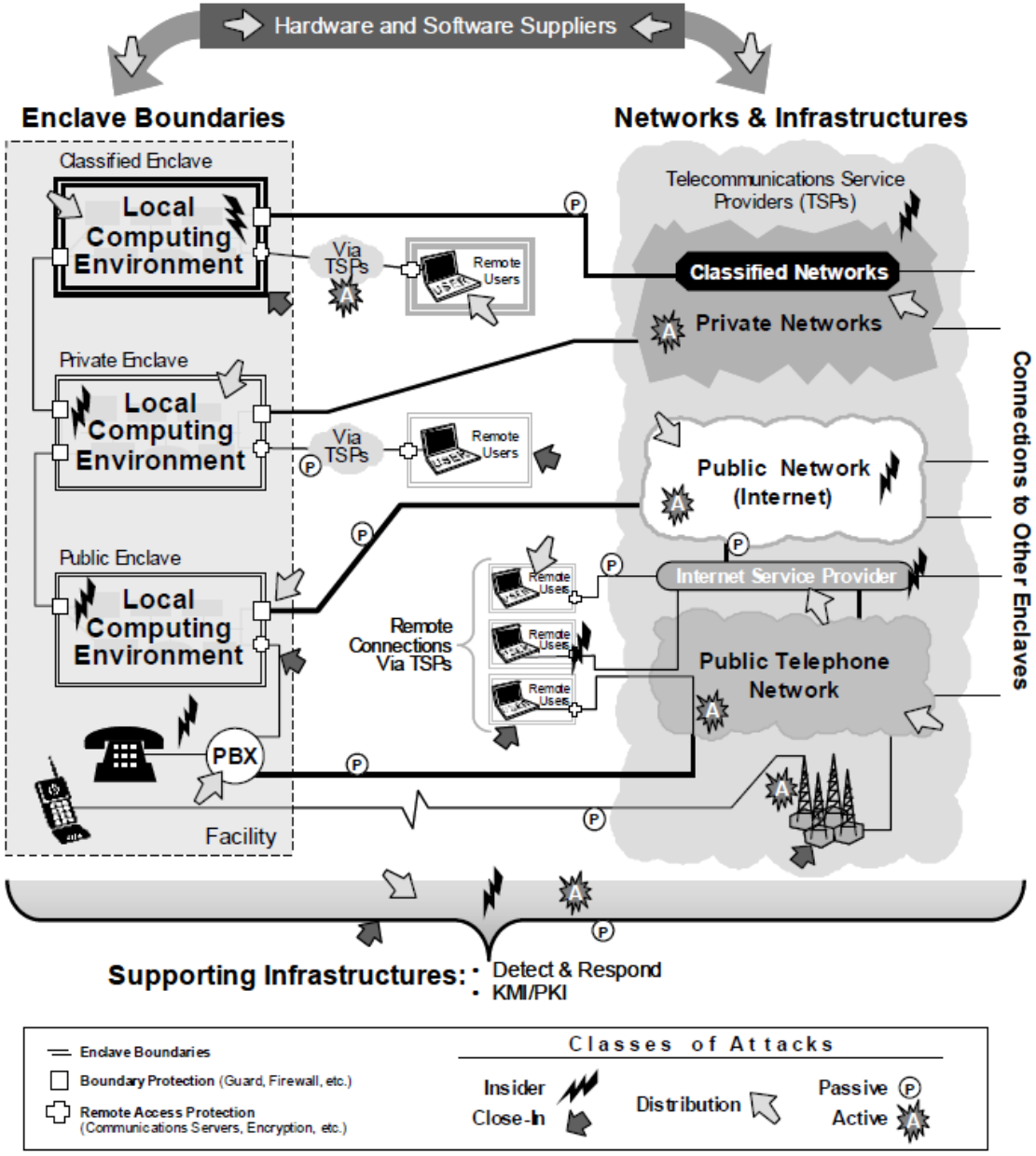
ISACA Czech Republic Chapter

Přístup hlavního architekta eGovernment



Zdroj: https://archi.gov.cz/nar_dokument:struktura_modelovanych_architektur

