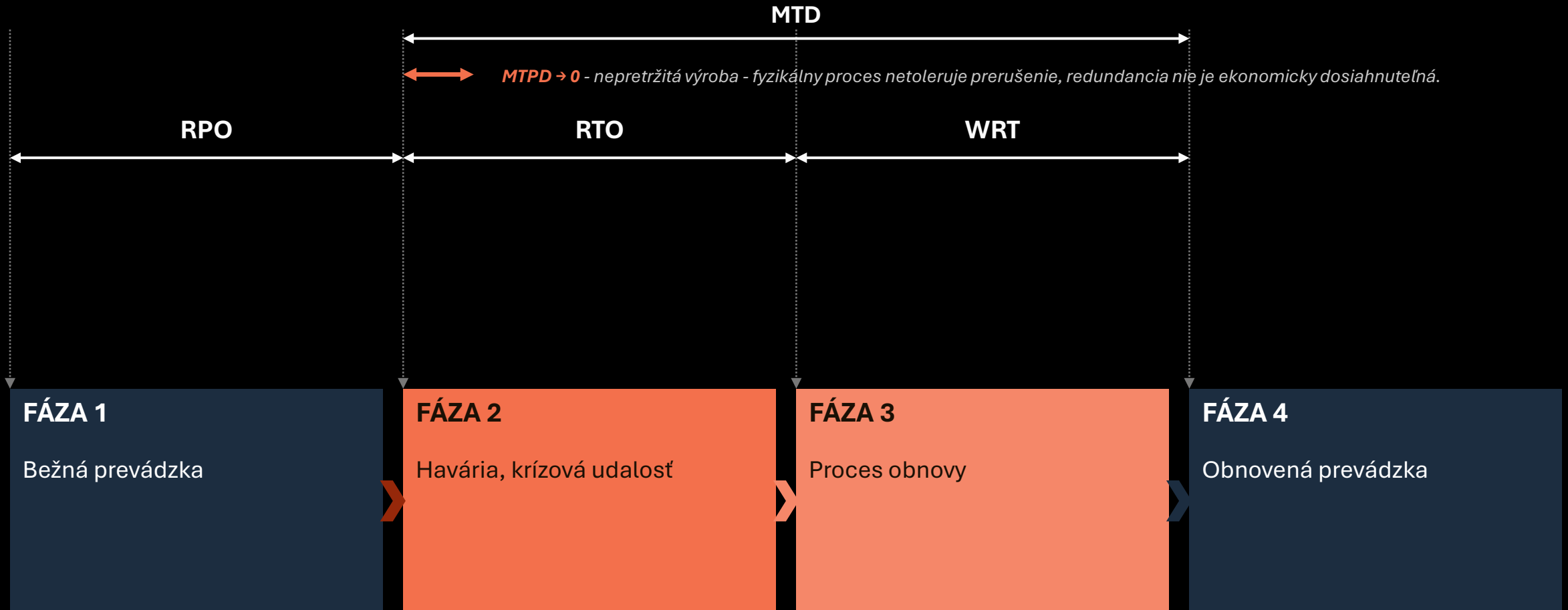


Analýza funkčného vplyvu (BIA)

BIA podľa ISO/TS 22317 vo výrobných podnikoch

BCM intervaly v kontexte **stavu prevádzky**



Jadro prezentácie: **RTO** a jeho základ

"RTO systému X bolo stanovené na 24 hodín - pri úniku dát by hrozila pokuta a poškodenie dobrého mena. Výpadok toho istého systému však okamžite zastavuje výrobnú linku."

Dopad z kompromitácie dát, alebo dopad z výpadku prevádzky?

Odpoveď sa vrátime na záverečnom slajde.

Mechanizmus zámeny typu dopadu pri určovaní RTO

Osem typov dopadu (5.3.2)

Obchodné ciele

Business objectives

Environmentálny

Environmental

Finančný

Financial

Zdravie a bezpečnosť

Health & safety

Právny / zmluvný

Legal/regulatory/contractual

Podiel na trhu

Market share

Prevádzkový

Operational

Reputačný

Reputational

Organizácia si volí, ktoré typy dopadu bude v BIA sledovať - tvoria spoločný slovník pre celý zvyšok metodiky.

Mechanizmus **nesprávneho** určenia RTO

Otázka, na ktorú sa (nesprávne) odpovedá

Aké legal/regulačné a reputačné riziko hrozí pri úniku dát z tohto systému?

→ typy dopadu: legal/regulatory, reputational

Otázka, na ktorú treba odpovedať

Aký prevádzkový dopad má výpadok tejto aktivity na výrobu?

