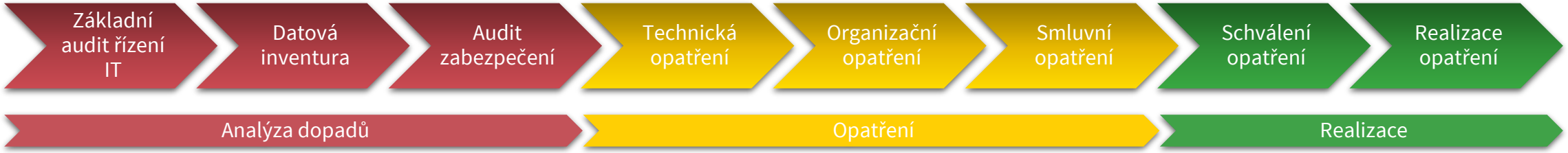
M-COM
ICT COMPANY

# Shoda s GDPR do 4-6 měsíců ! Sen či utopie ?

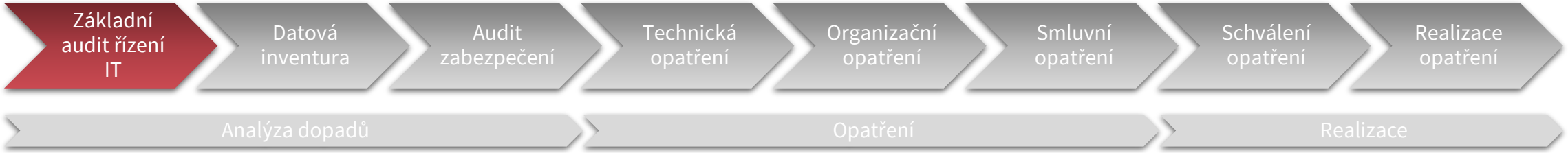
Tomáš Veselý | 14. 9. 2017 | Praha

# Od cíle jste jen 8 kroků



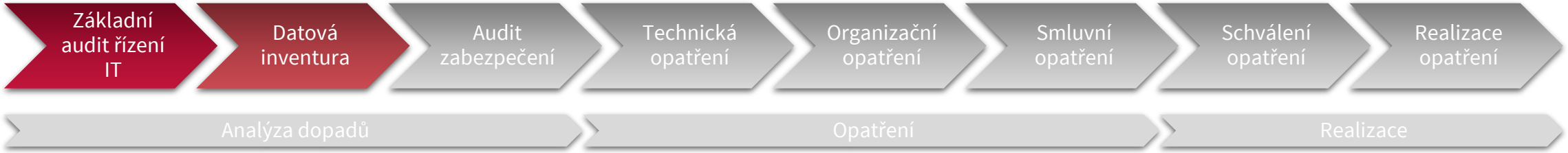

# GDPR

# A1. Základní audit řízení IT



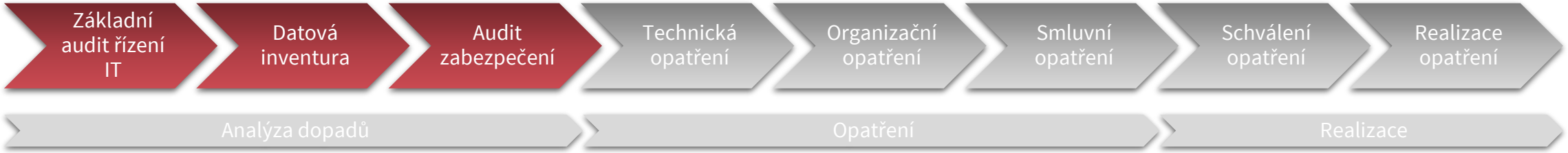

- Obsah:
  - Strategie řízení IT
  - Definice IT služeb
  - Zálohovací plány
  - Školení zaměstnanců
  - Bezpečností směrnice pro IT apod.
- Výstup: Základní hodnocení dle souladu s normou ISO27000
- Doba: 1 den

