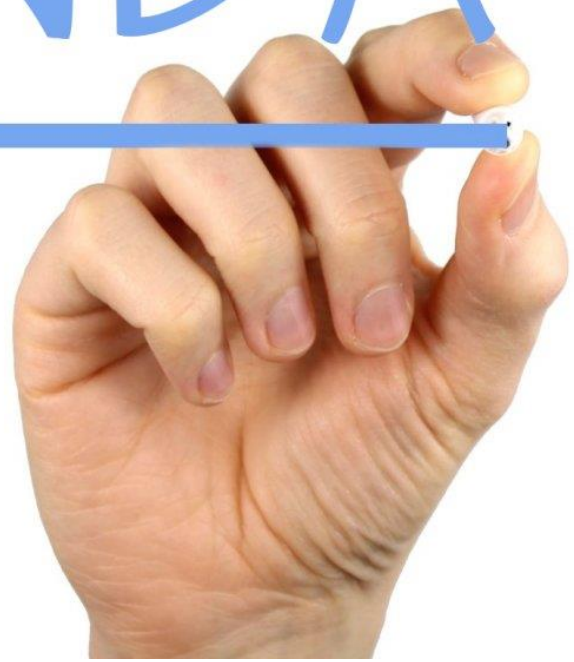
RADA PRO VEŘEJNÝ DOHLED
NAD AUDITEM

Kyberbezpečnost & Kontrola kvality auditu

Jiří Diepolt

3. 11. 2022

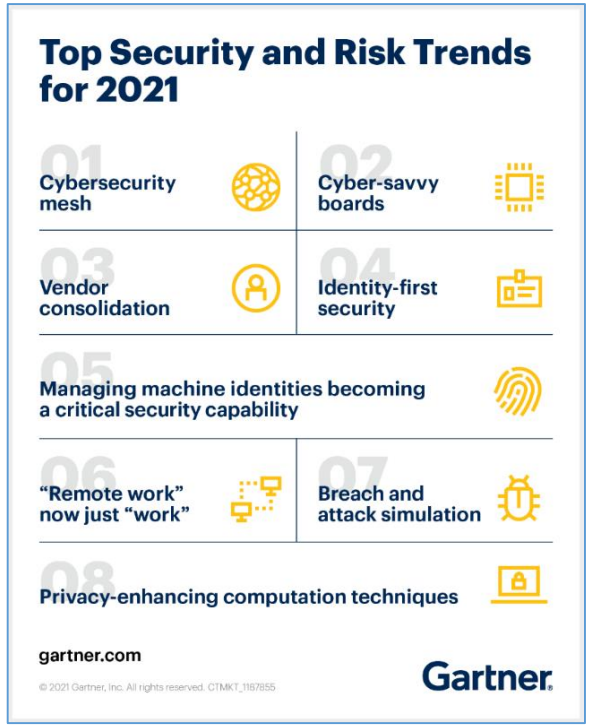
AGENDA



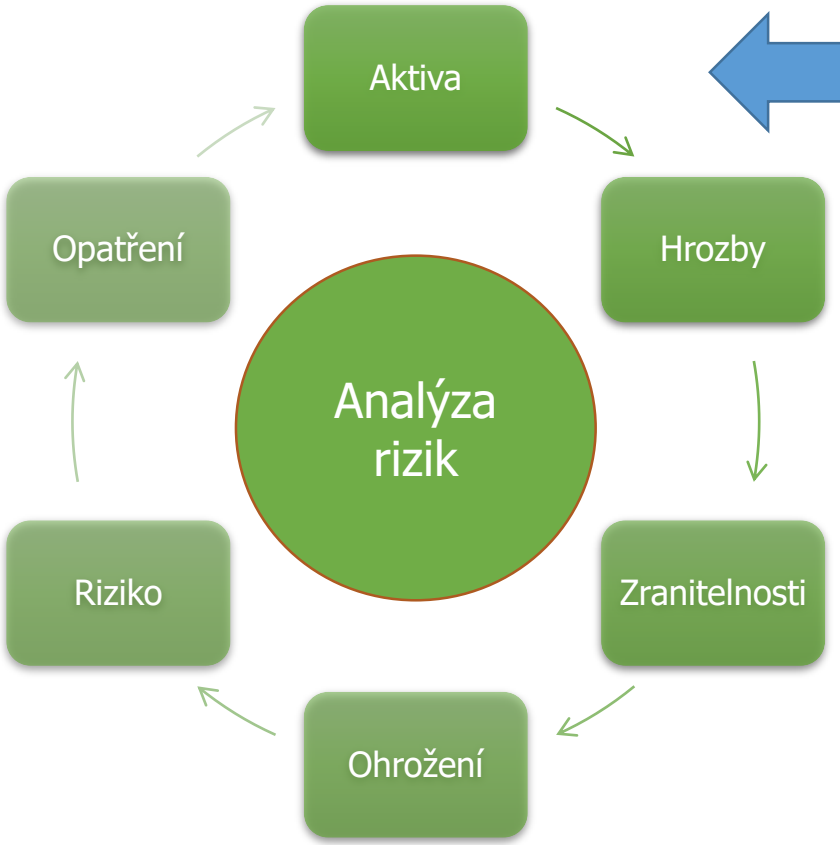
1. Úvod
   - Trendy
   - Co je kyberbezpečnost?
2. Kontrolní činnost RVDA
   - Přístup kontrol RVDA
   - Zjištění z kontrol kvality
3. Závěr

Kyberbezpečnost – trendy

1) Nárůst **počtu aktiv**, které **nejsou pod kontrolou** (práce z domova, …)
2) Systém detekce a reakce na ohrožení identity
3) Riziko **nárůstu digitalizace** dodavatelského řetězce
4) Konsolidace dodavatelů řešení
5) Cybersecurity „mesh"
6) Distribuovaná rozhodování
7) „Klasická" **bezpečnostní školení nestačí**