→ typy dopadu: operational, business objectives

RTO patrí k pravej otázke - nie k ľavej. Obe sú legitímne typy dopadu podľa 5.3.2; chybou je zámena, nie voľba mimo normy.

CIA verzus AIC

Bežná OT/IT konvencia - AIC nie je formálny ISO termín

CIA - bežná IT hierarchia

Confidentiality → Integrity →
Availability

Dostupnosť je ekonomicky
obnoviteľná redundanciou a
failoverom - je až tretia.

AIC - konvencia nepretržitej výroby

Availability → Integrity →
Confidentiality

Fyzikálny proces netoleruje
prerušenie a redundancia
veľkých celkov je nedosiahnuteľná.

Priorita sa preklápa presne vtedy, keď MTPD konverguje k nule (slajd 2) - dostupnosť prestáva byť jednou z priorít a stáva sa dominantnou.

Prečo servisná/IT šablóna **vo výrobe zlyháva**

1 Norma pokrýva osem kategórií zdrojov (5.6.1).

Ľudia, dáta, fyzická infraštruktúra, zariadenia, ICT, logistika, financie, dodávatelia - rovnocenne.

2 Servisná šablóna **zvyhodňuje dáta a ICT.**

Formulár aj mentálny model facilitátora sú postavené okolo kategórií b) a e).

3 Fyzické a dodávateľské závislosti zostanú nezachytené.

Kategórie c), d), h) sa vyplňajú povrchno alebo vôbec - nie preto, že ich norma neuvádza.

Toto je odlišný mechanizmus od zámeny typu dopadu na predchádzajúcom slajde - tu ide o kategórie zdrojov (5.6.1), nie o typy dopadu (5.3.2).

Výsledok

Fyzické a dodávateľské SPOF zostávajú nezachytené - šablóna sa na ne nepýta.

Miesto ISO/TS 22317 v systéme ISO

ISO 22301:2019

Požiadavky BCMS.
Normové zakotvenie BIA -
klauzula 8.2.

ISO/TS 22317

Metodika implementácie BIA
(táto prezentácia).

ISO/TS 22331

Nadväzujúci výber
stratégií kontinuity.

Kritický produkt **nie je** kritický proces

Prioritu produktu určuje top manažment (5.4).

Procesy a čiastkové aktivity sa posudzujú osobitne.

Vysoko prioritný produkt môže mať nízko-prioritný čiastkový proces.

Kritickosť produktu nemožno automaticky preniesť na každý proces, ktorý sa naň viaže.

Single Point of Failure - **jediný bod zlyhania**

Prvok systému, ktorého porucha spôsobí zlyhanie celého systému alebo kritickej služby, pretože nemá funkčnú náhradu.

Príklady

- jediný server bez zálohy
- jediný internetový prívod
- jediný administrátor poznajúci kritický postup
- jediný dodávateľ služby
- jediný zdroj dát pre AI systém

Nielen technický problém

Môže ísť aj o človeka, proces, dodávateľa alebo rozhodovaciu právomoc.

Odstraňuje sa najmä redundanciou, zastupiteľnosťou, zálohovaním a otestovaným postupom obnovy.

Kde sa vo výrobe **skrýva SPOF**

Zariadenie - napr. jediný CNC stroj na kritickej operácii.

Fyzická infraštruktúra.

Dodávateľ alebo logistika bez alternatívy.

Podcenený zber neznamená
iba nepresné RTO
Môže skryť SPOF (5.6.2)

Prehľad procesu BIA - kapitola 5



Tento diagram (podľa Figure 3 normy, rozšírený o informatívnu validačnú techniku) je navigačnou mapou pre nasledujúce slajdy.

Plánovanie BIA

Alokácia zdrojov

Kompetentní ľudia a zdroje pre proces.

Zoskupovanie produktov

Podľa typu, geografie alebo línie biznisu.

Komunikačný plán

Očakávania participantov a harmonogram.

Rozsah a hranice

Ktoré jednotky a produkty sú zahrnuté.

Metodika zberu dát

Dotazníky, workshopy, rozhovory.

Kritériá úspešnosti

Kedy je BIA kompletná a schváliteľná.

Dohoda na prístupe

Typy dopadu - 8 kategórií (5.3.2).

Časové rámce a worst-case scenár (5.3.4 a).

Pravidlo $RTO \leq MTPD$ (5.3.4 c).