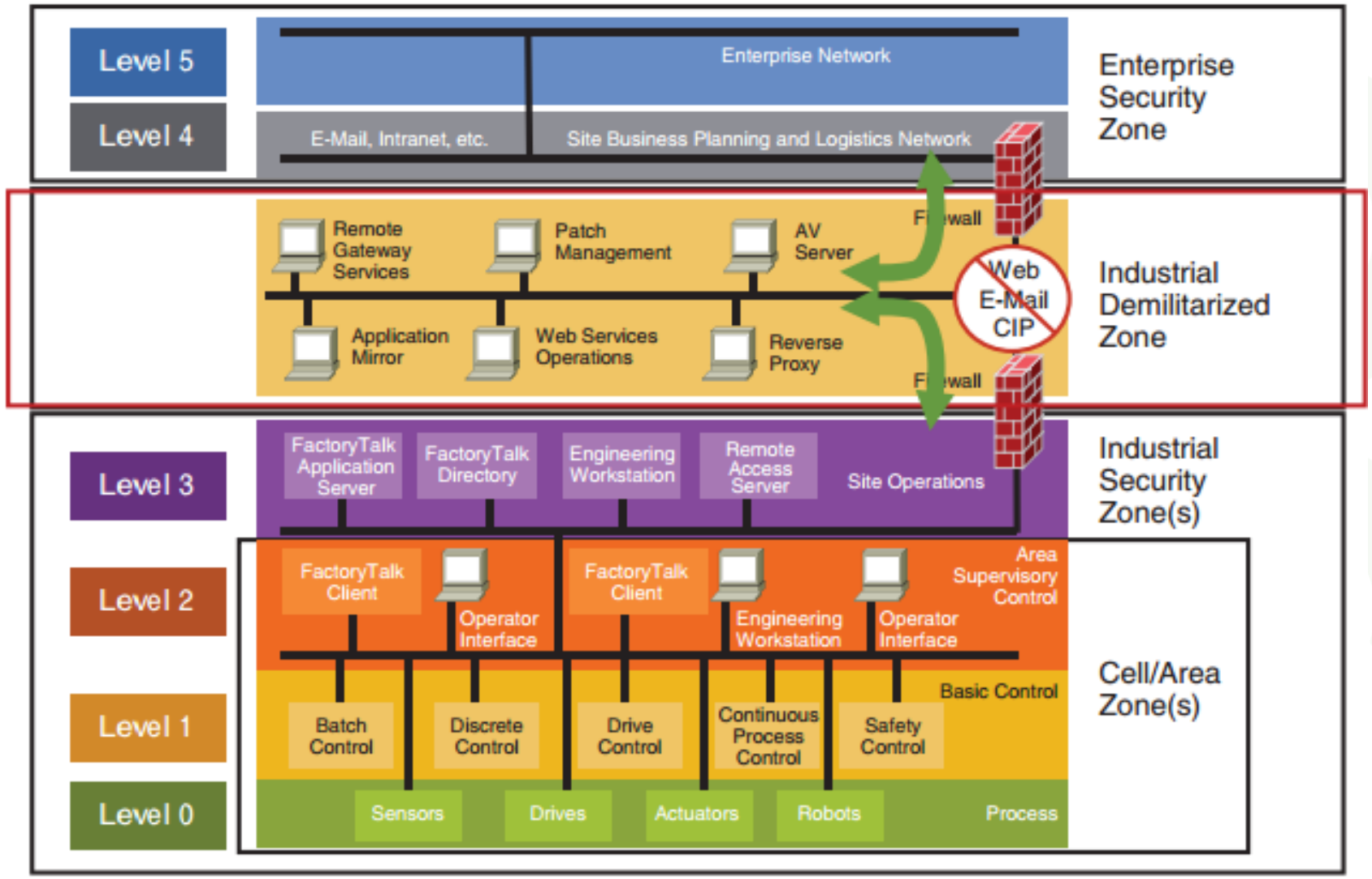
Příklad řešení: Ochrana v hloubce



Zdroj: IATF framework

ISACA Czech Republic Chapter

Příklad řešení: Purdue model



Enterprise:

- **Level 5**: Enterprise network
- **Level 4**: Site business and logistics

Industrial Demilitarized zone

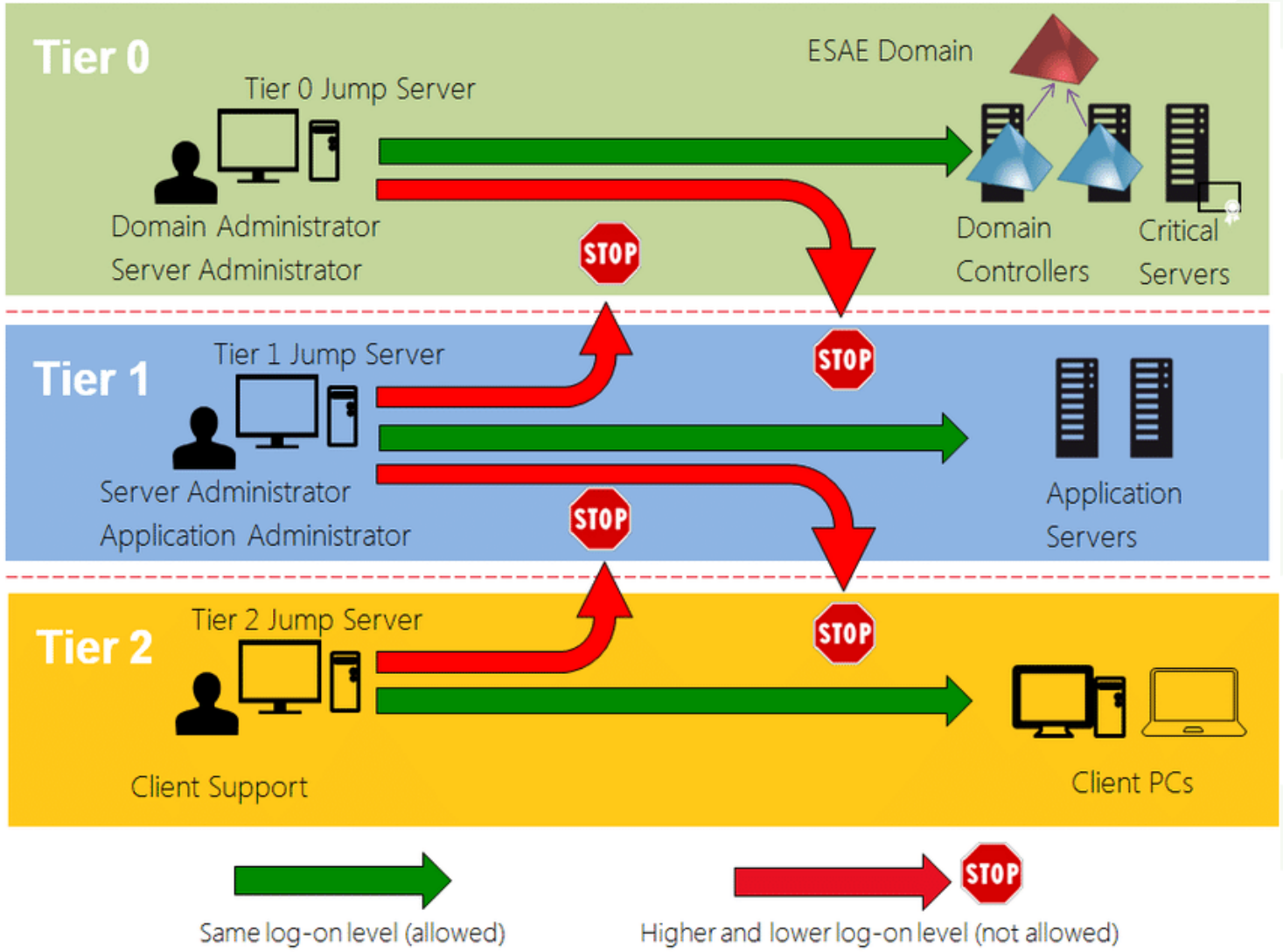
Manufacturing zone (Industrial zone):

- **Level 3**: Site operations
- **Level 2**: Area supervisory control
- **Level 1**: Basic control
- **Level 0**: The process