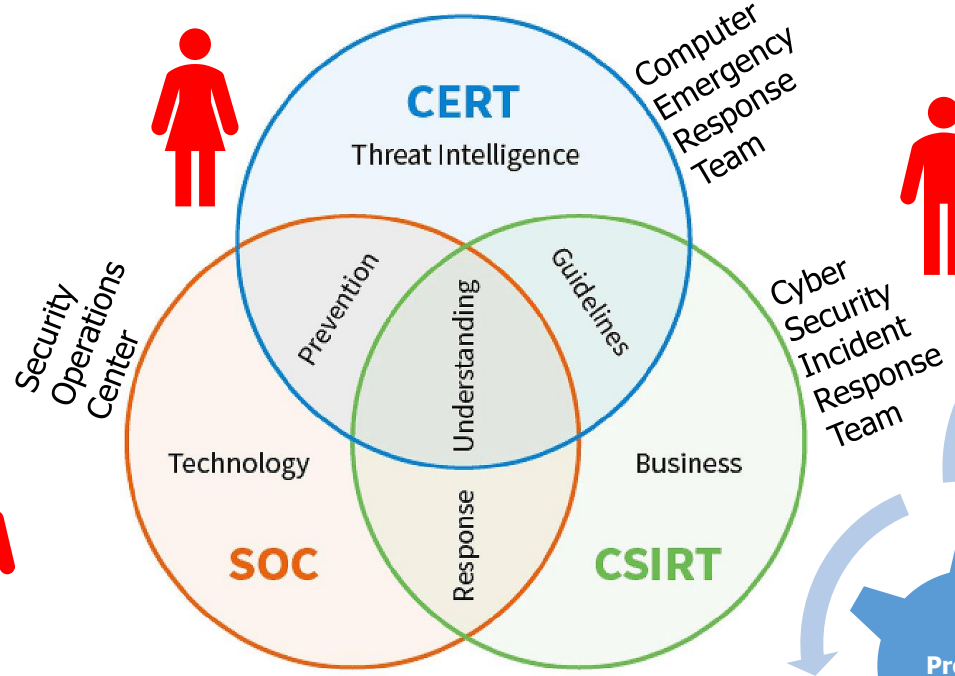


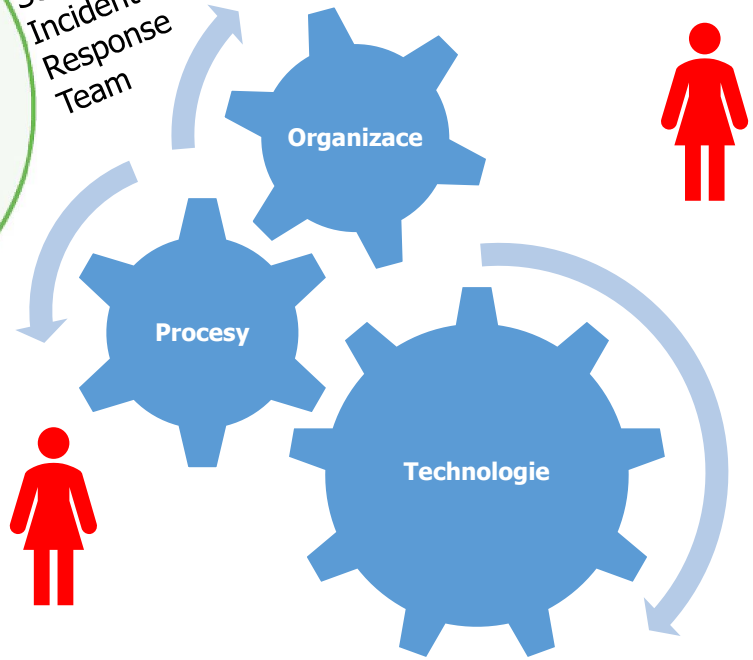
Co je to kyberbezpečnost?
Jak řídit informační bezpečnost?



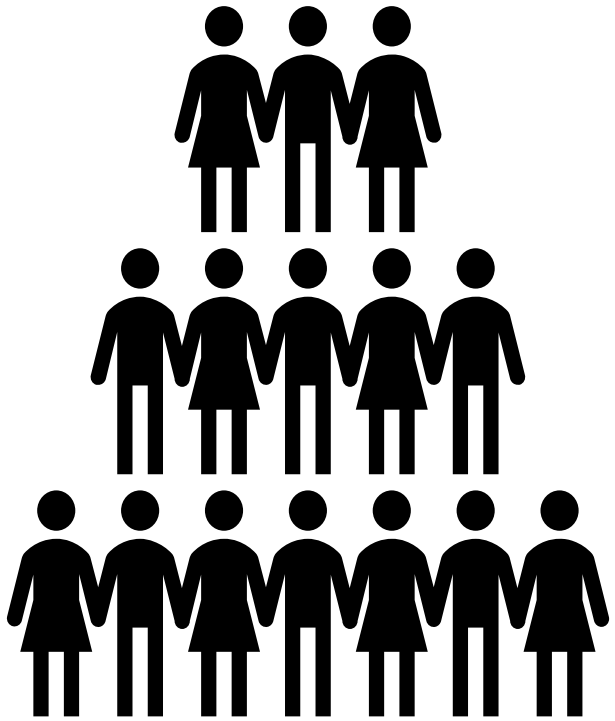
Ochrana informačních aktiv prostřednictvím eliminace hrozeb působících na informace zpracovávané, uchovávané a přenášené propojenými informačními systémy.

Co je to kyberbezpečnost?
Jak řídit informační bezpečnost?





Kdo řeší kyberbezpečnost ?



Vedení	IT	Security	Audit	IT	Zaměstnanci	Poskytovatel (IT) služeb
CEO	CIO	**Security Manažer**	IT Security Auditor	IT vývoj	všichni	Dodavatel služeb
CDO	IT vývoj	**Security Architekt**	IT Auditor	IT provoz	…	…
COO	IT provoz	**Security forum**	Penetrační tester	IT architekt		
CIO	…	…	Externí auditor	IT admin		
…			….	….		

Normy, standardy, rámce, organizace, úřady, legislativa, regulace, ….

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

ISO 27001

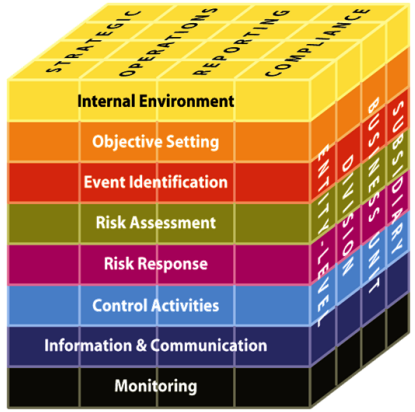
CIS Center for Internet Security®
Creating Confidence in the Connected World.