# A2. Datová inventura



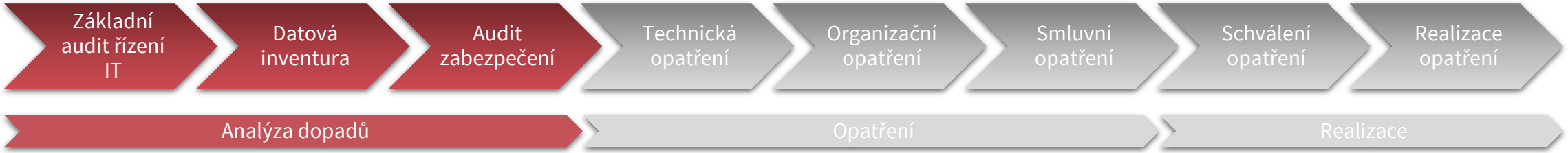

- Obsah:
  - Identifikace informačních systémů, služeb a fyzických dokumentů obsahující OÚ
    - Výčet osobních údajů
    - Kategorie OÚ
    - Právní základ
    - Agregace
    - Forma
    - Zdroj dat
    - Doba archivace a způsob skartace
    - Přístup k datům a řízení přístupu
    - Předávání dat
    - Objem zpracovávaných dat
- Výstup: Metadata pro GDPR
- Doba: cca 3–6 týdnů

# A3. Audit zabezpečení



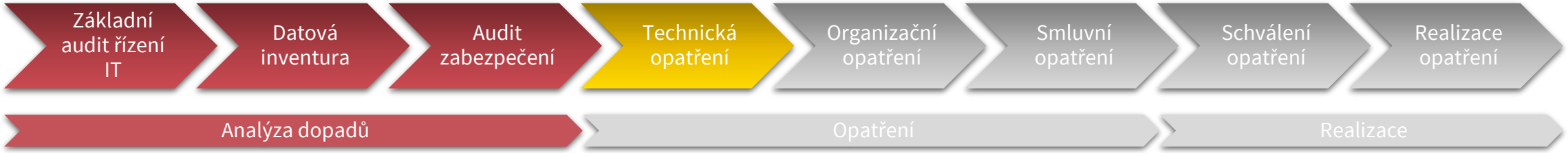

- Obsah:
  - Technické (IT) zabezpečení
  - Fyzické zabezpečení
- Výstup: Podklady pro rizikovou analýzu
- Doba: 1-3 týdny

# A. Výstup



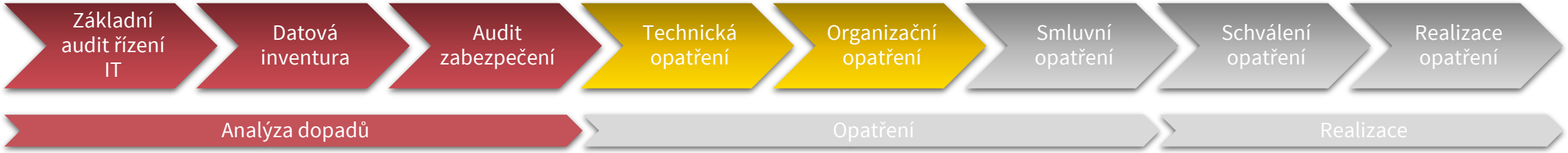

- Základní hodnocení IT dle souladu s normou ISO27000
- **Metadata pro GDPR**
- Analýza rizik
- **Posouzení vlivu na ochranu osobních údajů**

