DŮLEŽITÝ KROK PŘI ZAVÁDĚNÍ POVINNOSTÍ NIS2

www.gordiccybersec.cz

KYBERNETIKA, BEZPEČNOST DŘÍVE A DNES

KYBERNETIKA
JE ANALYTICKÉ STUDIUM
HOMOMORFISMU
SDĚLOVÁNÍ A ŘÍZENÍ
V ORGANISMECH
MECHANISMECH
A SPOLEČNOSTI

Zdroj: Česká televize – pořad iNDUSTRIE

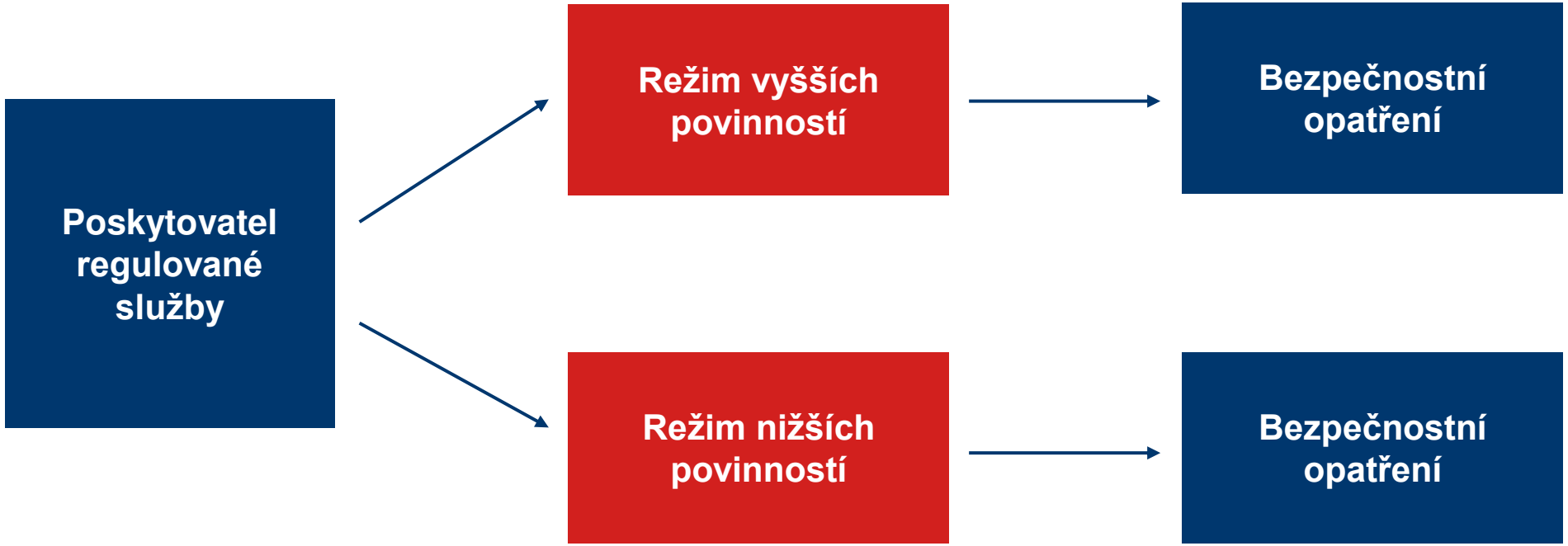
Nejdůležitějším krokem je:

pochopit a srozumitelně definovat

co potřebujeme chránit.