ISO 27018:2019

ISO/IEC 27037 STANDARD

CNB CZECH NATIONAL BANK

NIS 2



International Standards of Auditing ISA

OWASP Open Web Application Security Project

NIST National Institute of Standards and Technology

NÚKIB

úřad pro ochranu osobních údajů the office for personal data protection

DIGITAL OPERATIONAL RESILIENCE ACT

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Národní úřad pro kybernetickou a informační bezpečnost

ISO 27031

COBIT GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY

COBIT CYBER SECURITY AUDIT
CYBERSECURITY FUNDAMENTALS
IT RISK FUNDAMENTALS
IT AUDIT FUNDAMENTALS

General Data Protection Regulation

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data

Manufacturers PCI PTS PIN Entry Devices
Software Developers PCI PA-DSS Payment Applications
Merchants & Service Providers PCI DSS Secure Environments
PCI Security & Compliance
P2PE

RADA PRO VEŘEJNÝ DOHLED
NAD AUDITEM

Kontrolní činnost RVDA

Auditní & kontrolní rámec pro oblast IT

Plánování IT auditu

- **Základní informace o IT prostředí** – aplikace, technická infrastruktura, procesy, …
- **Vyhodnocení rizik**
- **Zapojení** IT specialistů
- **Zadání** IT specialistům

Provedení IT auditu

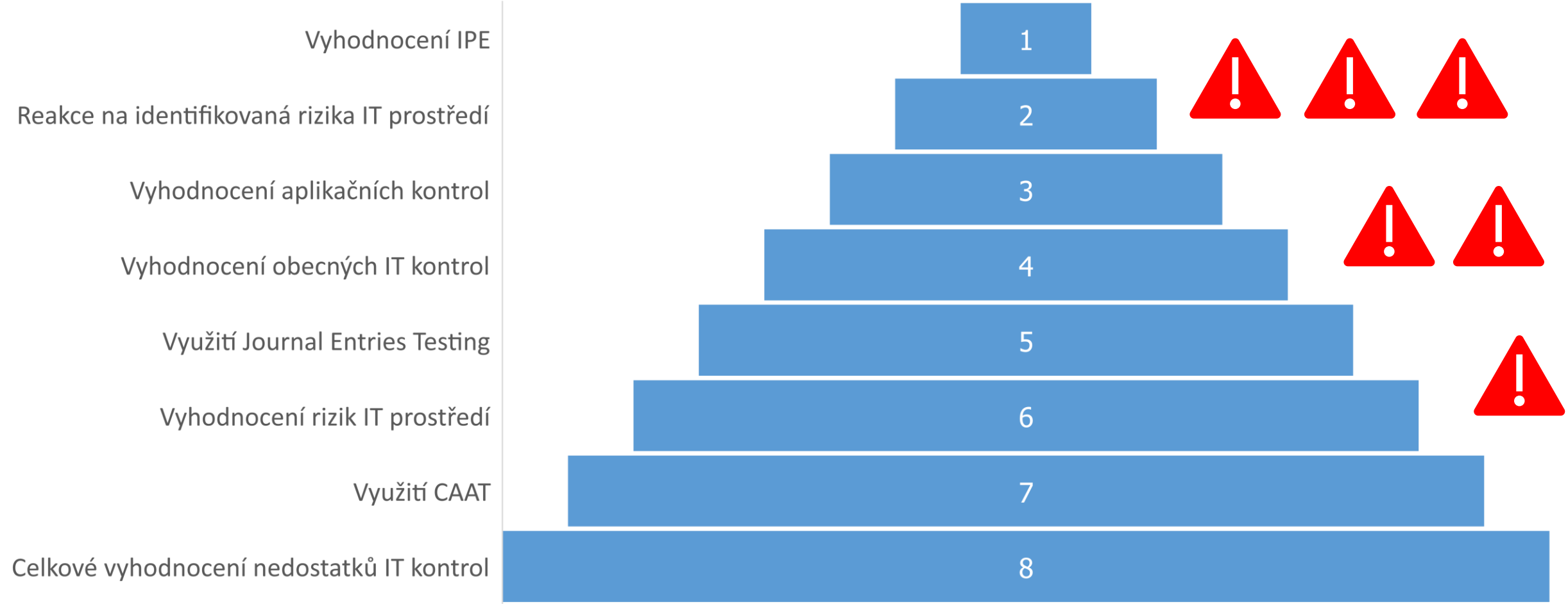
- **ITGC** (návrh, implementace, provozní účinnost)
- **ITAC** (návrh, implementace, provozní účinnost)
- „Speciální" testy (**JET**, Data Analytics, IPE)

Závěry IT auditu

- Celkové **zhodnocení IT prostředí** a kontrol,
- **Posouzení dopadů** na audit, reakce na IT zjištění
- **Dokumentace závěrů IT** auditu (interní memo, externí reporty)

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

Kontrolní činnost RVDA
Identifikované nedostatky z Kontrol kvality



Případová studie (fiktivní firma & fiktivní auditor)