MTPD / RTO vzťah

**MTPD = max. tolerovaná doba
prerušenia aktivity.**

**RTO = čas do obnovy -
vždy kratší než MTPD.**

Priority a stanovenie RTO

Top manažment



Priority produktov a služieb (5.4)

Vlastníci aktivít



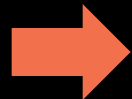
MTPD a RTO pre každú aktivitu (5.5)

BIA líder



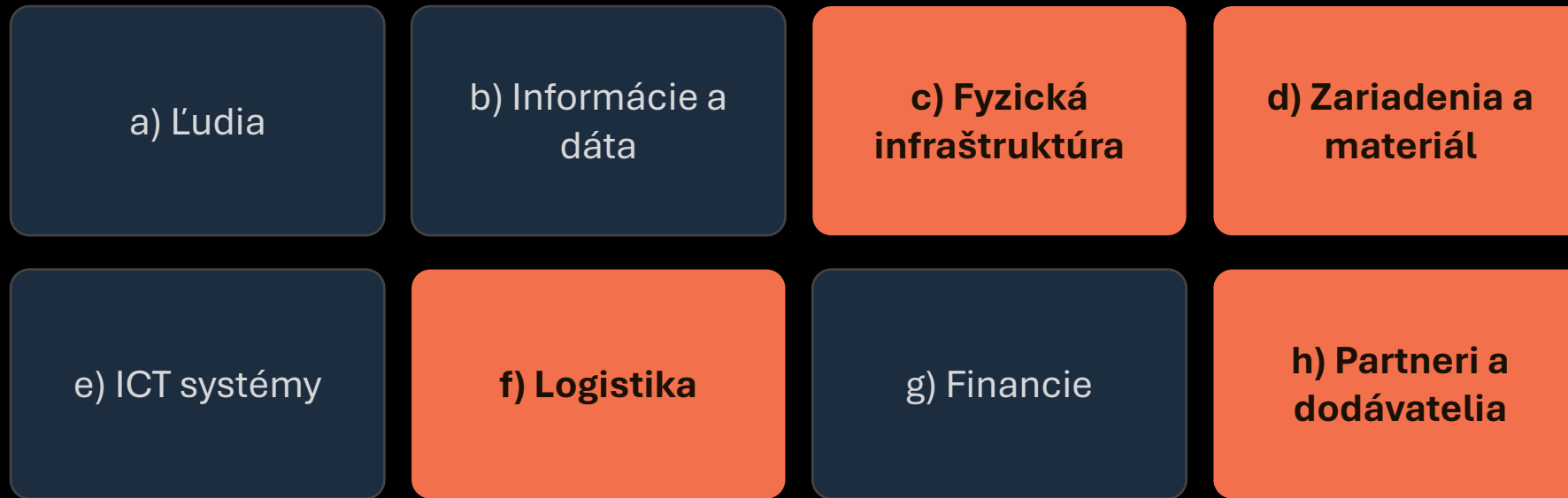
Konsolidácia, kontrola konzistentnosti

Top manažment



Schválenie (5.8)

Identifikácia zdrojov a závislostí - SPOF



Zvýraznené: výrobné kritické kategórie, kde najčastejšie vzniká SPOF.

BIA identifikuje SPOF.

Ich analýza patrí do risk assessmentu (Annex C.5).

Konsolidácia a schválenie BIA

Krok 1 - Kvalita dát (5.7)

Correct

Credible

Consistent

Current

Complete

Krok 2 - Schválenie (5.8)