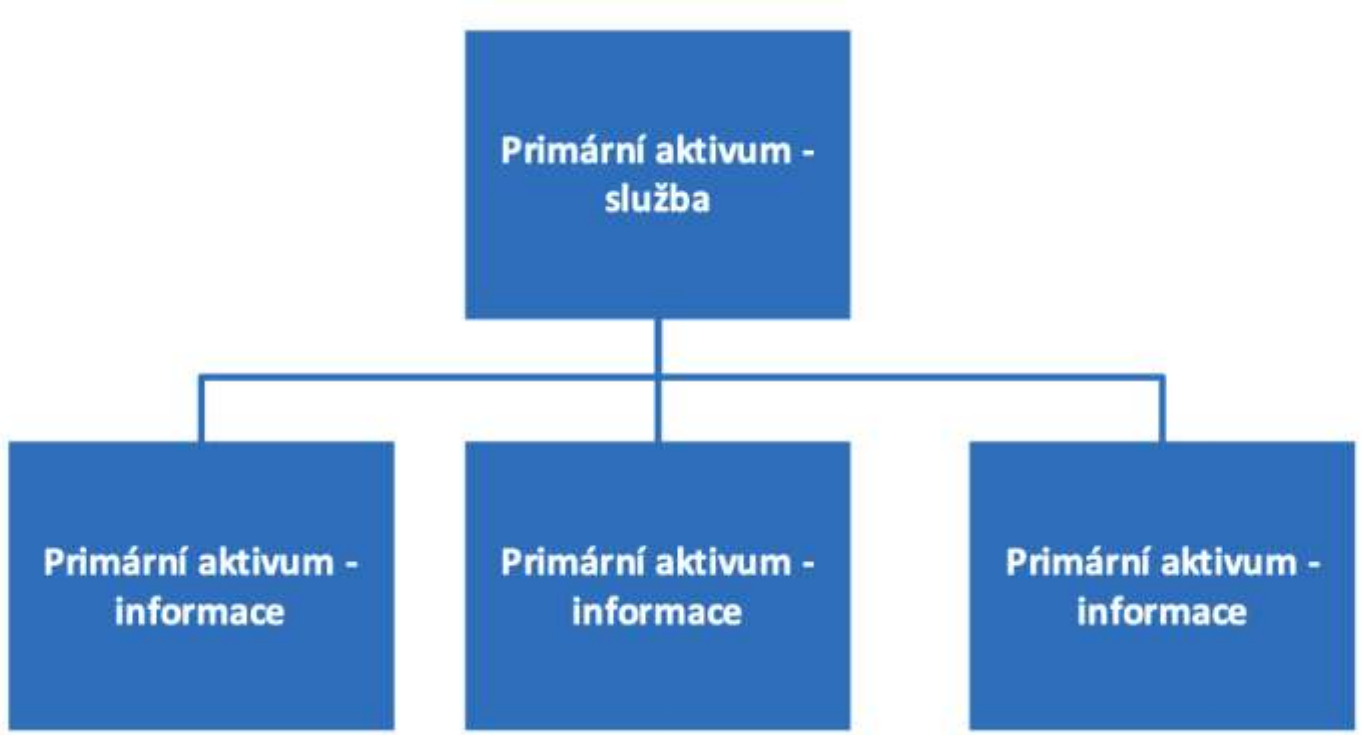
Identifikace aktiv → Analýza rizik → Bezpečnostní opatření → Kontinuální zlepšování

POCHOPIT A DEFINOVAT



*zdroj NÚKIB

POCHOPIT A DEFINOVAT



**zdroj NÚKIB*

Slabá místa NESYSTÉMOVÉ analýzy rizik

- **Kapacity**
- **Identifikace aktiv**
- Absence **vazeb** mezi aktivy
- Nevhodně zvolená **metodika** pro analýzu rizik
- **Nesrozumitelné** výstupy
- **Motivace** zaměstnanců při dlouhotrvajících projektech

SYSTÉMOVÁ analýza rizik (CSA)

- Kompletní **metodika** vyhlášky a zákona o Kybernetické bezpečnosti „**ZoKB**“
- Dostupnost **24/7**
- Zvýšení integrity dat
- Elektronizace **Prohlášení o aplikovatelnosti**
- Elektronizace **Plánu zvládání rizik**
- **Intuitivní** a **uživatelsky** přívětivé prostředí
- Zdroj informací pro kontrolní orgány

Dashboard
Číselníky
Aktiva
Mapa aktiv
Hodnocení rizik
Zvládání rizik
Plány kontinuity
Prohlášení o aplikovatelnosti
Události a incidenty
Hodnocení dodavatelů
Auditní log