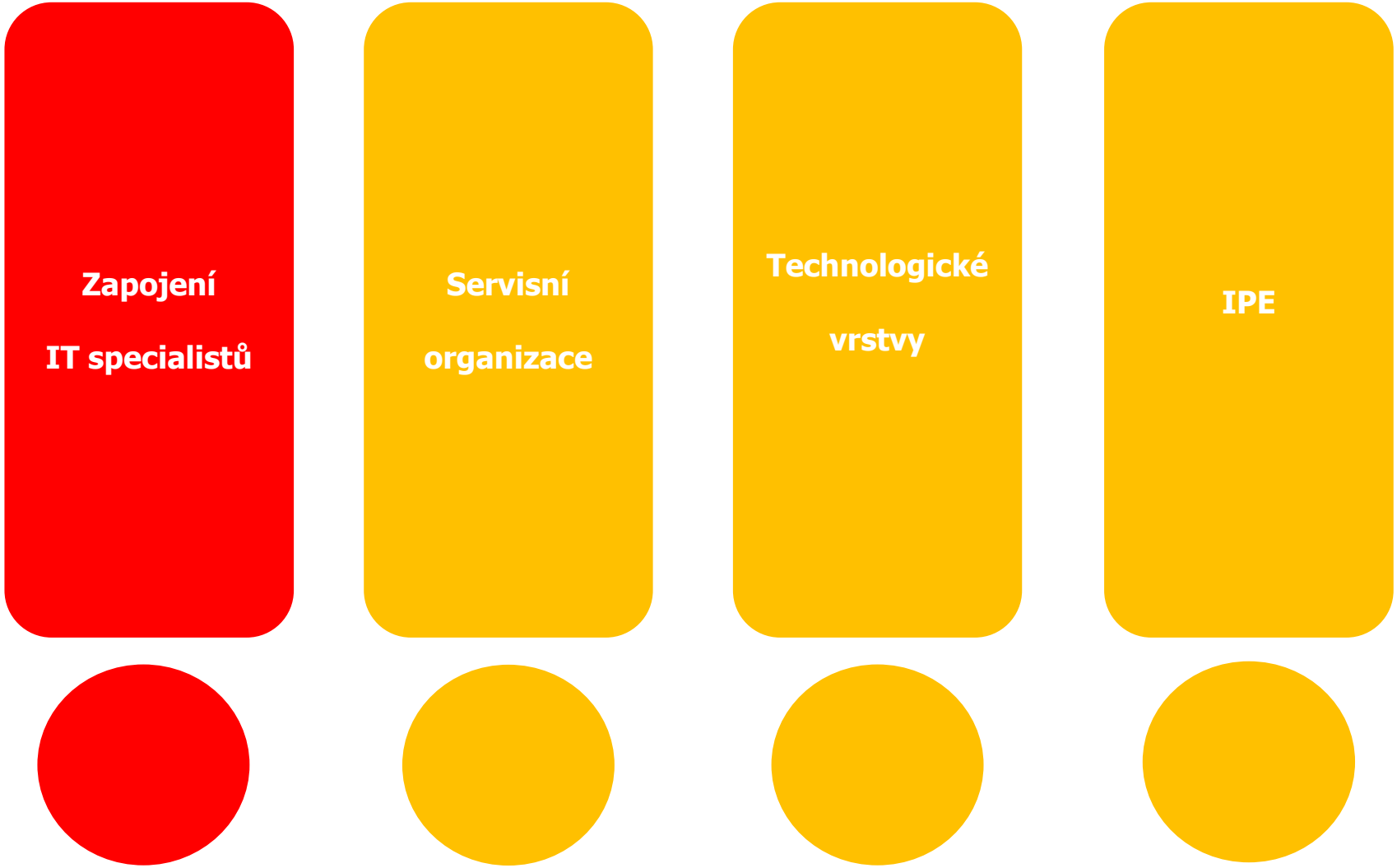
Retailový obchod

- Předměte činnosti: velkoobchodní a maloobchodní prodej zboží
- Roční tržby: stovky milionů - jednotky miliard Kč
- Distribučními kanály: síť prodejen + internetový prodej
- Počet transakcí/den: jednotky/desítky tisíc
- Počet klientů/rok: stovky tisíc klientů
- Transakce: v řádech stovek či jednotek tisíc Kč
- Informační systémy: podpora podnikových procesů - nákup & prodej, účetnictví, sklad, platební systém, datová analýza (datový sklad); Využití služeb servisní organizace
- Závislost na IT: vysoká míra užití IS/IT = vysoce závislá na IT

Auditor

- Středně velká společnost
- Auditor nevyužívá interní nebo externí IT specialisty
- Auditního klienta „zná několik let“

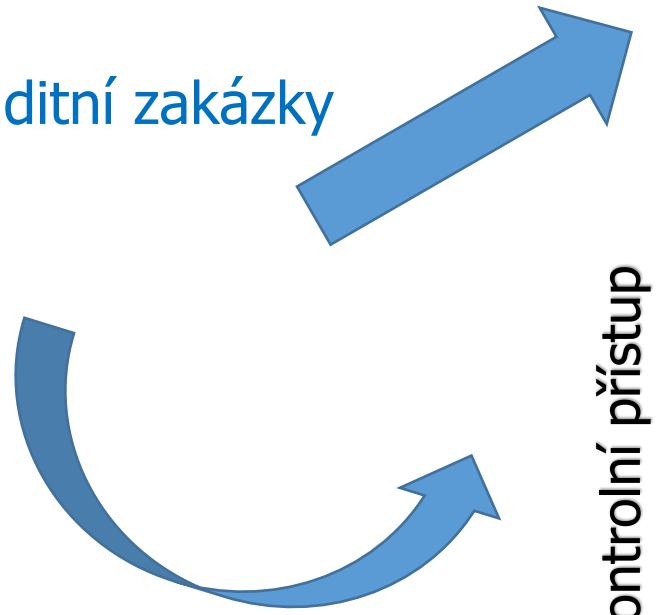
Případová studie – typická zjištění z KK



Zapojení IT specialistů

Kdy zvažuje auditor potřebu provedení ITGC & ITAC ?

- ✓ Akceptace auditní zakázky
- ✓ Plánování
- ✓ Provedení
- ✓ Ukončení



Základní otázky

- Je možné realizovat auditní zakázku bez zapojení IT expertů?
- Jedná se o komplexní IT prostředí?
- Zpracovává klient velké množství transakcí a dat?
- Působí klient v sektorech – banky a pojišťovny, utility, retail, ?

Kontrolní přístup

Je možné se spolehnout na IT

- Testování ITGC
- Testování ITAC
- Testování JET

Substantivní přístup

Není možné se spolehnout na IT

- Dokumentace IT prostředí
- Testování reportů
- Použití nástrojů pro JET, Data Analytics

- ITGC netestováno
- ITAC netestováno

Zapojení IT specialisty – zjištění z KK

A) Akceptace auditní zakázky

- Auditor před akceptací auditní zakázky nedostatečně posoudil auditní přístup specifika zakázky a potřebu odbornosti týmu provádějícího auditr zakázku, včetně potřeby zapojení IT specialistů k zakázce a (případné) zapojení IT specialistů."
- Rozhodnutí o akceptaci zakázky bez dostatečné znalosti IT / možnosti využít IT specialistu

B) Plánování auditu

- V týmu není zahrnut IT specialista, přestože začlenění je relevantní.
- Není jednoznačné zadání rozsahu testování obecných a aplikačních kontr

C) Provedení auditu

- Ověření obecných IT kontrol je formální
- Nedostatečná dokumentace IS/IT a business procesů v oblasti maloobchodního prodeje.

Ilustrativní IT dotazníku auditora

Otázka	Odpověď klienta
Máte zaveden proces řízení přístupových práv	Ano
Kontroluje někdo nezávislý nastavení přístupových práv	Ne
Měli jste v loňském roce bezpečnostní incidenty	Nemáme žádné incidenty
Máte zaveden proces „Problem management"	Nemáme žádné problémy
Máte se svým poskytovatelem IT služeb smlouvu včetně SLA	Ano, ale neposkytneme ji
….	…

Vyhodnocení IT dotazníku auditorem:

IT prostředí je spolehlivé

Proč je nedostatek IT specialistů?

Interní auditor(ka) se zaměřením na IT

Analytik IT Auditu – Associate Consultant

IT Auditor/ka

IT Internal Auditor

INTERNÍ IT AUDITOR (plný nebo 3/4 úvazek)

IT Interní auditor

Junior konzultant – tým Technologické a procesní audity

Konzultant / auditor kybernetické bezpečnosti

Senior IT Auditor for CEE region (Generali CEE Holding)

Zdroj: www.jobs.cz 27. 10. 2022

Jak se vypořádat s nedostatkem IT specialistů?