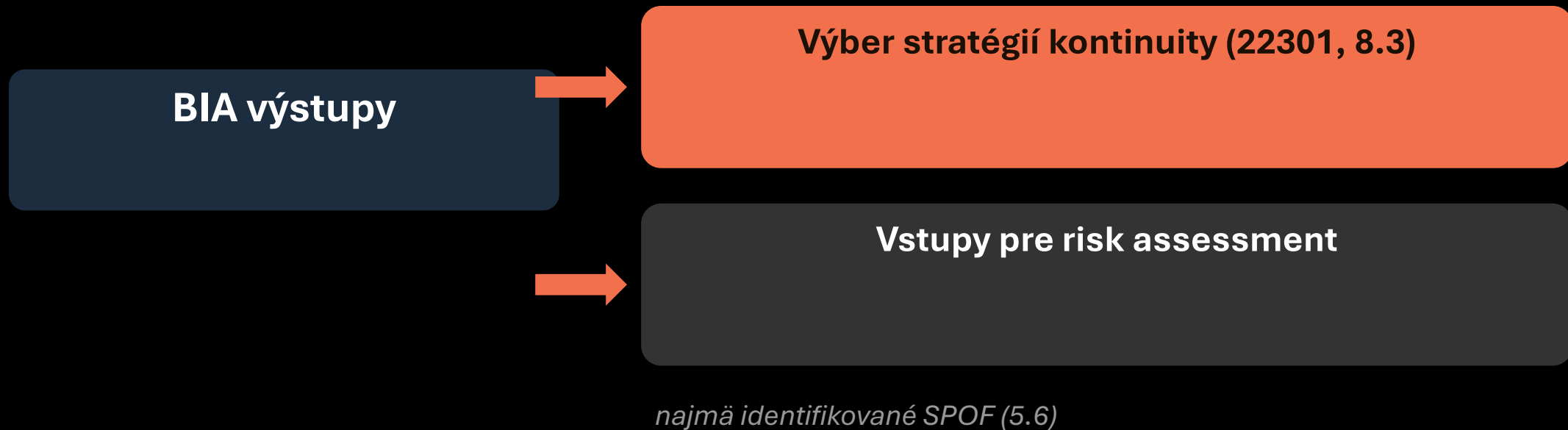
Schvaľuje top manažment

Potvrďuje priority a RTO

Až potom nasleduje výber

stratégií (ISO/TS 22331)

BIA ako vstup do ISO 22301 a ISO 31000



ISO 31000 - praktická interpretácia, nie citácia normy

Klíčové posolstvo

Zakotvené v 5.3.2 a 5.5

Vo výrobnom podniku RTO nemá odrážať legal/regulačný a reputačný dopad prípadného úniku dát - má odrážať prevádzkový dopad výpadku aktivity (zastavenie výroby) a čas, po ktorom sa tento dopad stáva neprijateľným (MTPD).

Kontrolná otázka

Ktorý typ dopadu (5.3.2) bol pri tomto RTO skutočne použitý - a je to ten správny?

Normový odkaz: typy dopadu 5.3.2, vzťah RTO/MTPD 5.3.4 c, validovateľné technikou z Annex D.3.

BIA pre výrobný podnik: špecifiká

Dostupnosť je prvá priorita - AIC, nie CIA.

Pri nepretržitých procesoch sa MTPD blíži k nule (slajd 2, 6).

RTO odráža prevádzkový dopad, nie riziko úniku dát.

Zámena typu dopadu legal/reputačný ↔ operačný (5.3.2, slajd 5).

Kritický produkt ≠ kritický proces.

Priorita produktu sa neprenáša automaticky na každý čiastkový proces (5.4).

Fyzické SPOF unikajú pozornosti.

Kategórie c) d) h) - infraštruktúra, zariadenia, dodávatelia - sú v IT šablónach podcenené (5.6.1).

Norma s výrobou explicitne počíta.

Annex C.2 prepája časové požiadavky výroby so zásobami surovín a dielov.

Ďakujem za pozornosť

Kontakt

Makatura & Semančín, s.r.o.

makaturasemancin.sk

imakatura@makaturasemancin.sk

linkedin.com/in/makatura

Prezentácia dostupná na požiadanie.

Annex D.1 - kompletný príklad



Annex D.2 - alternatívna metodika

Prahový prístup (D.1-D.7)

Princíp: vopred definované prahy MTPD.

Kontext: jednoduchší, rýchlejší.

Výsledok: MTPD a RTO.

Impact matica (D.8-D.11)

Princíp: kvalitatívny popis úrovni dopadu.

Kontext: detailnejší, konzistentnejší.

Výsledok: MTPD a RTO.

Obe metodiky vedú k rovnakému výstupu - líšia sa v spôsobe zdôvodnenia rozhodnutia.

Výpočet impact ratingu

Customer Help Desk

39

RTO 3 dni - nad trendom

Accounts Payable

14

RTO 3 dni - pod trendom

Rovnaké RTO nemusí znamenať porovnateľný dopad.

Annex C.2 - výrobný kontext v norme

"Knowing the time imperatives of various parts of a manufacturing process can improve the optimization of stocks of raw materials or spare parts."

- ISO/TS 22317, Annex C.2

BLA prepája časové požiadavky výroby so zásobami surovín a náhradných dielov.