Zdroj: https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems

ISACA Czech Republic Chapter

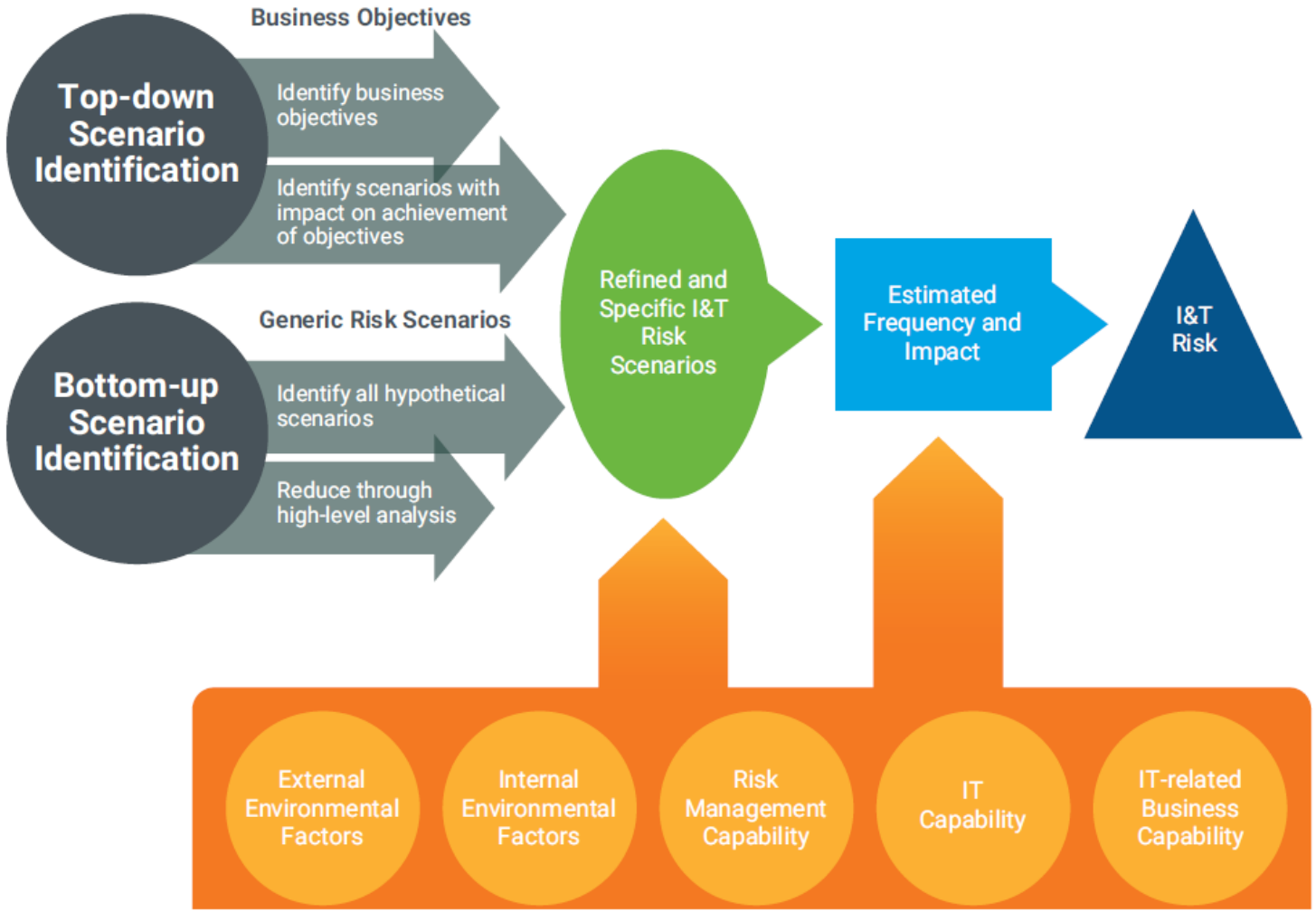
Příklad řešení: TIER model pro administraci



Zdroj: https://www.researchgate.net/figure/Modified-Microsofts-administrative-three-tier-Model-2_fig2_293807740

ISACA Czech Republic Chapter

Metodika ISACA: Risk IT



Zdroj: Risk IT (2020)

Významné kategorie rizikových scénářů:

- Rozhodování spojené s investicemi do IT
- Řízení životního cyklu programů a projektů
- Přehled o výdajích v rámci IT
- IT odbornost, dovednosti a chování
- Architektura organizace/IT
- Řízení dat a informací
- …

Výzvy

Zvládnutí zavedení NIS2/ZKB

- Nízká míra inovací spojených s řízením informační a kybernetické bezpečnosti

Neopakovat chyby související s GDPR

Architektura kybernetické bezpečnosti je účinným nástrojem pro všechny

Závěr

Architektura kybernetické bezpečnosti je klíčovým prvkem zvládnutí současných výzev informační a kybernetické bezpečnosti

Architektura kybernetické bezpečnosti účinně pomůže při pochopení a rozvoji

Užitečný obrázek je více než řada popisného textu

Znalosti se dají pomocí architektury relativně rychle a jednoduše sdílet

Máme se na co těšit!

ISACA Czech Republic Chapter

Kontakt

Luděk Novák
ISACA CRC
T: + 420 603 248 295
E: ludekn@email.cz

ISACA
Czech Republic Chapter