V0) Člen auditního týmu (není IT specialista)

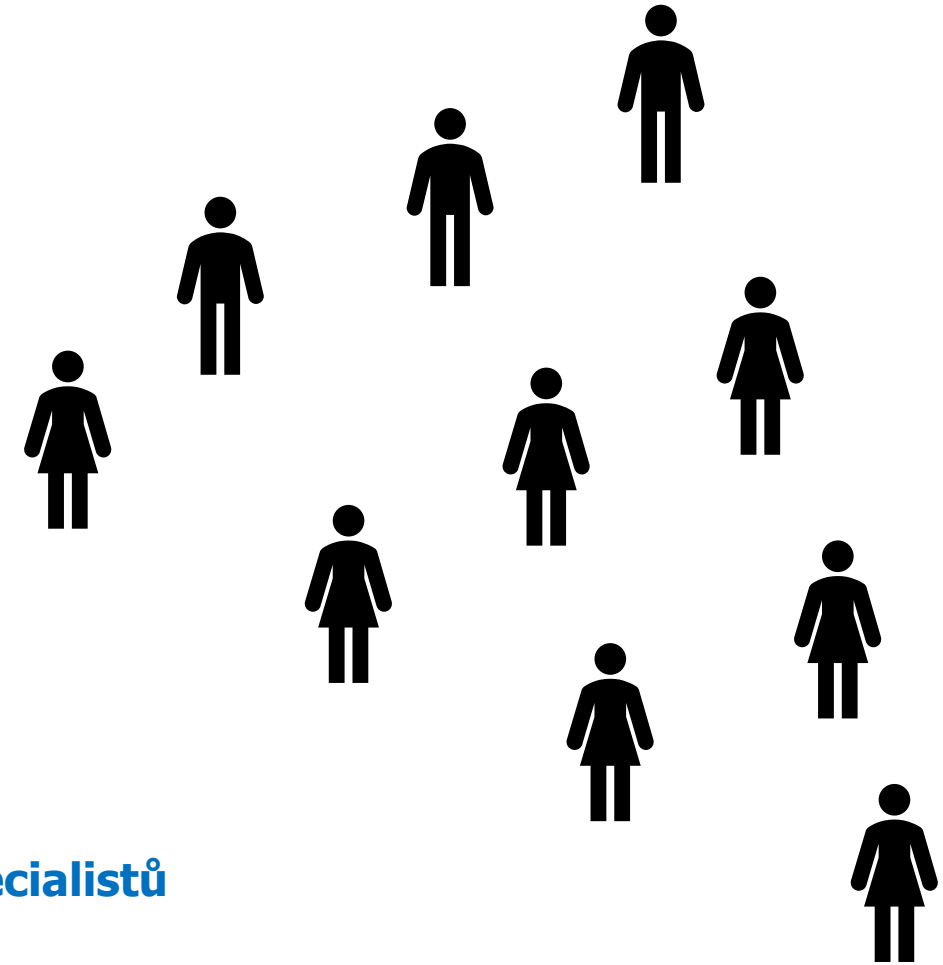
- Zkušený auditor „se vztahem k IT"
- „Vhodný" pro ne příliš komplexní IT prostředí

V1) Interní IT experti

- Potřeba průběžného vzdělávání (interní, externí)
- Certifikace (CISA, CIA, ISO 27000 Auditor, …)
- Riziko fluktuace (Jak dlouhodobě udržet IT auditora ?)
- Dlouhodobý náklad
- Větší porozumění potřebám auditu

V2) Externí IT specialisté

- Specializace
- Jednorázový náklad
- Nutné zohlednit náklady při sjednání auditní smlouvy



V3) Nesjednávat zakázky, kde je potřeba zapojení IT specialistů

Jak se vypořádat s nedostatkem IT specialistů?

Bezpečnostní incidenty mají pozitivní dopad na zvyšování ceny za audit

- Nárůst využití IT specialistů zvyšuje interní náklady
- Jsou auditní klienti ochotni akceptovat vyšší auditní fee?

- Dle uvedené studie ano.

H1: The cybersecurity incidents have positive impact on the high audit fees.

https://www.indecs.eu/2021/indecs2021-pp375-390.pdf

CYBER-SECURITY RISKS ASSESSMENT BY EXTERNAL AUDITORS

Tran Nguen Bao Ngo[1] and Andrea Tick[2,*]

[1]University of Danang
Danang, Vietnam

[2]Óbuda University
Budapest, Hungary

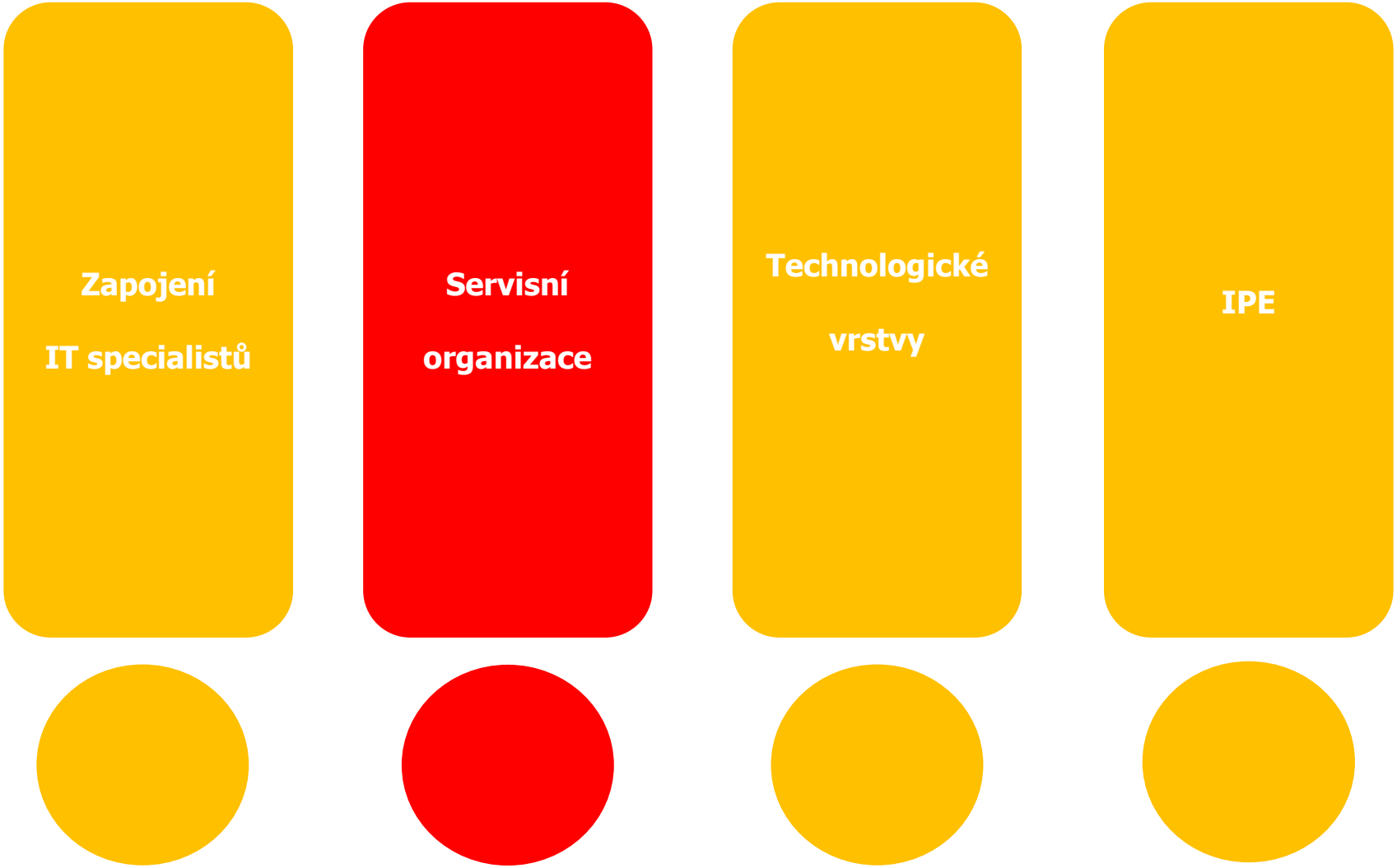
DOI: 10.7906/indecs.19.3.3
Regular article