A1: Služba GCS

Druh	primární aktivum
Typ	Služba
Garant	EN Erika Nejedlá
Schváleno VKB	☑

Hodnocení aktiva

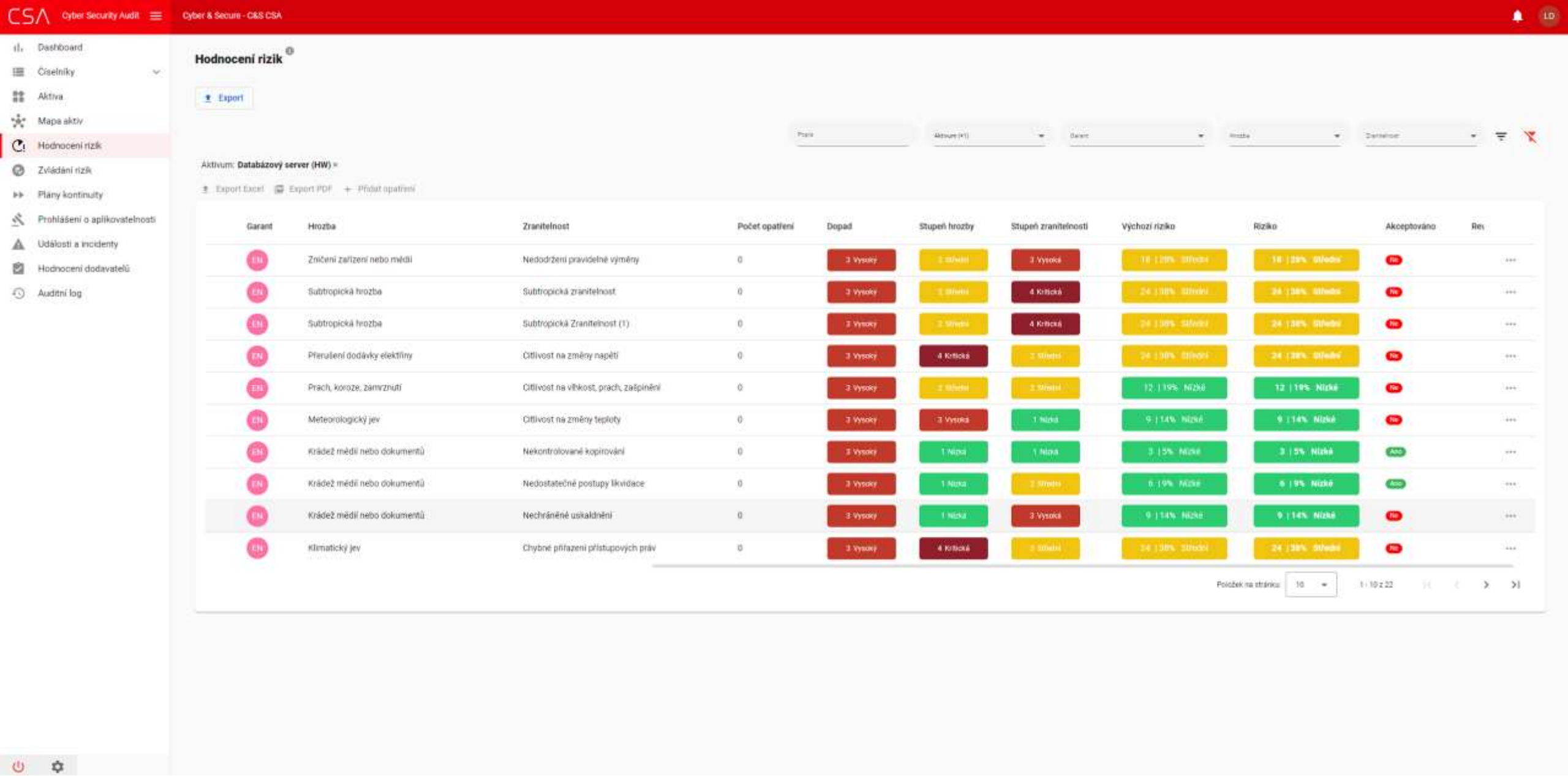
Důvěrnost (C)	2 Střední
Integrita (I)	4 Kritická
Dostupnost (A)	3 Vysoká

