Analýza rizik kybernetické bezpečnosti
-
od teorie k praxi

František Janů

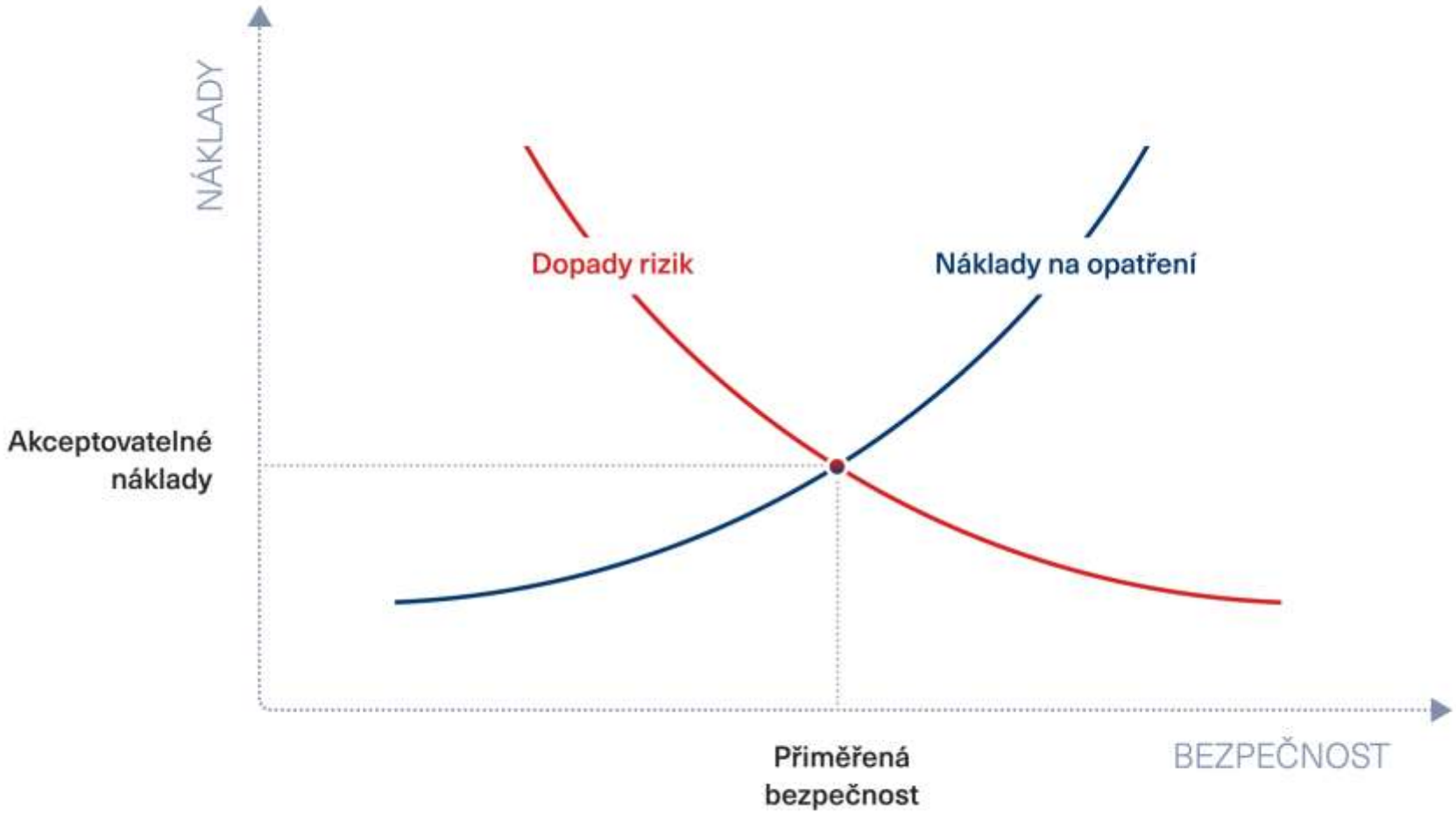
K čemu nám vlastně je analýza rizik?

- Jakým hrozbám může být organizace vystavena?
- Jsou naše aktiva zranitelná?
- Jaké dopad by to mohlo mít na naši organizaci?
  - Finanční ztráta
  - Poškození pověsti atd…

Co je cílem analýzy rizik?

- Pomoci najít „přiměřenou bezpečnost“
  - Abychom byli v bezpečí
  - Abychom určili přiměřené náklady

Jak najít „přiměřenou“ bezpečnost?