Received: 17 July 2020.
Accepted: 14 May 2021.

ABSTRACT

The rise in cybercriminal activities in recent years has sparked concern about the costs of technological advancement and the growing reliance of humans on technology. The seriousness of this situation in the business world is indeed more noteworthy and more prominent than other areas, prompting many people to wonder how external auditors – who are responsible for identifying any accounting flaws – will respond to cybersecurity-affected businesses – the ones which can make an honest effort to mask and conceal their difficulties and challenges from their investors and stakeholders. Consequently, the aim of this study is to search whether external auditors focus harder on cybersecurity-attacked firms and businesses by charging higher audit fees. The study found a positive correlation between audit fees and breach employing a sample of 100 global small-, medium-sized, and large businesses. This indicates that external auditors find more risks and spend more effort while auditing cybersecurity-attacked businesses.

Případová studie – typická zjištění z KK



Servisní organizace

	WHAT	WHO
SOC 1	Financial reporting internal control	Users controller's office and User auditor
SOC 2	Control of security, availability, integrity, confidentiality and privacy	Shared with any party under NDA by regulators or management
SOC 3	Control of security, availability, integrity, confidentiality and privacy	Public available to anyone
Bridge Letter	Ga letter to cover a gap period between SOC reports	Public available to anyone or shared under NDA

Základní otázky v rámci auditu/kontroly

- Seznam poskytovatelů IT služeb / servisních organizací
- Význam servisní organizace z pohledu podpory business procesů
- Procesy řízení servisní organizace
- Existence a pravidelné hodnocení SLA
- Dostupné externí audity (např. SOC reports)
- Přehled (a analýza příčin) incidentů
- Vyhodnocení servisních organizací z pohledu rizik a dopadů na audit

Servisní organizace – příklady zjištění z KK

ISA 402.9
ISA 402.10

A) Servisní organizace nejsou identifikovány
(např. provozovatel aplikační a technické infrastruktury, účetnictví a mzdy, …)

- Není provedeno posouzení a dokumentace servisních organizací

B) Servisní organizace jsou identifikovány, ale

- Vytvořen pouze přehled servisních organizací
- Není provedeno vyhodnocení rizik servisní organizace z pohledu auditu
- Auditor se výhradně spoléhá na (nedostatečné?) kontroly prováděné servisní organizací
- Auditor nevyhodnotil návrh a zavedení příslušných kontrol v uživatelské účetní jednotce

C) Testování IT kontrol u servisní organizace sice provedeno, ale

- Nepokrývá všechna (klíčová) identifikovaná rizika
- Nejsou provedeny dodatečné auditní procedury v případně obtížnosti či nesoučinnosti prověřené servisní organizace (např. sdílené IT centrum je v zahraničí, auditovaný subjekt neposkytne IT SLA smlouvy, apod.)

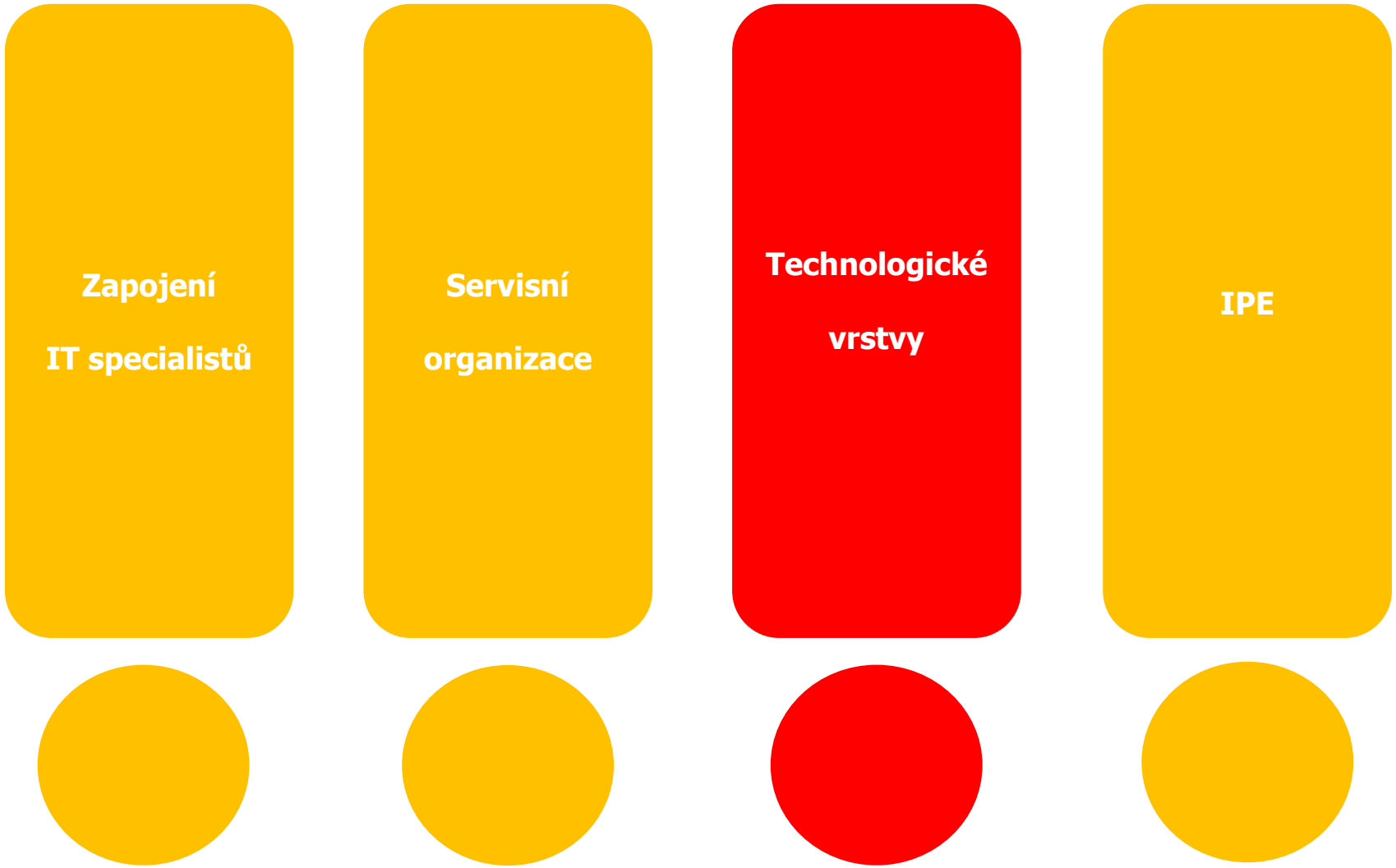
Servisní organizace – cloudové služby – příklad incidentu 09/2022