Výsledný dopad: 4 Kritický

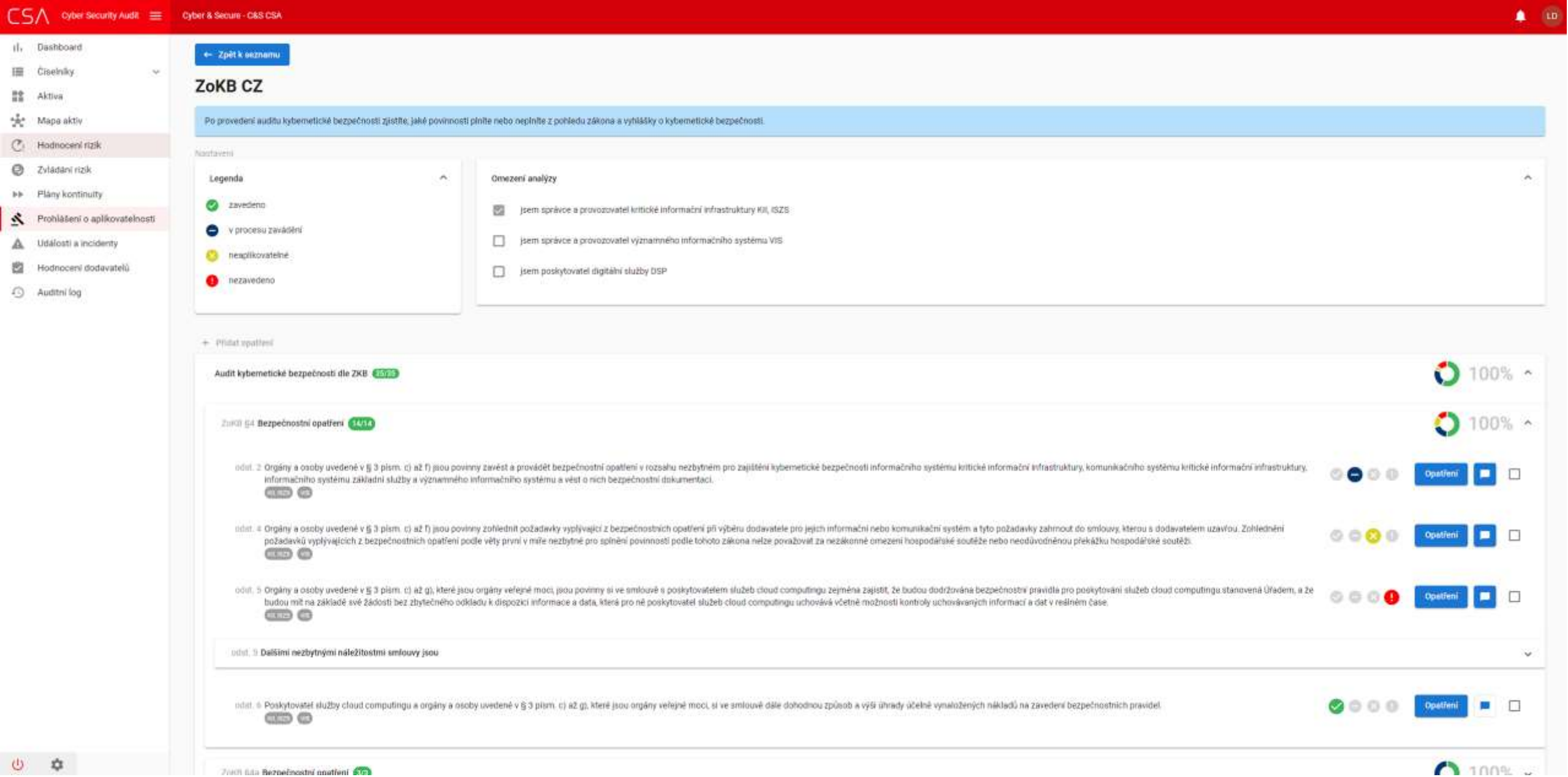
Může znamenat existenční potíže organizace.