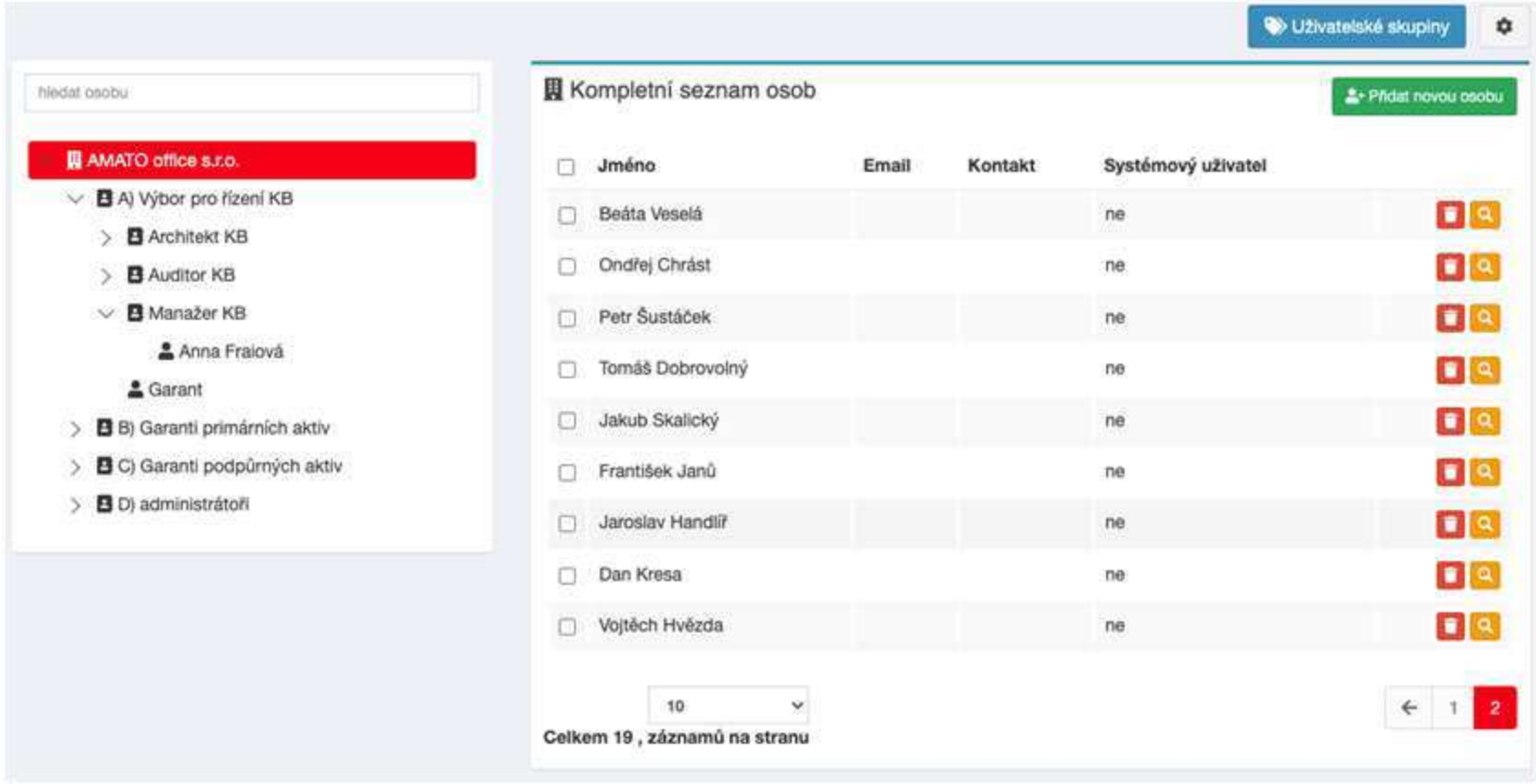


GORDIC

CSA

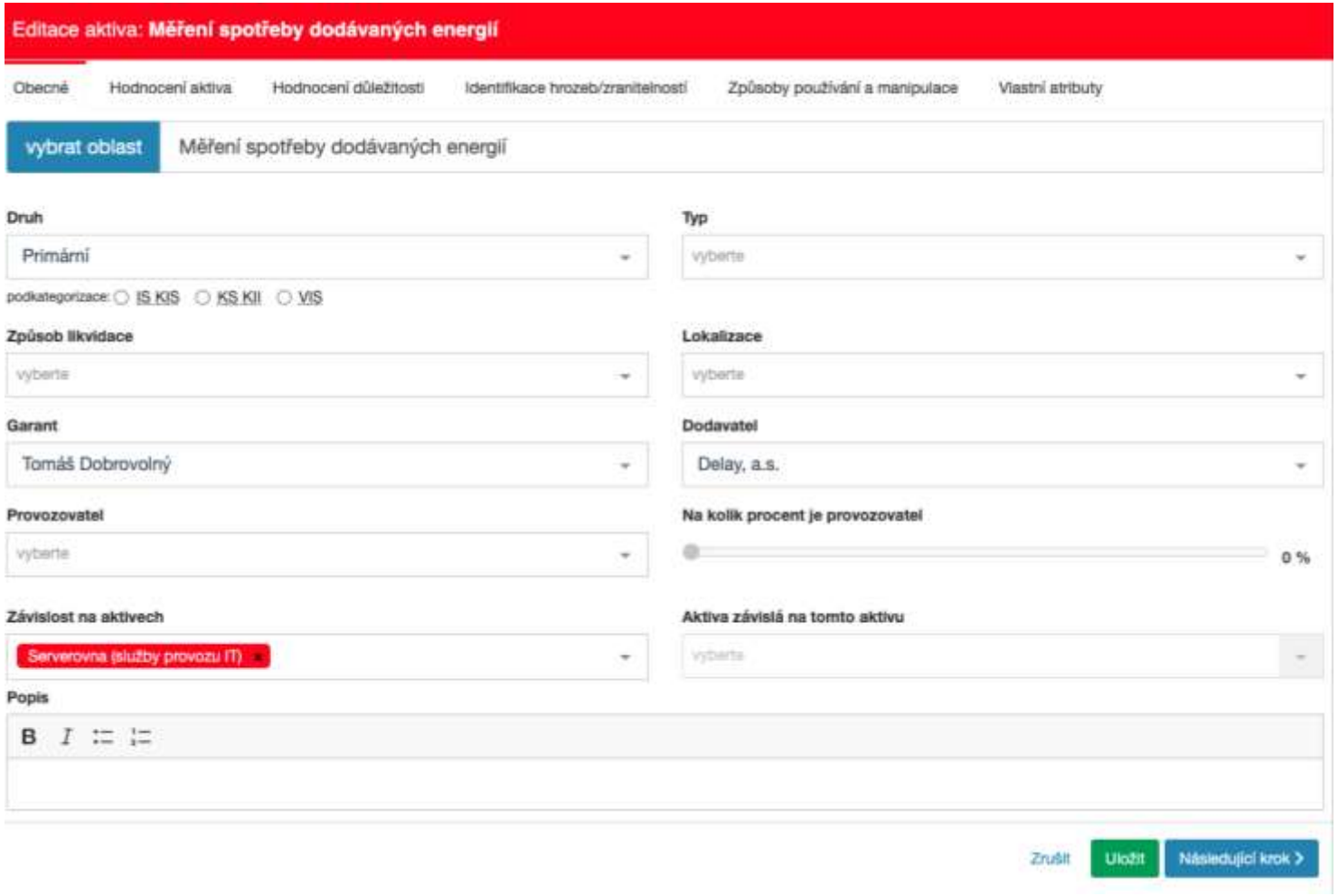
CSA – online analýza rizik

Bezpečnostní role



§ 6 Organizační bezpečnost | § 7 Bezpečnostní role

Analýza aktiv



§ 4 Řízení aktiv

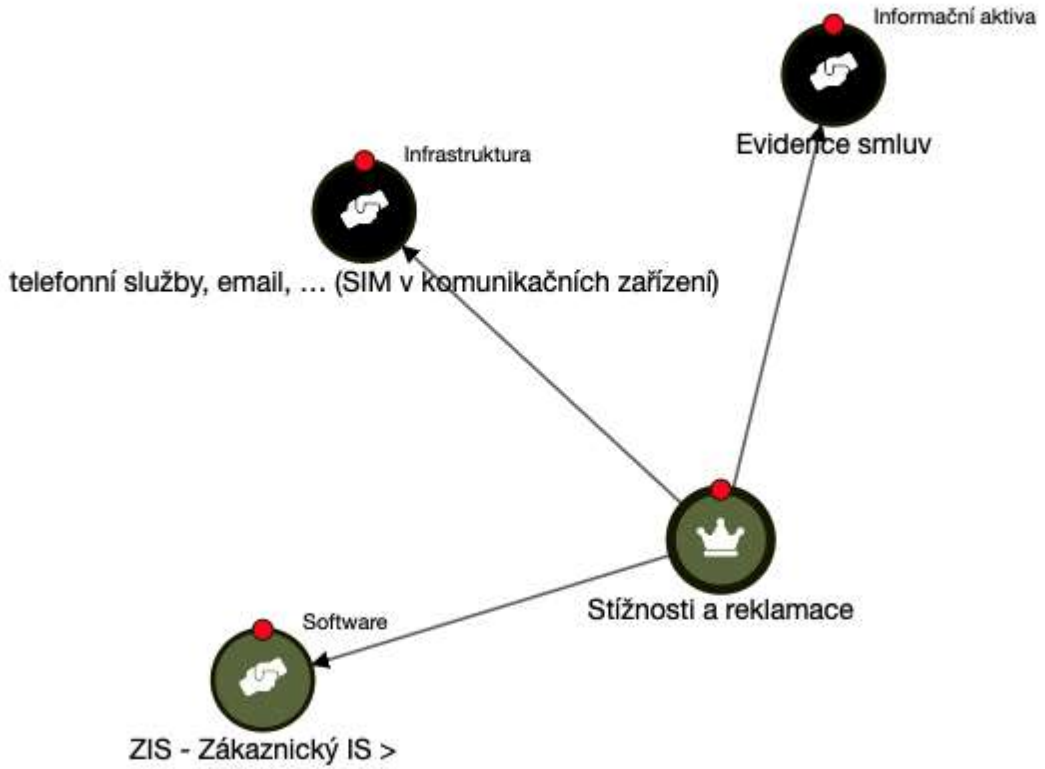
Určení vazeb mezi aktivy

Druhy aktiv

- Podpůrné ☑
- Primární ☑
  IS KIS / KS KII / VIS
- Nezařazeno ☑

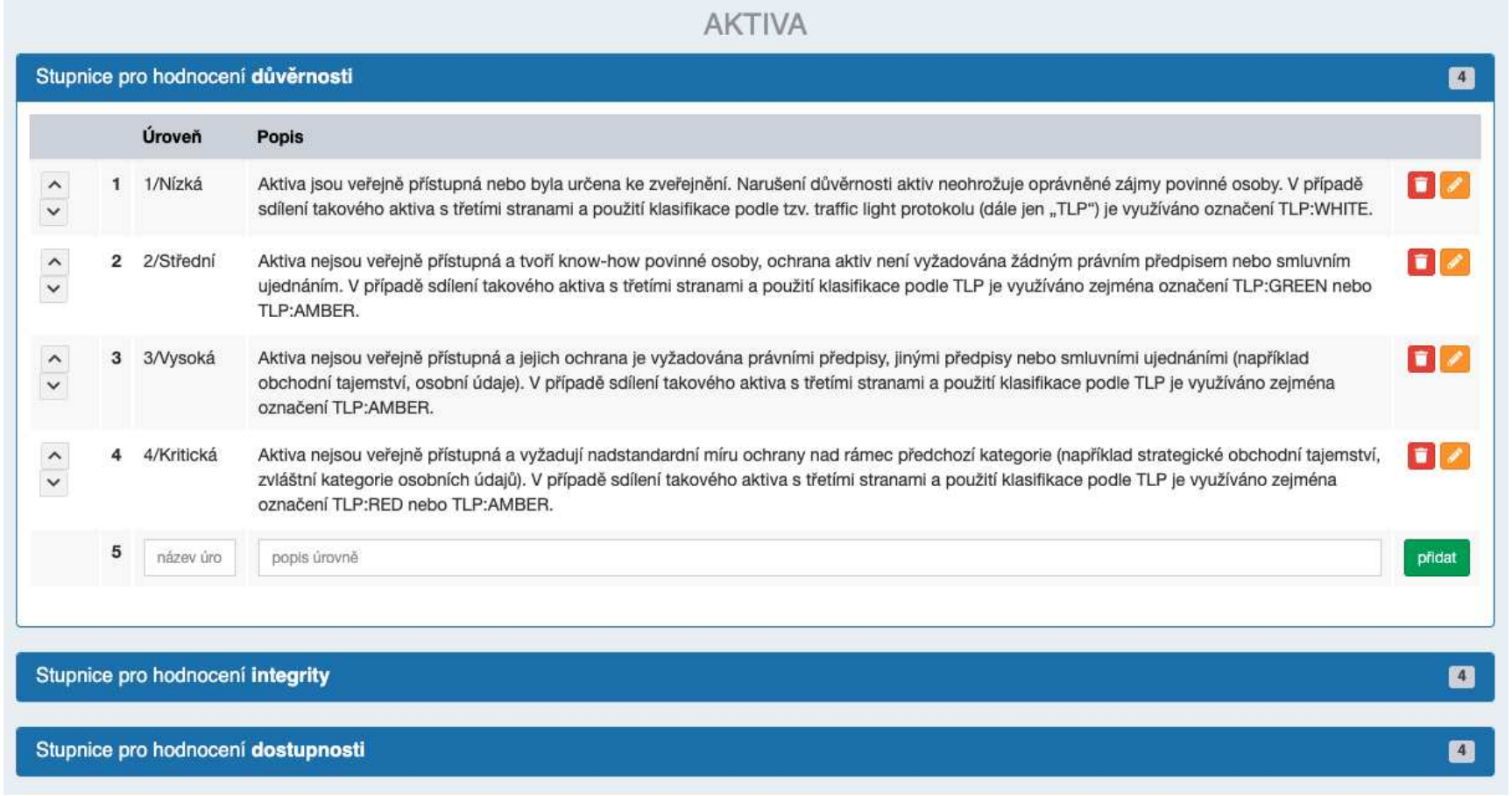
Klasifikace rizik

- Nízké
- Střední
- Vysoké
- Kritické
- Neohodnoceno