Globální cloudové systémy patří mezi jedny z **nejkritičtějších infrastruktur**, na jejichž spolehlivosti a bezpečnosti závisí miliony uživatelů a firem. Velké incidenty se zde naštěstí neobjevují velmi často.

Oficiální zpráva **společnosti Microsoft**, informovala o rozsáhlém úniku privátních informací z jejich cloudové služby. Zranitelnost byla objevena koncem září cybersecurity firmou **SOCRadar** a byla pojmenována jako **„Bluebleed".**

Microsoft ihned problém opravil a popsal jej jako chybnou konfiguraci **Azure Blob Storage.** Chyba umožňovala **neautentizovaný přístup** k obsahu **objektového úložiště**, jež způsobila expozici více než **dvou terabajtů dat z let 2017 až 2022, týkajících se 65 tisíc firemních zákazníků** ze **111 států**, včetně firme a státních organizací České republiky. Mezi dokumenty měly být například **smlouvy, faktury, objednávky,** projektové dokumenty a další „byznys-kritické" soubory.

Případová studie – typická zjištění z KK



Bezpečnostní (technologické) vrstvy

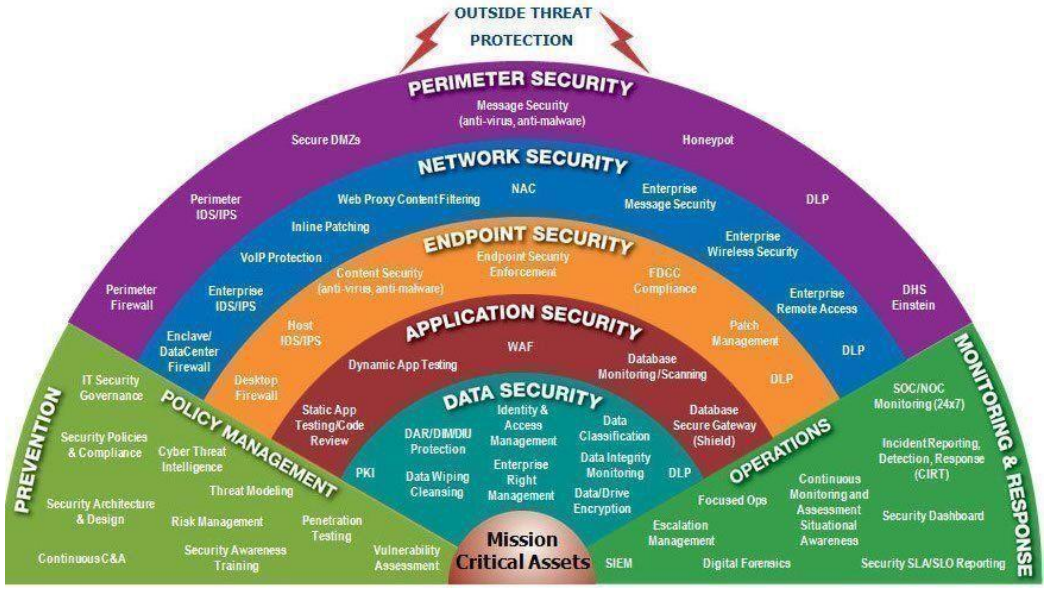
Základní otázky

- Jsou implementovány všechny (relevantní) vrstvy?
- Jaké jsou aktuální hrozby & zranitelnosti?
- Kdo je zodpovědný za implementaci a pravidelnou kontrolu?
- Jaká je úroveň Design/Implementace/Efektivita kontrol jednotlivých vrstev?
- Je nutné ověřovat všechny vrstvy v rámci auditu?

Bezpečnostní (technologické) vrstvy – příklad zjištění z KK

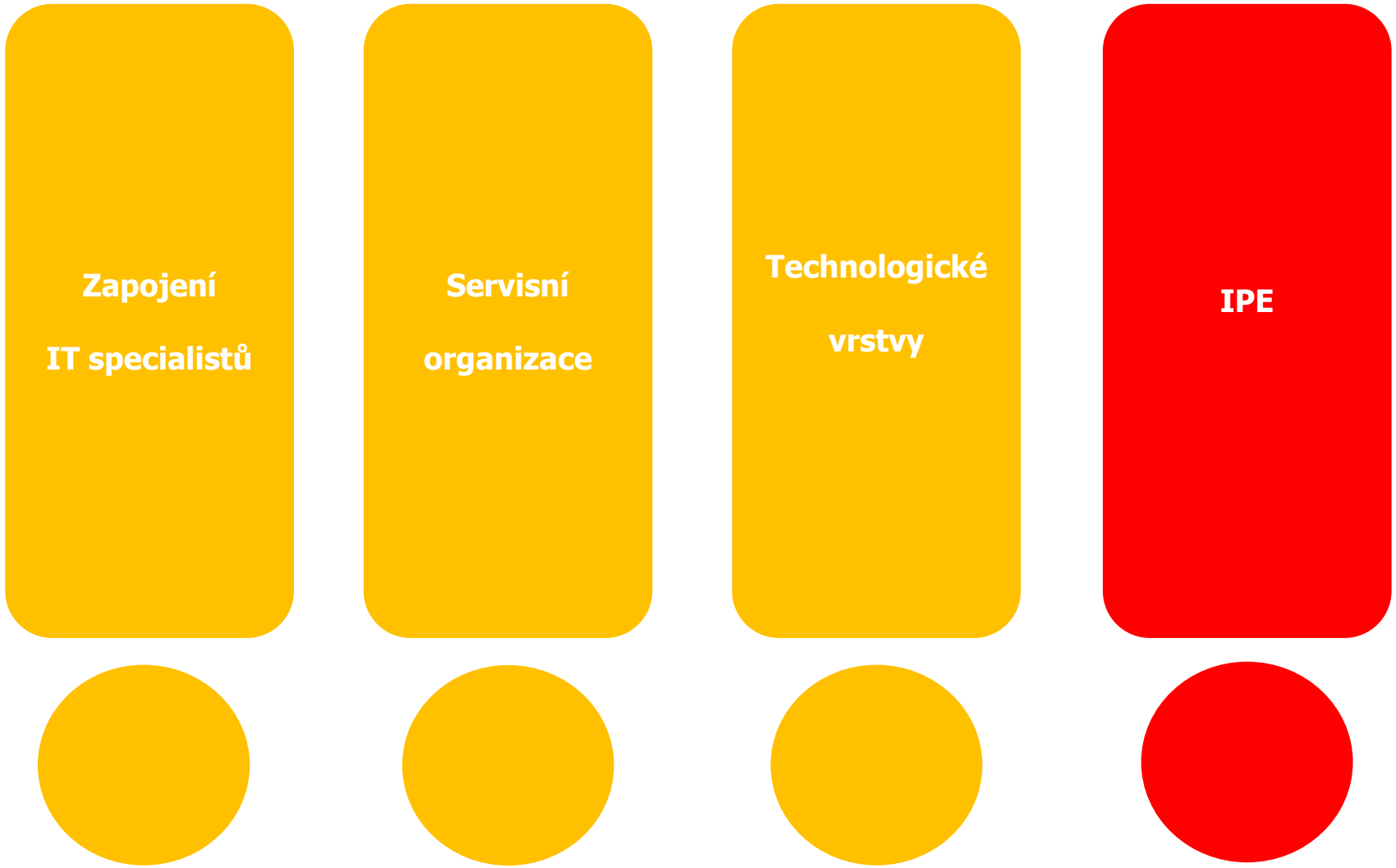
A) IT auditor nevyhodnotil (rizika, kontroly) relevantní dílčí technologické komponenty (vrstvy)