Informatívna príloha - nie normatívna požiadavka

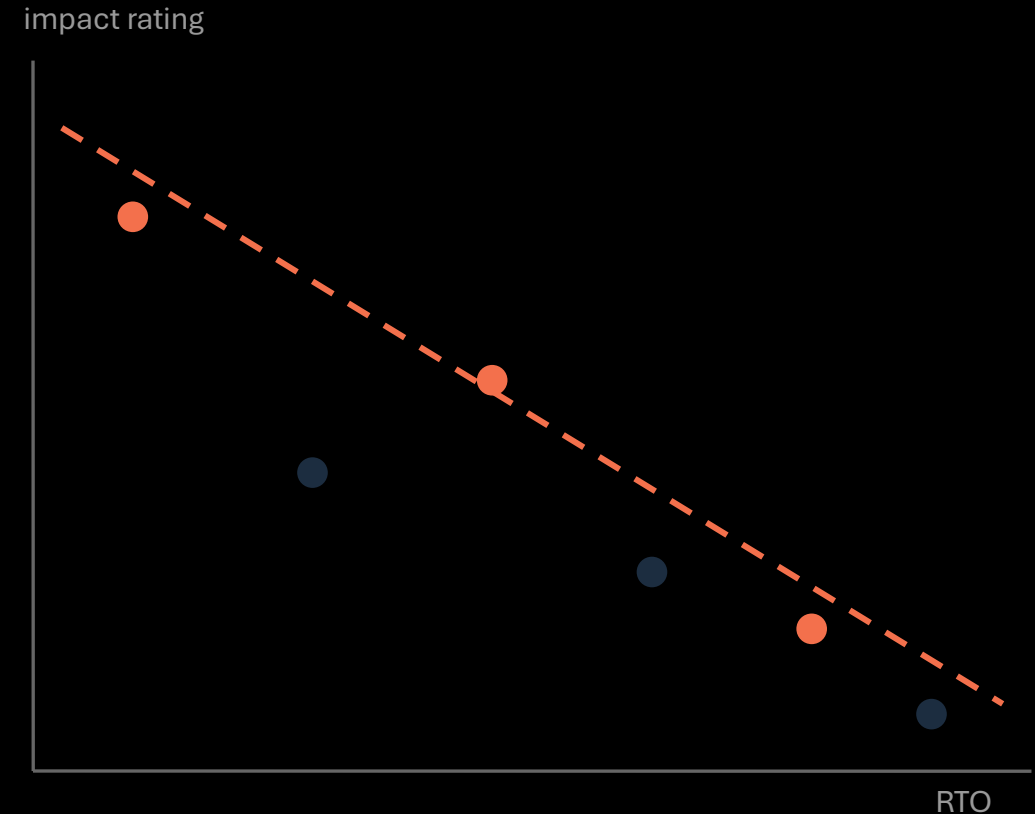
Ako validovať konzistentnosť RTO

Pre každú aktivitu: RTO + impact rating.

Aktivity sa vynesú do grafu (RTO vs. impact rating).

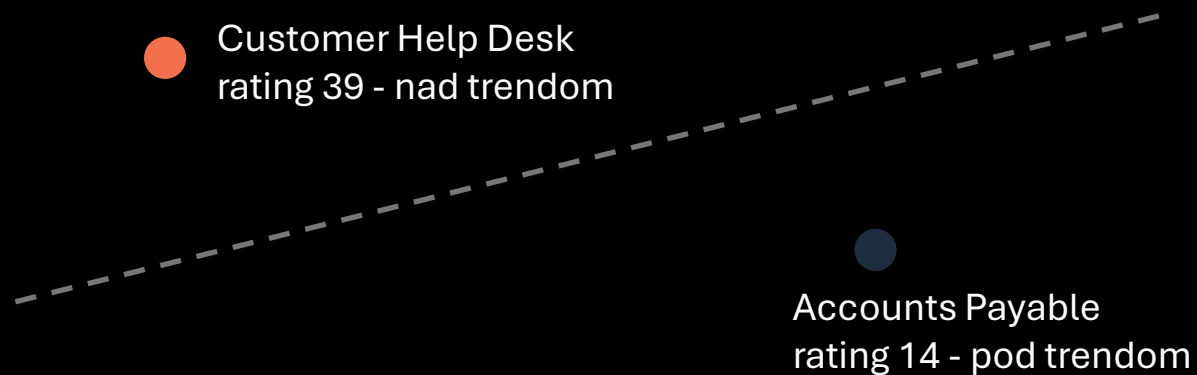
Odchýlky od trendu otvárajú otázku konzistentnosti.

Rozhodnutie zostáva na vlastníčkovi aktivity.



Informatívna technika z Annex D.3 - nie normatívna požiadavka

Čo znamená **odchýlka od trendu**



Nad trendom

RTO môže byť nastavené príliš neskoro
vzhľadom na skutočný dopad.

Pod trendom

RTO môže byť nastavené príliš
konzervatívne vzhľadom na dopad.

Signál na preskúmanie, nie automatický verdikt.