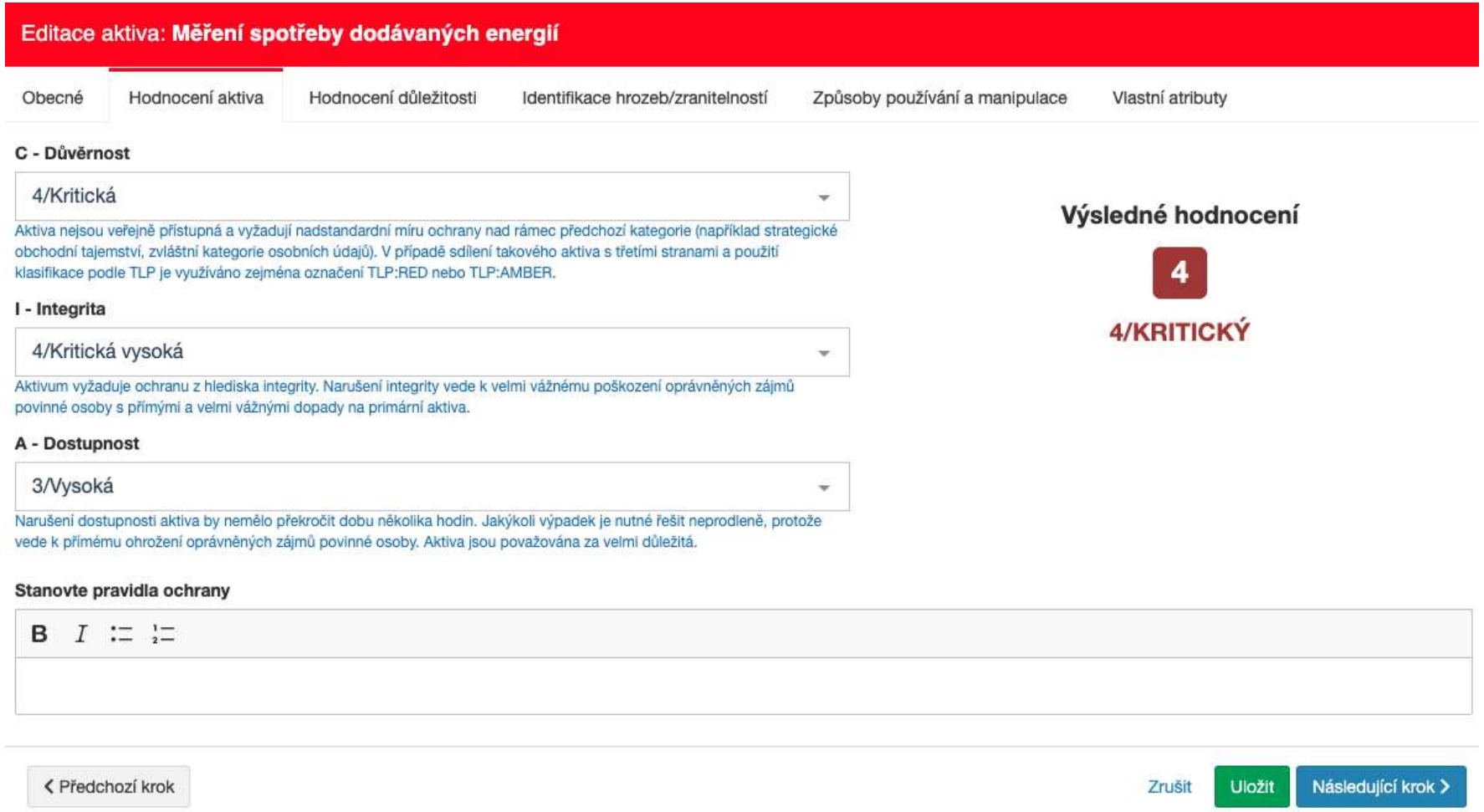
§ 4 Řízení aktiv

Hodnocení aktiv



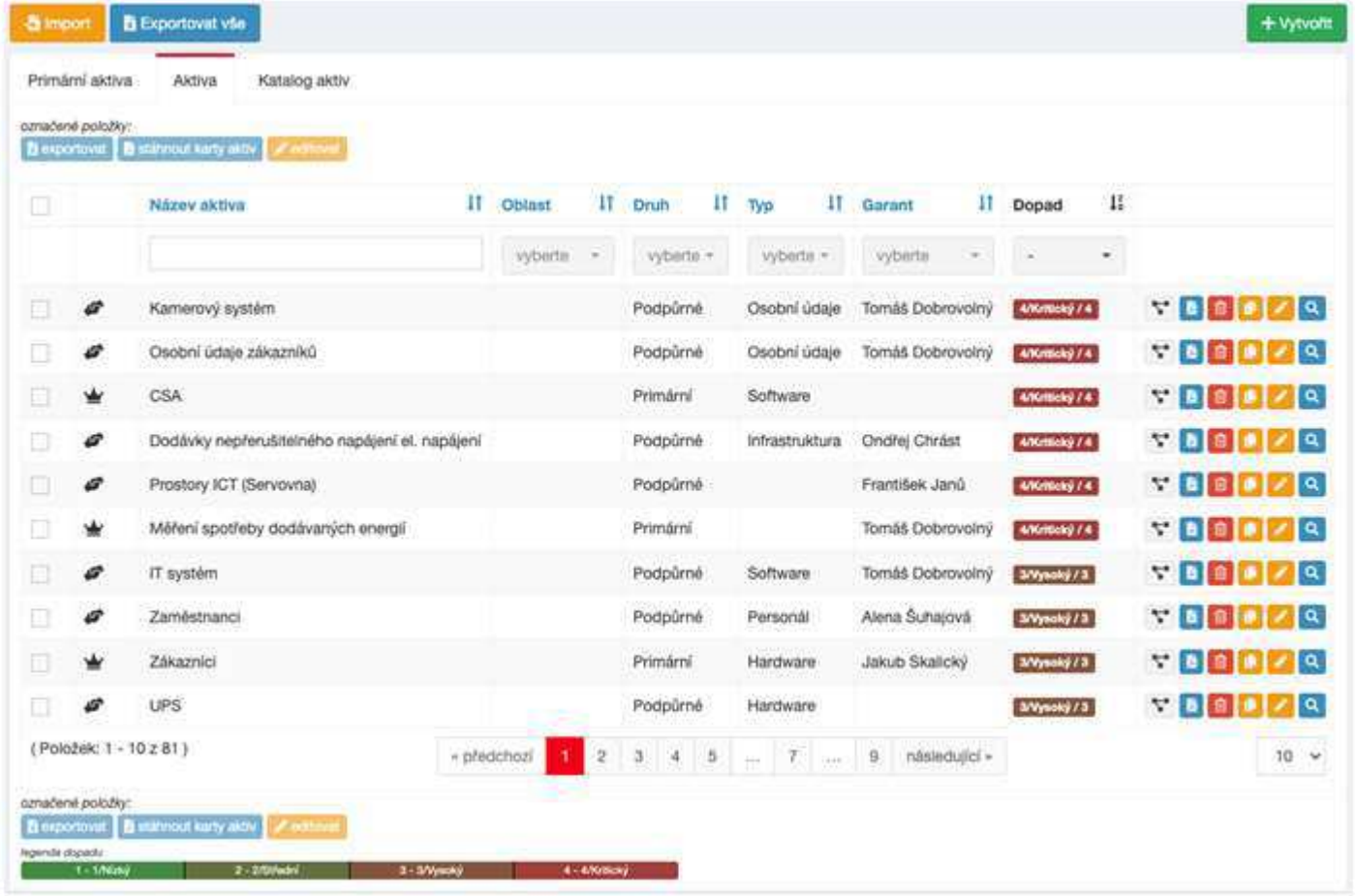
§ 4 Řízení aktiv

Hodnocení aktiv



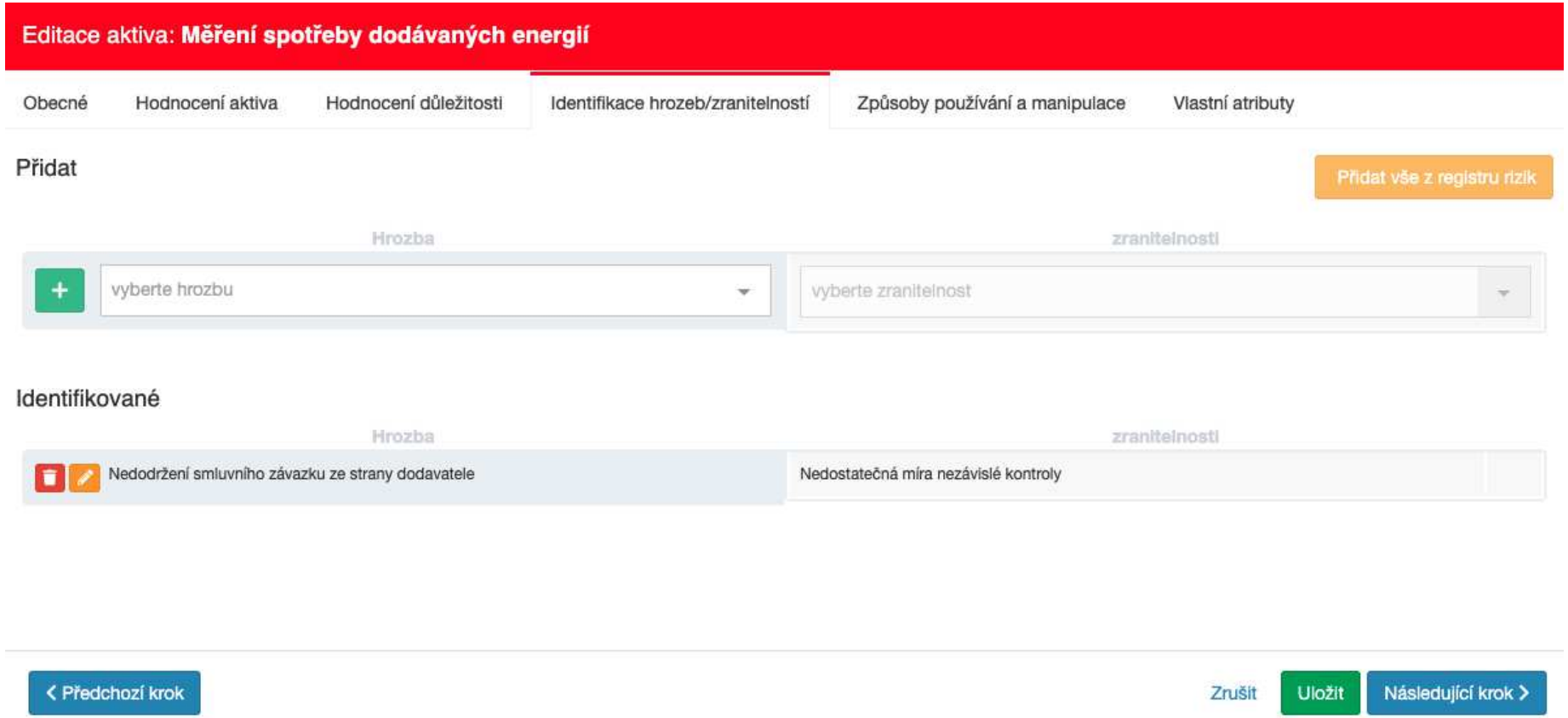
§ 4 Řízení aktiv

Analýza aktiv



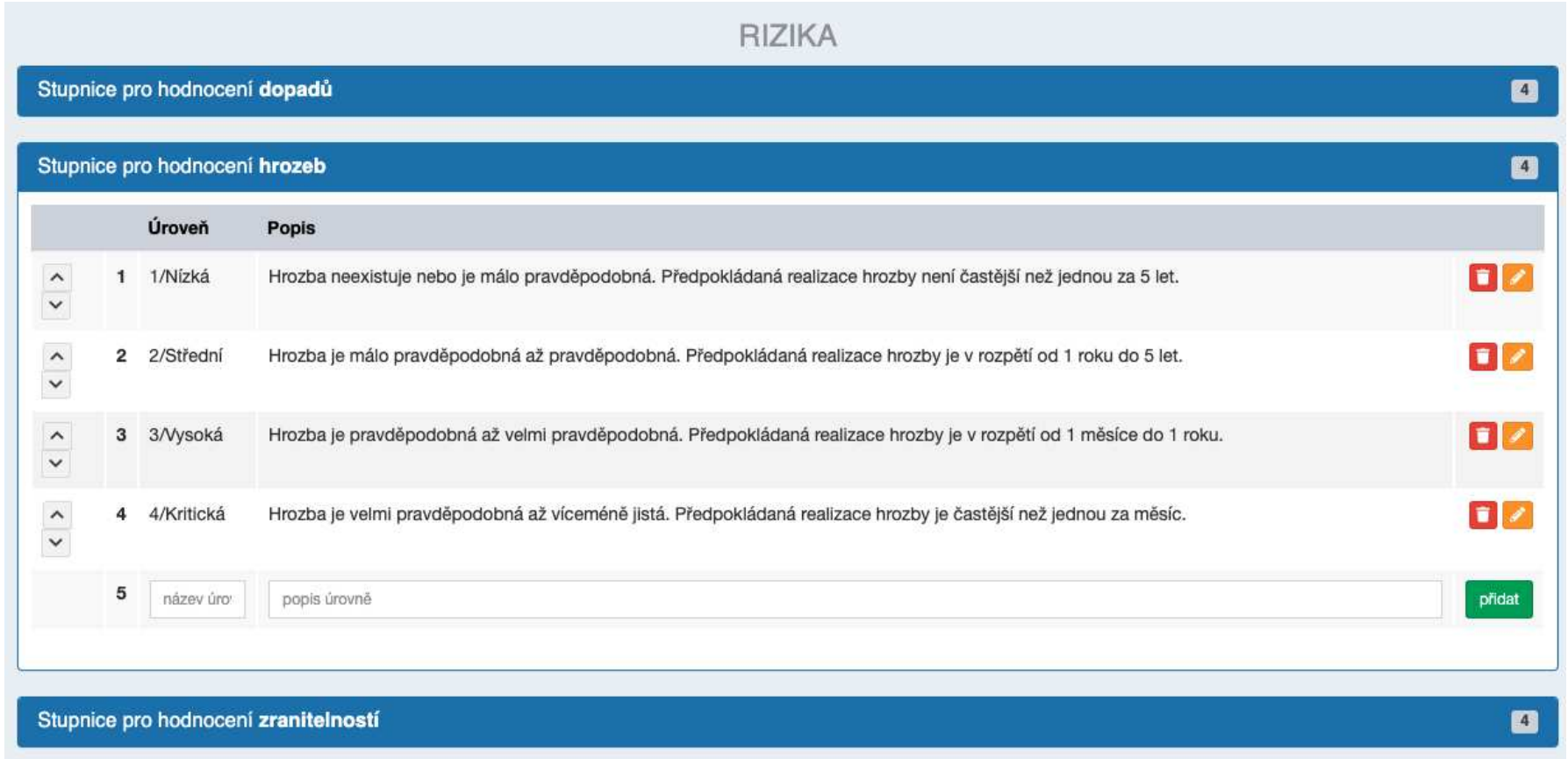
§ 4 Řízení aktiv

Identifikace hrozeb a zranitelností



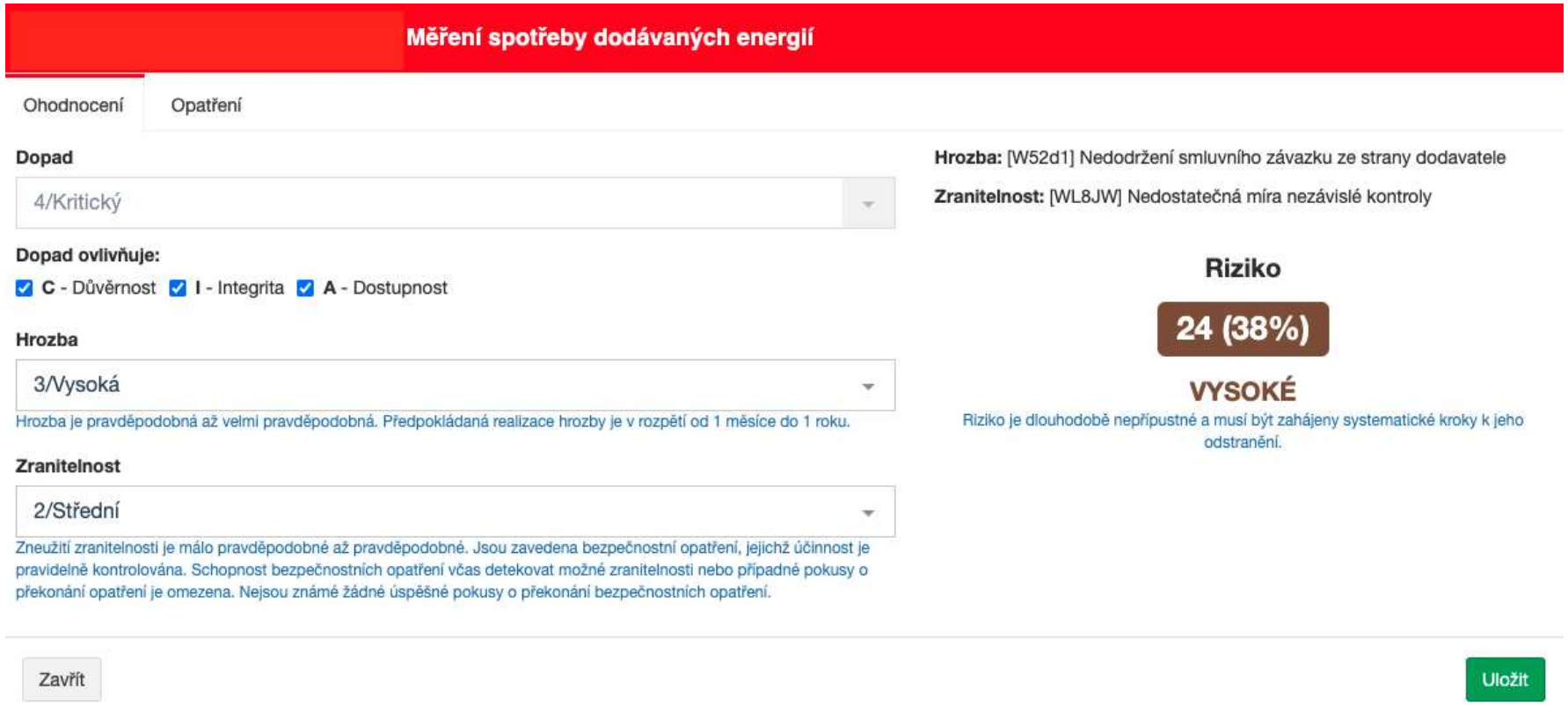
§ 4 Řízení aktiv | § 5 Řízení rizik

Hodnocení rizik



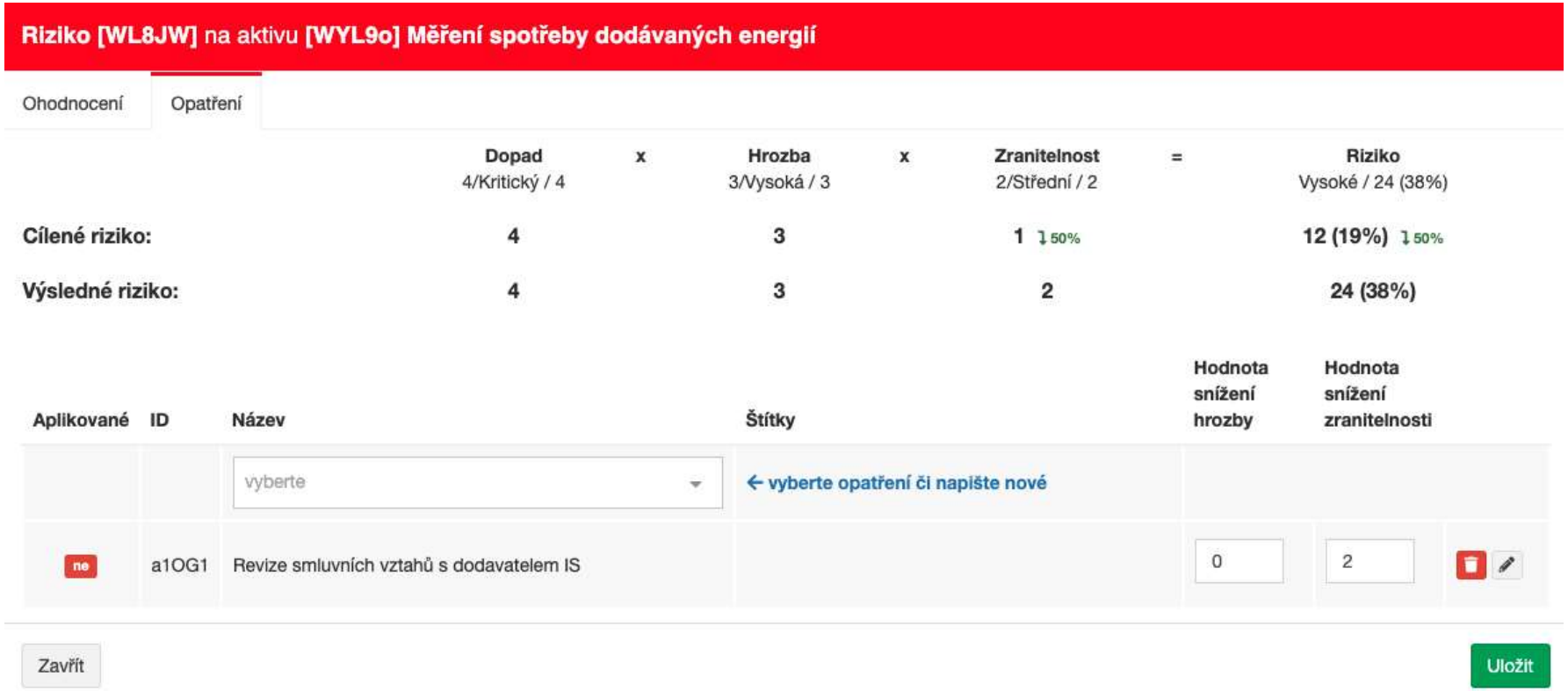
§ 5 Řízení rizik

Hodnocení rizik



§ 5 Řízení rizik