- Aplikace
- Operační systém
- Databáze
- Síťové prostředí
- Technická infrastruktura
- Fyzická lokalita



B) IT auditor neprovedl anebo nezdokumentoval výběr relevantních vrstev k testování

Případová studie – typická zjištění z KK



RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

IPE (informace vytvořené účetní jednotkou)

Základní otázky

- Jaké informace/reporty jsou potřeba pro audit?
- Jak ověřím přesnost a úplnost dat
- Jsou ve společnosti zavedeny procesy / kontrolní mechanismy pro řízení kvality dat?
- Byly v minulosti zaznamenány incidenty týkající se kvality dat v klíčových systémech (co bylo kořenovou příčinou problému)?

Using Information Produced by the Company

.10 When using information produced by the company as audit evidence, the auditor should evaluate whether the information is sufficient and appropriate for purposes of the audit by performing procedures to: [3]

- Test the accuracy and completeness of the information, or test the controls over the accuracy and completeness of that information; and
- Evaluate whether the information is sufficiently precise and detailed for purposes of the audit.

IPE - příklad zjištění z KK

Příklady zjištění

- Auditor nezmapoval informační toky relevantní z pohledu tvorby finančních výkazů
- Auditor neověřil zdroje dat pro IPE
- Nedostatečná dokumentace IPE použitých v rámci auditu
- Auditor neověřil **přesnost / úplnost dat** (reportů použitých v rámci auditu)
- **Nedostatečná dokumentace** provedených testů IPE
- Auditor nezohlednil zjištěné nedostatky při vyhodnocení IPE
- Auditor neověřil obecné IT kontroly relevantní z pohledu IPE
- Auditor nedostatečně ověřil EUC (týkající se IPE) ;

ISA 315.12 & A70
ISA 500.7
ISA 500.9 & A50-A51
ISA 330.10 & A29-A31

RADA PRO VEŘEJNÝ DOHLED
NAD AUDITEM

Shrnutí

Shrnutí

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

ISO 27001

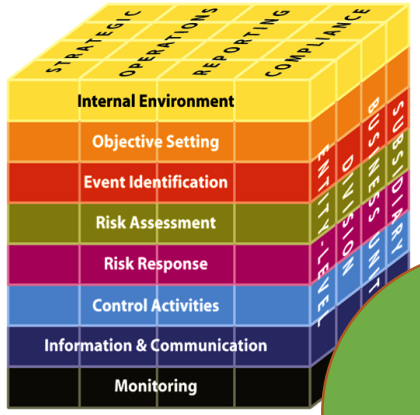
CIS Center for Internet Security®
Creating Confidence in the Connected World.

ISO 27018:2019

ISO/IEC 27037 STANDARD

Primární aktiva
Informační aktiva
Podpůrná aktiva

NIS 2



International Standards of Auditing
ISA

OWASP
Open Web Application Security Project

NIST
National Institute of Standards and Technology

úřad pro ochranu osobních údajů
the office for personal data protection

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Analýza rizik

DIGITAL OPERATIONAL RESILIENCE ACT

General Data Protection Regulation

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

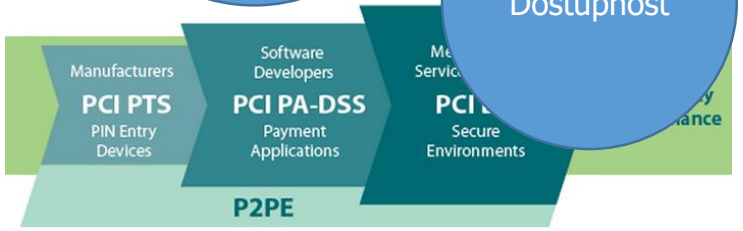
ISO 27031

Integrita
Důvěrnost
Dostupnost

COBIT
GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY

COBIT
CYBER SECURITY AUDIT
CYBERSECURITY FUNDAMENTALS
IT RISK FUNDAMENTALS
IT AUDIT FUNDAMENTALS

PAYM... SECU...



Kyber(ne)bezpečnost
se týká **každého z nás.**

Klíčovou roli v kyberbezpečnosti
hrají (zatím) **lidé**
nikoli (pouze) informační technologie.

IT audit je jedním z několika pilířů systémů řízení bezpečnosti.

Kybersecurita?
Nedělej, že se Tě netýká.
Ať sedíš na benzince
Nebo s kamarády u piva.
Vezmi notebook s sebou.
Ochraňuj svá informační aktiva.
…
Ať pracuješ v kanceláři.
Nebo pozoruješ venku oblohu.
Ať jste mladí nebo staří.
Myslete na pravidelnou zálohu.
…
Když ztratíš svá data.
Když ztratíš firemní informace.
Snad horší než ztráta zlata.
Už nemusíš se zpátky vracet.

Dotazy

Kontakt

Jiří Diepolt

RVDA
jiri.diepolt@rvda.cz