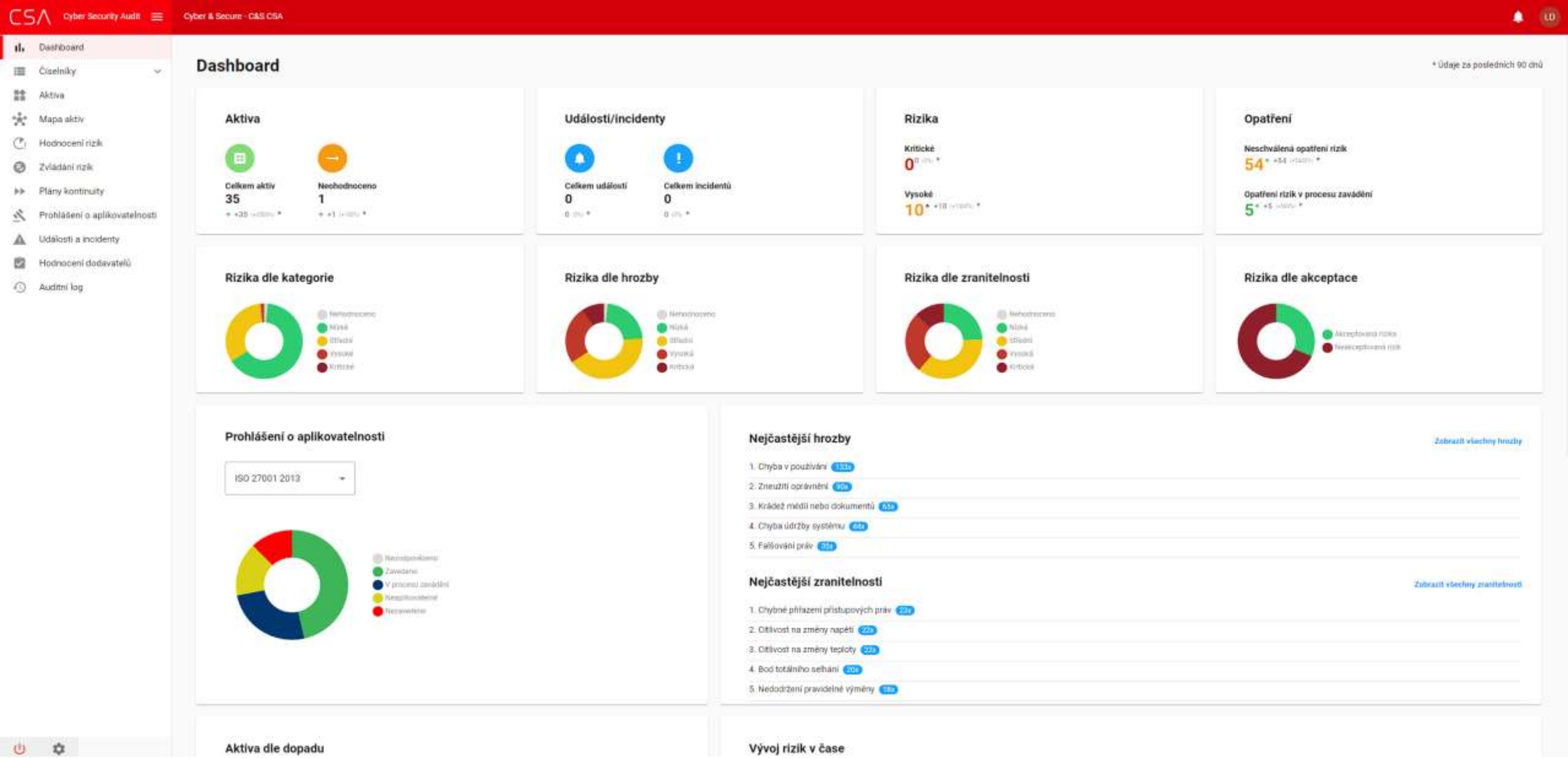
8	1	36 Vysoké	
Celkový počet rizik	Počet navržených opatření	Hodnota nejvyššího rizika	Vývoj nejvyššího rizika v čase