# B1. Technické opatření



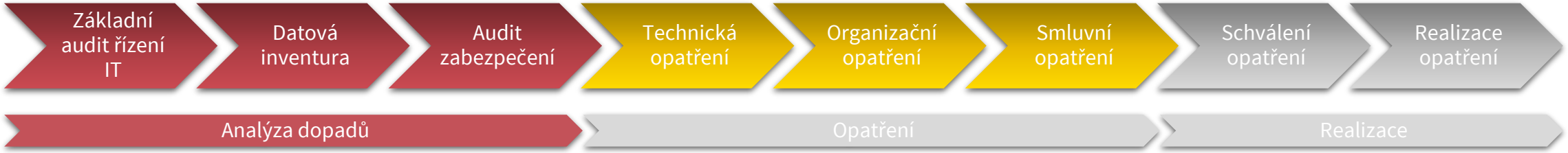

- Obsah:
  - Návrh IT opatření/projektů
  - Návrh opatření zajišťující fyzickou bezpečnost
- Výstup: Opatření
- Doba: 1-4 týdny

# B2. Organizační opatření



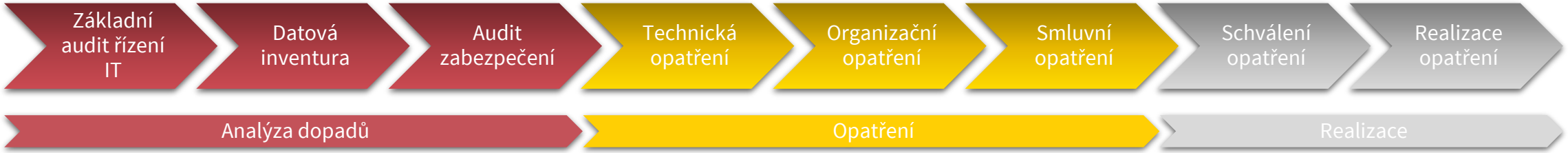

- Obsah:
  - Doplnění postupů (žádost o informace, výmaz, námitka apod.)
  - Aktualizace předpisů
    - Nakládání s OÚ
    - Archivační a skartační řád
    - Vnitřní předpis nakládání s výpočetní technikou
- Výstup: Návrh aktualizovaných předpisů
- Doba: 2-4 týdny

# B3. Smluvní opatření



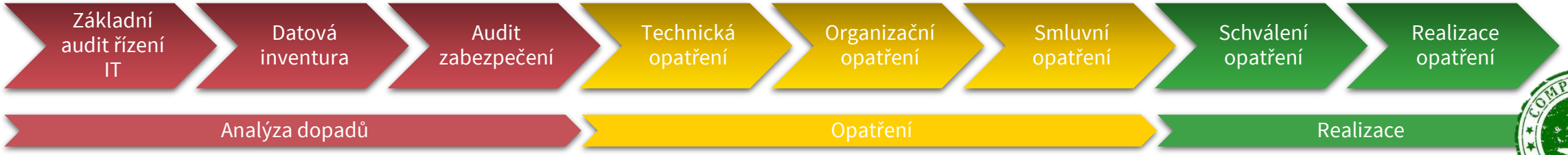

- Obsah:
  - Kontrola externích služeb
  - Kontrola případných udělovaných souhlasů se zpracováním OÚ
- Výstup: Návrh udělovaných souhlasů s OÚ a návrh změn smluv
- Doba: 1-2 týdny

# B. Výstup




- Návrh opatření/projektů
- Aktualizované předpisy a procesy
- Aktualizované smlouvy a udělované souhlasy s OÚ

# C. Realizace





- Obsah:
  - Schválení opatření
  - Realizovaná technická opatření
  - Realizovaná organizační opatření
  - Realizovaná smluvní opatření
  - Školení
- Doba: měsíce

# Typická data a systémy s OÚ

- Zaměstnanecká data
- Dodavatelsko-odběratelské vztahy
- Smluvní vztahy
- DMS
- CRM
- Kamerový systém
- E-maily
- Vnitřní evidence
- Sdílená úložiště

# Typická data a systémy s OÚ

- Evidence
  - Zápůjček (IT zařízení, auta, další..)
  - Karty (CCS, platební)
  - VPN, certifikáty
- Technické zařízení a systémy
  - Mobilní telefony
  - Počítače (cookies)
  - Auta (GPS)
  - Bezpečnostní a technické systémy (logy, žurnály)