Návrh opatření pro snížení rizik



§ 5 Řízení rizik

Prezentace výsledných rizik

označené položky:

exportovat | stáhnout karty rizik

Aktivum	Druh	Garant	Druh hrozby	Druh zranitelnosti	Dopad	Hrozba	Zranitelnost	Riziko	Cílené riziko	Výsledné riziko	Akceptováno
	vyberte	vyberte			vyberte	vyberte	vyberte	vyberte	vyberte	vyberte	-
Service desk	Podpůrné		Chybné fungování aplikačního programového vybavení	Nejasné nebo neúplné zadání pro vývojáře	3/Vysoký / 3	4/Kritická / 4 !	4/Kritická / 4	Vysoké / 48 (75%)	Vysoké / 48 (75%)	Vysoké / 48 (75%)	ne
Zaměstnanci	Podpůrné	Alena Šuhajová	Zdravotní stav	Covid-19	3/Vysoký / 3	4/Kritická / 4	4/Kritická / 4	Vysoké / 48 (75%)	Vysoké / 48 (75%)	Vysoké / 48 (75%)	ne
Service desk	Podpůrné		Zneužití oprávnění	Známé chyby v programech	3/Vysoký / 3	4/Kritická / 4	4/Kritická / 4	Vysoké / 48 (75%)	Vysoké / 48 (75%)	Vysoké / 48 (75%)	ne
IT systém	Podpůrné	Tomáš Dobrovolný	Falšování práv	Nechráněné tabulky s hesly	3/Vysoký / 3	4/Kritická / 4	3/Vysoká / 3	Vysoké / 36 (56%)	Vysoké / 36 (56%)	Vysoké / 36 (56%)	ne
Dodávky nepřerušitelného napájení el. napájení	Podpůrné	Ondřej Chrást	Narušení fyzické bezpečnosti	Nedostatečná ochrana aktiv	4/Kritický / 4	3/Vysoká / 3	3/Vysoká / 3	Vysoké / 36 (56%)	Vysoké / 36 (56%)	Vysoké / 36 (56%)	ne | A
Dodávky nepřerušitelného napájení el. napájení	Podpůrné	Ondřej Chrást	Pochybení ze strany zaměstnanců	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů	4/Kritický / 4	3/Vysoká / 3	3/Vysoká / 3	Vysoké / 36 (56%)	Vysoké / 36 (56%)	Vysoké / 36 (56%)	ne | A