Obecné | Vazby aktiv | Rizika | Hodnocení důležitosti | Způsoby používání a manipulace | Přijmuté položky | Historie aktiva



GORDIC KYBERNETICKÁ BEZPEČNOST


CSA Cyber Security Audit
Cyber & Secure - C&S CSA
LD
Dashboard
Číselníky
Aktiva
Mapa aktiv
Hodnocení rizik
Zvládání rizik
Plány kontinuity
Prohlášení o aplikovatelnosti
Události a incidenty
Hodnocení dodavatelů
Auditní log
← Zpět k seznamu
ZoKB CZ
Po provedení auditu kybernetické bezpečnosti zjistíte, jaké povinnosti plníte nebo neplníte z pohledu zákona a vyhlášky o kybernetické bezpečnosti.
Nastavení
Legenda
zavedeno
v procesu zavádění
neaplikovatelné
nezavedeno
Omezení analýzy
jsem správce a provozovatel kritické informační infrastruktury KII, ISZS
jsem správce a provozovatel významného informačního systému VIS
jsem poskytovatel digitální služby DSP
+ Přidat opatření
Audit kybernetické bezpečnosti dle ZKB 35/35
100%
ZoKB §4 Bezpečnostní opatření 14/14
100%
odst. 2 Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.
Opatření
odst. 4 Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.
Opatření
odst. 5 Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase.
Opatření
odst. 9 Dalšími nezbytnými náležitostmi smlouvy jsou
odst. 6 Poskytovatel služby cloud computingu a orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, si ve smlouvě dále dohodnou způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel.
Opatření
ZoKB §4a Bezpečnostní opatření


CSA
Cyber Security Audit
Cyber & Secure - C&S CSA
Dashboard
Číselníky
Aktiva
Mapa aktiv
Hodnocení rizik
Zvládání rizik
Plány kontinuity
Prohlášení o aplikovatelnosti
Události a incidenty
Hodnocení dodavatelů
Auditní log
Dashboard
* Údaje za posledních 90 dnů
Aktiva
Celkem aktiv
35
Nechodnoceno
1
Události/incidenty
Celkem událostí
0
Celkem incidentů
0
Rizika
Kritické
0
Vysoké
10
Opatření
Neschválená opatření rizik
54
Opatření rizik v procesu zavádění
5
Rizika dle kategorie
Rizika dle hrozby
Rizika dle zranitelnosti
Rizika dle akceptace
Akceptovaná rizika
Neakceptovaná rizika
Prohlášení o aplikovatelnosti
ISO 27001 2013
Nejčastější hrozby
Zobrazit všechny hrozby
1. Chyba v používání 133x
2. Zneužití oprávnění 90x
3. Krádež médií nebo dokumentů 65x
4. Chyba údržby systému 44x
5. Falšování práv 35x
Nejčastější zranitelnosti
Zobrazit všechny zranitelnosti
1. Chybné přiřazení přístupových práv 23x
2. Citlivost na změny napětí 22x
3. Citlivost na změny teploty 22x
4. Bod totálního selhání 20x
5. Nedodržení pravidelné výměny 18x
Aktiva dle dopadu
Vývoj rizik v čase

Úspěšné posouzení shody

Reference


MĚSTSKÁ ČÁST
PRAHA 8


Český úřad pro zkoušení zbraní a střeliva
www.cuzzs.cz


ÚŘAD PRO CIVILNÍ LETECTVÍ


EOP
ELEKTRÁRNY
OPATOVICE


Karlovarský
kraj


SPRÁVA
ZÁKLADNÍCH
REGISTRŮ


mero
MERO ČR, a.s.


jihočeské
nemocnice


Draslovka


PROGRESSIVE
PSTCLC
LOGISTICS
MITSUI-SOKO GROUP


energy
Energie pro budoucnost a stabilitu


innogy

GORDIC

Děkuji za pozornost

František Janů

773 049 126

www.gordiccybersec.cz