# Prokázání jednání za účelem shody

- Zpracování jen oprávněných dat
- Nastavení procesu včetně odpovědností
- Promítnutí procesu do směrnic
- Prokazatelné seznámení zaměstnanců a dalších dotčených osob s touto směrnicí
- Pravidelné školení
- Kontrola funkčnosti procesu

# Poznatky s GDPR auditů

- Hned první odpovědi IT auditu ukazují, jak bude dále složitá cesta
- Každá organizace je jiná z hlediska uspořádání (garanti, IT, dodavatele)
- Když nemá organizace vnitřní know-how tak je to složité
- Není pravda že do května 2018 musíte mít realizovaná všechna opatření….

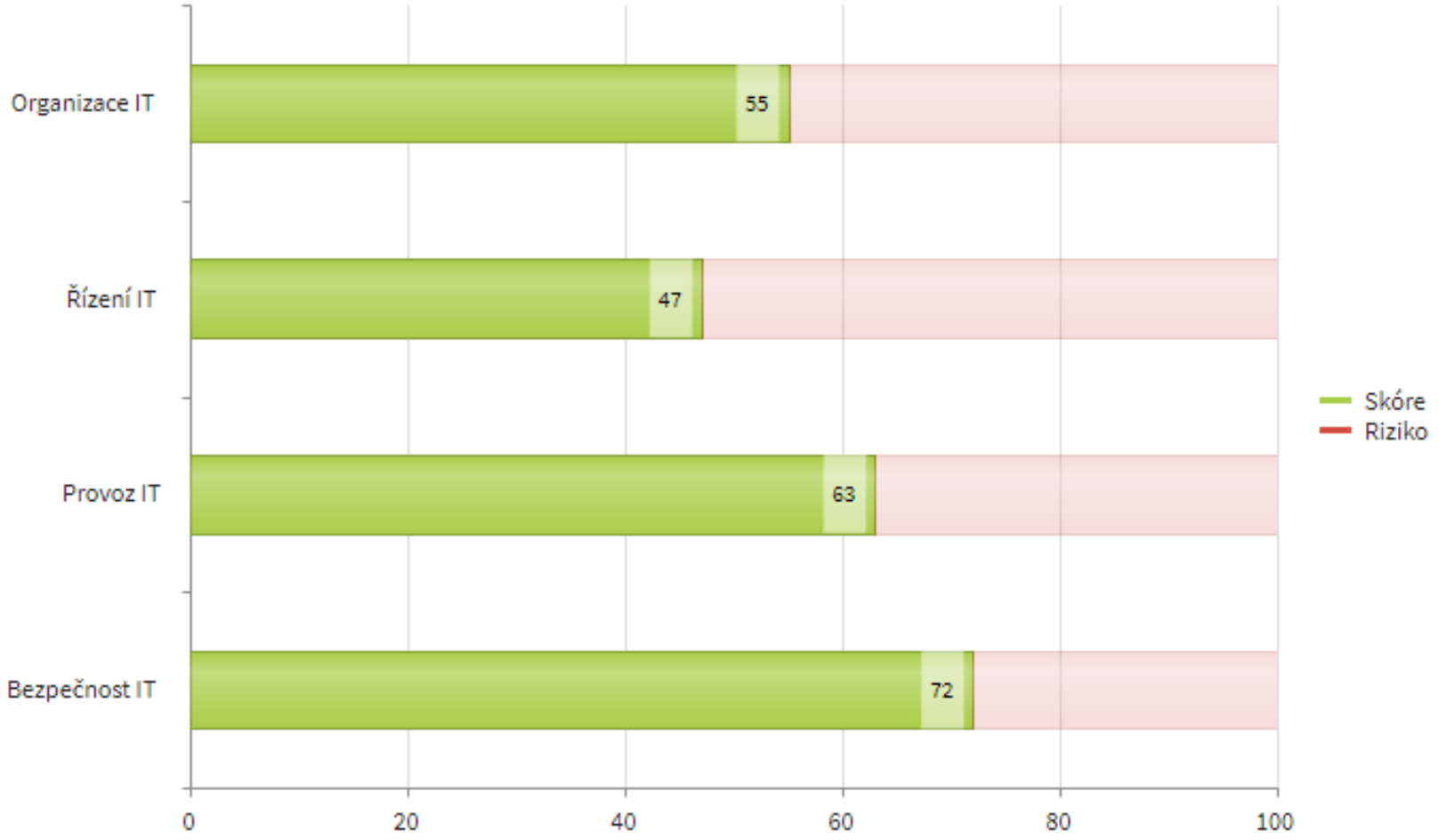
# Jak jsou na tom české firmy a organizace s řízením a bezpečností IT