GORDIC

Prezentace výsledných rizik

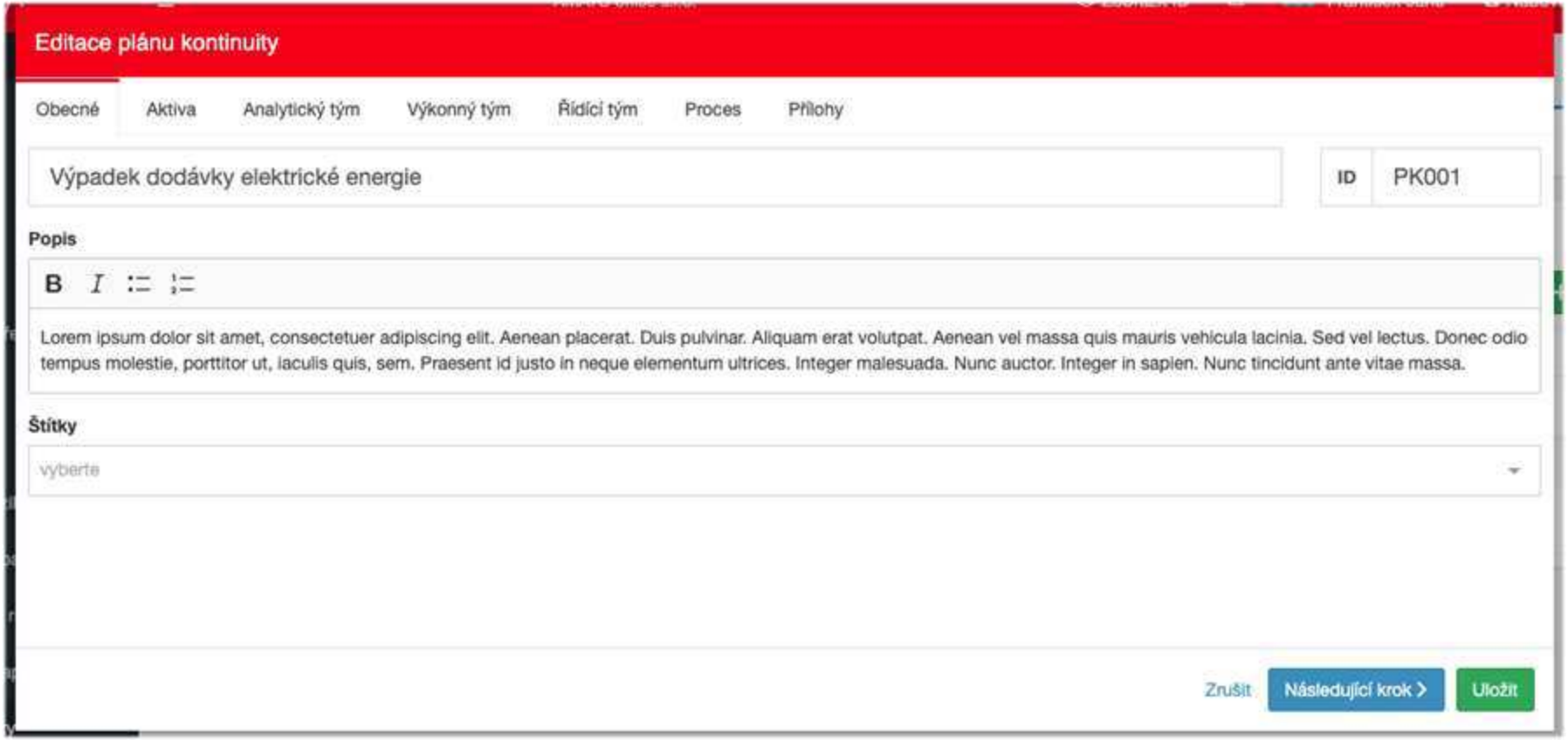
Aktiva s nejvyšší hodnotou rizika | Rizika

Aktivum	Druh	Garant	Nejvyšší riziko
	vyberte	vyberte	vyberte
Service desk	Podpůrné		Vysoké / 48 (75%)
Zaměstnanci	Podpůrné	Alena Šuhajová	Vysoké / 48 (75%)
Dodávky nepřerušitelného napájení el. napájení	Podpůrné	Ondřej Chrást	Vysoké / 36 (56%)
IT systém	Podpůrné	Tomáš Dobrovolný	Vysoké / 36 (56%)
Interní procesy	Podpůrné	Lucie Juřičková	Vysoké / 32 (50%)
Zákazníci	Primární	Jakub Skalický	Vysoké / 27 (42%)
Žádosti o přípojky	Primární	Jaroslav Handlíř	Vysoké / 27 (42%)
Osobní údaje zákazníků	Podpůrné	Tomáš Dobrovolný	Vysoké / 24 (38%)
Prostory ICT (Servovna)	Podpůrné	František Janů	Vysoké / 24 (38%)
Měření spotřeby dodávaných energií	Primární	Tomáš Dobrovolný	Vysoké / 24 (38%)

