

SECURITY 2013



21. ročník konference o bezpečnosti v ICT

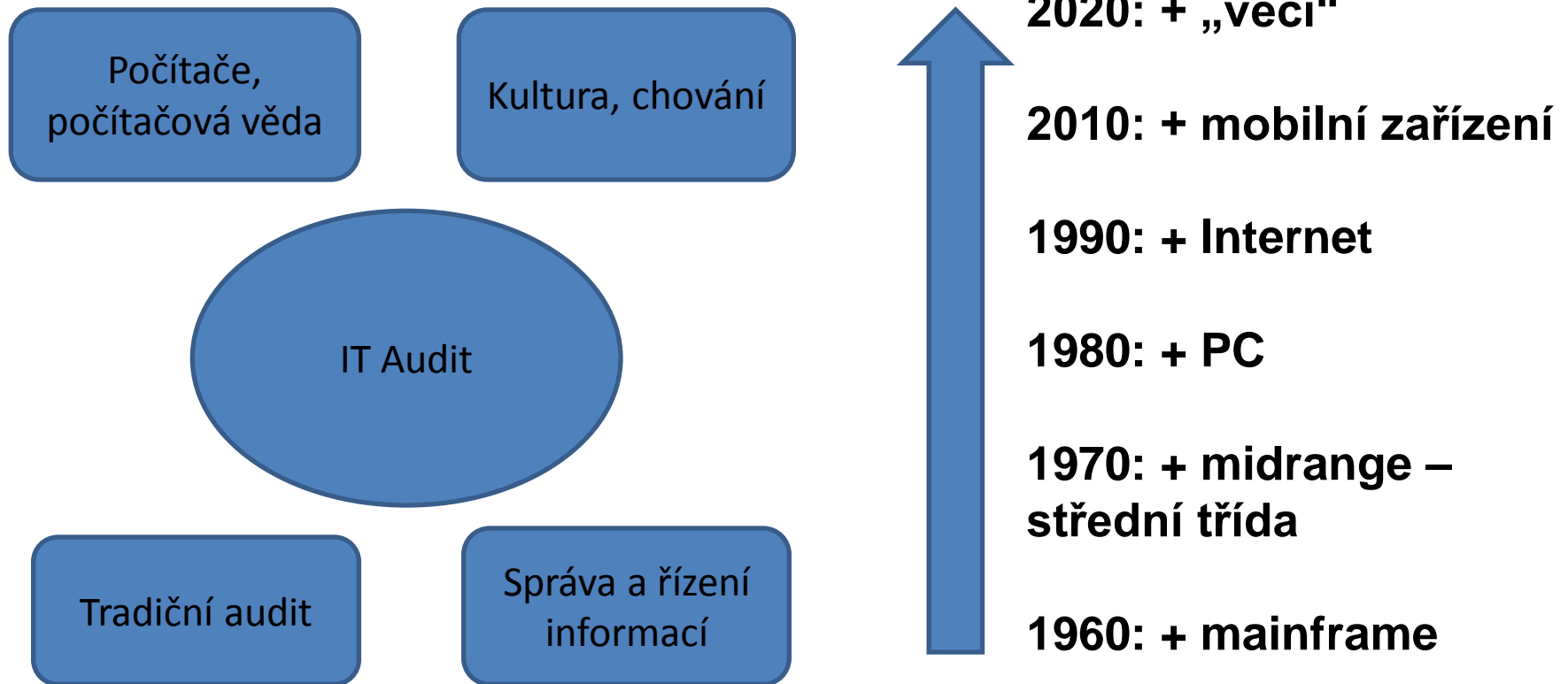
IT Audit a testy

Luboš Klečka
Česká spořitelna





IT Audit v3





Proces provádění auditu

- Příprava auditu a tvorba programu auditu
- Provádění auditu (*získávání, zkoumání a vyhodnocování informací*)
- Ukončení auditu
- Hodnocení kvality auditu
- Ověřování plnění opatření





Příprava auditu a tvorba programu

- Určení auditorského týmu
- Návrh programu auditu
 - testové otázky
 - Zaměření
 - Způsob ověření – analýza, pokus o průnik, výpisy konfigurací....
 - externí testy – návrh zadání, výběr partnera, příprava smlouvy
 - harmonogram
 - auditní vzorek
- Oznamovací dopis



Prevence



Smlouva.....

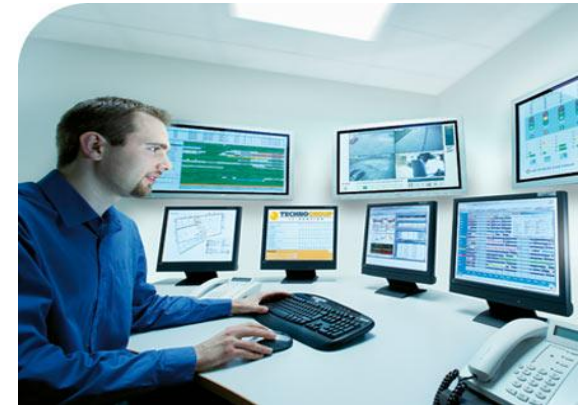
- Výběr partnera
- Určení kontaktních osob
- Zajištění mlčenlivosti
- Podrobný popis jednotlivých kroků
- Práva a povinnosti odběratele a dodavatele
 - Zajištění bezpečnostní politiky
 - Způsob ověřování
 - Formy spolupráce
 - Řešení škod
 -





Provádění auditu

- Zahájení auditu
 - Schůzka kontaktních osob
 - Předání informací
- Vlastní testy
- Záznamy a předávání informací
 - Informace o zjištěních
 - Předání auditovaným k seznámení
 - Workshopy administrátorů
- Formulace zprávy
- Projednání zprávy z auditu





Testy....

- Audity ve většině případů nejsou překvapivou činností
- Auditní kroky jsou službou klientům, pomáhají najít/specifikovat slabiny
- Mají informativní a vzdělávací charakter
- Předání podrobných informací
- Management je s nimi seznámen
- Hledá se vhodné časové okno
- Společná příprava na audit



Shrnutí....

- Preventivní opatření a spolupráce vs



"It's safe to come out - the auditors have gone."



Literatura

- Přednášky konference EuroCACCS a ISRM
- www.isaca.org

SECURITY 2013



21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Luboš Klečka, CISA, CRISC

Česká spořitelna

lklecka@csas.cz