# Oblasti hodnocení řízení IT

- **Organizace** formalizace pravidel práce s výpočetní technikou, systematické vzdělávání uživatelů, životní cyklus zaměstnanců
- **Řízení** katalog služeb, analýza požadavků, trendy, prezentace výsledků IT managementu, finanční plánování, risk management
- **Provoz** pravidla provozu IT systémů, provozní plány, plány obnovy, komunikace uživatelů, dokumentace aplikací
- **Bezpečnost** zabezpečení a ochrana firemních dat, správa přístupových oprávnění, monitoring operací v klíčových systémech

Pro hodnocení je použita norma ISO27000

# Výsledky (více jak 500 respondentů)



# Hrozby – Organizace (55 %)

- Neexistují pravidla pro práci s výpočetní technikou
- Nejsou školeni zaměstnanci v oblasti bezpečné práce s výpočetní technikou
- Není definovaný životní cyklus zaměstnanců

# Hrozby – Řízení (47 %)

- Není definovaný katalog služeb
- Nejsou předkládány zprávy o stavu IT
- Není definován žádný plán rozvoje IT

# Hrozby – Provoz (63 %)

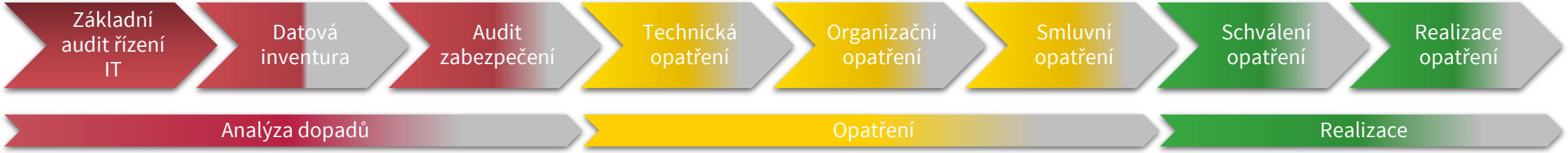
- Není k dispozici zálohovací plán a není odsouhlasený businessem
- Není plán obnovy klíčových IT systémů po havárii
- Není plán kontinuity činností
- Nejsou vypracovány pracovní postupy pro pravidelnou údržbu klíčových systémů
- Není dokumentace ke klíčovým IT systémům

# Hrozby – Bezpečnost (72 %)

- Není definován seznam informačních aktiv
- Není bezpečnostní politika
- Nejsou určeny systémy, které pracují s osobními daty

# Je možné zajistit shodu s GDPR do 4-6 měsíců ?

- Řízení IT na dobré úrovni
- Vnitřní procesy zohledňují soulad se zák. 101/2000
- Znalost aplikací, dat, dokumentů, procesů



M-COM
ICT COMPANY

# Děkuji za pozornost

**M-COM s.r.o.**
Jana Růžičky 1165/2
148 00  Praha 4

+420 242 405 220

obchod@m-com.cz

www.m-com.cz