(Položek: 1 - 10 z 81) « předchozí 1 2 3 4 5 ... 7 ... 9 následující » 10

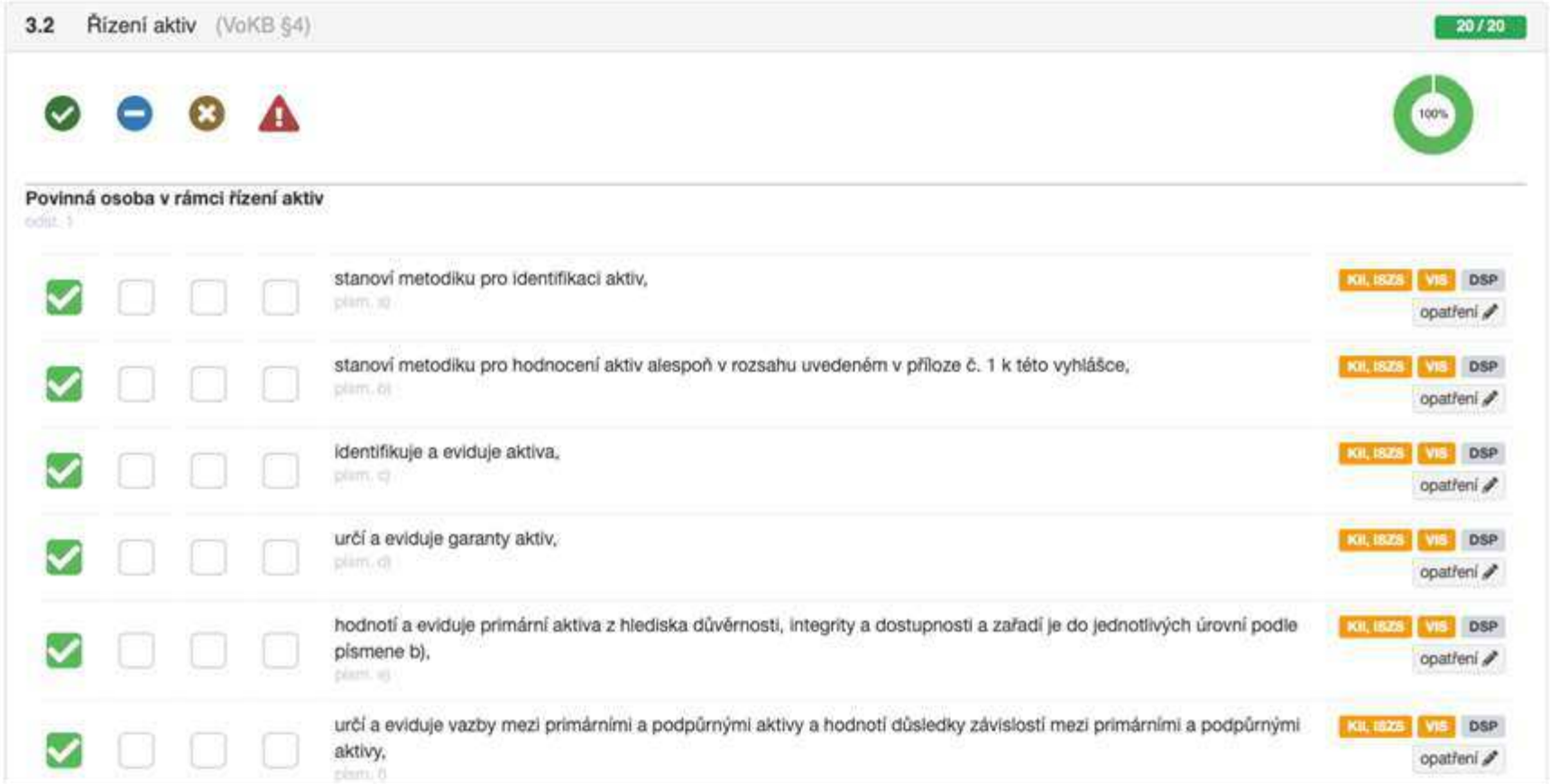
GORDIC

Plány kontinuity



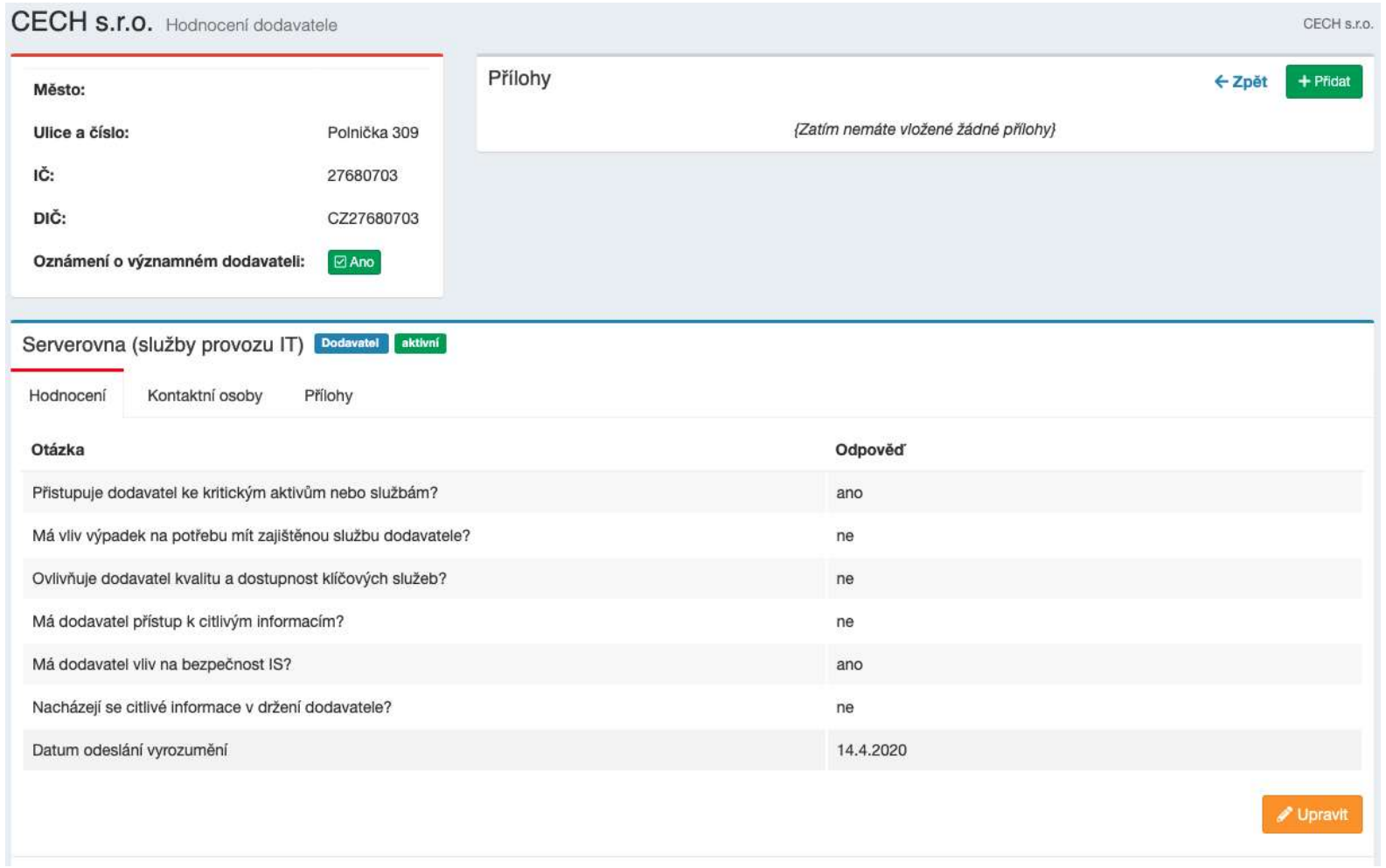
§ 15 Řízení kontinuity činností

Plnění legislativních povinností



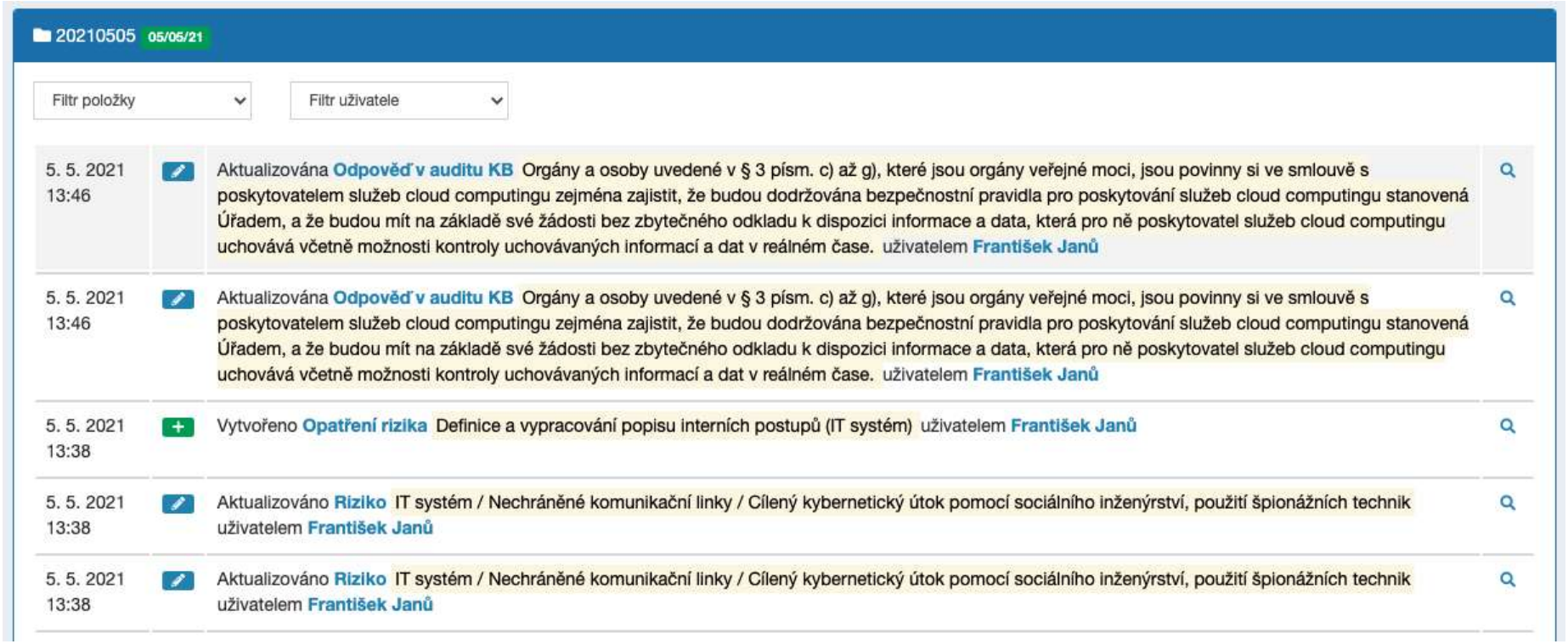
GORDIC

Hodnocení dodavatelů



§ 8 Řízení dodavatelů

Auditní log


20210505 05/05/21
Filtr položky
Filtr uživatele
5. 5. 2021 13:46
Aktualizována Odpověď v auditu KB 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. uživatelem František Janů
5. 5. 2021 13:46
Aktualizována Odpověď v auditu KB 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. uživatelem František Janů
5. 5. 2021 13:38
Vytvořeno Opatření rizika Definice a vypracování popisu interních postupů (IT systém) uživatelem František Janů
5. 5. 2021 13:38
Aktualizováno Riziko IT systém / Nechráněné komunikační linky / Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik uživatelem František Janů
5. 5. 2021 13:38
Aktualizováno Riziko IT systém / Nechráněné komunikační linky / Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik uživatelem František Janů

Děkuji za pozornost.

František Janů

frantisek_janu@gordic.cz

+420 773 049 126