

Implementace řízení strategických a kybernetických rizik v Pražská teplárenské s podporou SW nástroje Risk management tool

Jiří Knápek – Manažer realizace NETIA® s.r.o.

NETIA® s.r.o

- Společnost poskytující konzultace v oblasti projektového řízení a řízení rizik
- Dodavatel SW pro řízení rizik a interních auditů
- Certifikovaný partner společnosti Oracle pro dodávky SW Primavera
- Certifikace pro dodávky aplikací a technologií Oracle – Oracle PPM, Oracle Innovation management, databáze Oracle
- Dodávky SW pro řízení rizik, interních auditů a kybernetické bezpečnosti – Risk management tool, Audit team assitant
- Dodávka a implementace SW pro řízení GDPR – SW GDPR assitant
- Projektové řízení (metodologie PRINCE2, PMI, IPMA)
- Založena 2000

Zadání projektu

Společnost Pražská teplárenská provozuje systémy Kritické infrastruktury státu – patří pod Zákon o kybernetické bezpečnosti:

- Zákon o kybernetické bezpečnosti (ZoKB) 181/2014 Sb, včetně novelizace – co se má dělat
- Vyhláška kybernetické bezpečnosti (VoKB) č. 82/2018 Sb., – jak se to má dělat

Řízení aktiv a řízení rizik – patří do organizačních opatření, základní metodický rámec je uveden ve vyhlášce – VoKB

Společnost má nastaveny procesy řízení strategických rizik a zpracování metodiku řízení rizik

Cíl: Implementace SW podpory uvedených procesů

Doba trvání projektu: od 1.10.2018 do 31.1.2019

POKRYTÉ PROCESY v SW Risk management tool (RMT)

- Řízení strategických rizik
- Práce s incidenty (řízení a evidence incidentů)
- Řízení aktiv, práce s aktivy – primární, podpůrná
- Řízení kybernetických rizik
- Práce s hrozbami, protiopatřeními
- Plány zvládání rizik

Pozn: SW se implementuje dle metodik používaných zákazníkem, není nezbytně nutné zahrnout všechny oblasti.

ÚVODNÍ OBRAZOVKA- Risk management tool

teamassistant

+

Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Domů

Dashboard

Nastavit jako výchozí

Reset

Přidat

Domů

Všechny mé úkoly

Název úkolu

Název případu

Vlastník případu

Datum zadání

Termín

Realizace opatření	RMS - KRISK-2019-00003/opatř...	Knápek Jiří	22.02.2019 16:37	
Analýza rizika (Externí dodavat...	RMS - KRISK-2019-00004 - Exte...	Mynář Josef	11.02.2019 9:35	
Hodnocení důležitosti primární...	RMS - AKTI-2019-00006: yyy	Mynář Josef	11.02.2019 9:29	
Zadat úkol	RMS - 19-00002	Mynář Josef	11.01.2019 9:11	
Zadání a hodnocení aktiva	RMS - AKTI-2019-00003	Mynář Josef	11.01.2019 8:15	
Analýza rizika (Server SAP)	RMS - KRISK-2018-00011 - Serv...	Mynář Josef	14.12.2018 13:28	
Rizika Provoz	RMS - RSRISK-2018-00005	Mynář Josef	14.12.2018 13:27	
Rizika IT	RMS - RSRISK-2018-00005	Mynář Josef	14.12.2018 13:27	
Rizika HR	RMS - RSRISK-2018-00005	Mynář Josef	14.12.2018 13:27	
Rizika Finance	RMS - RSRISK-2018-00005	Mynář Josef	14.12.2018 13:27	

1 / 7

Počet záznamů: ?

Rozšířit sloupce

Přehled - Strategická rizika

Název případu

Vlastník

Zadáno

V řešení

RMS - RSRISK-2019-00002	Mynář Josef	07.02.2019 9:12	Rizika Finance: Admin Admin, Riz...
RMS - RSRISK-2019-00001	Admin Admin	09.01.2019 19:57	Rizika Finance: Admin Admin, Riz...
RMS - RSRISK-2018-00005	Mynář Josef	14.12.2018 13:27	Rizika Finance: Mynář Josef, Rizik...
RMS - RSRISK-2018-00004	Mynář Josef	14.12.2018 13:27	Rizika Finance: Mynář Josef, Rizik...
RMS - RSRISK-2018-00003	Mynář Josef	14.12.2018 13:27	Rizika Finance: Mynář Josef, Rizik...
RMS - RSRISK-2018-00002	Admin Admin	03.12.2018 13:14	Rizika Finance: Admin Admin, Riz...
RMS - RSRISK-2018-00001	Admin Admin	20.11.2018 21:19	Rizika Finance: Admin Admin, Riz...

1 / 1

Počet záznamů: 7

Rozšířit sloupce

Přehled - Kybernetická rizika všechny

Číslo hláše...

Vlastník riz...

Informačn...

Dopad

Typ hrozby

Zranitelnost

Hrozba

Úroveň riz...

Strategie ř...

Status

RMS - KRIS...	mmmmmy	Server SAP	2,4	d) užívání...	3 - Vysoká	3 - Vysoká	21,6		V analýze
RMS - KRIS...									V zadávání
RMS - KRIS...									V zadávání
RMS - KRIS...	Hrubý	Server SAP	2,4	b) poškoze...	2 - Střední	2 - Střední	9,6	Akceptace...	
RMS - KRIS...	Stuchlý	SAP	2,7	a) porušen...	1 - Nizká	2 - Střední	5,4	Akceptace...	
RMS - KRIS...	Hrubý	Server SAP	2,4	a) porušen...	1 - Nizká	1 - Nizká	2,4	Akceptace...	
RMS - KRIS...	Hrubý	Server SAP	2,4	a) porušen...	4 - Kritická	1 - Nizká	9,6	Akceptace...	
RMS - KRIS...	Hrubý	Server SAP	2,4	b) poškoze...	2 - Střední	2 - Střední	9,6	Akceptace...	
RMS - KRIS...	Hrubý	Server SAP	2,4	f) škodlivý...	2 - Střední	4 - Kritická	19,2		V analýze

1 / 7

Počet záznamů: ?

Rozšířit sloupce

Přehled - Reporty/Registr ky...

Název případu

Zadáno

Registr rizik	20.11.2018 20:11
---------------	------------------

1 / 1

Počet záznamů: 1

Rozšířit sloupce

Kalendář

Březen 2019

Po	Út	St	Čt	Pá	So	Ne
25	26	27	28	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Tas 383270:b876d0487ce4 tas4 tas4

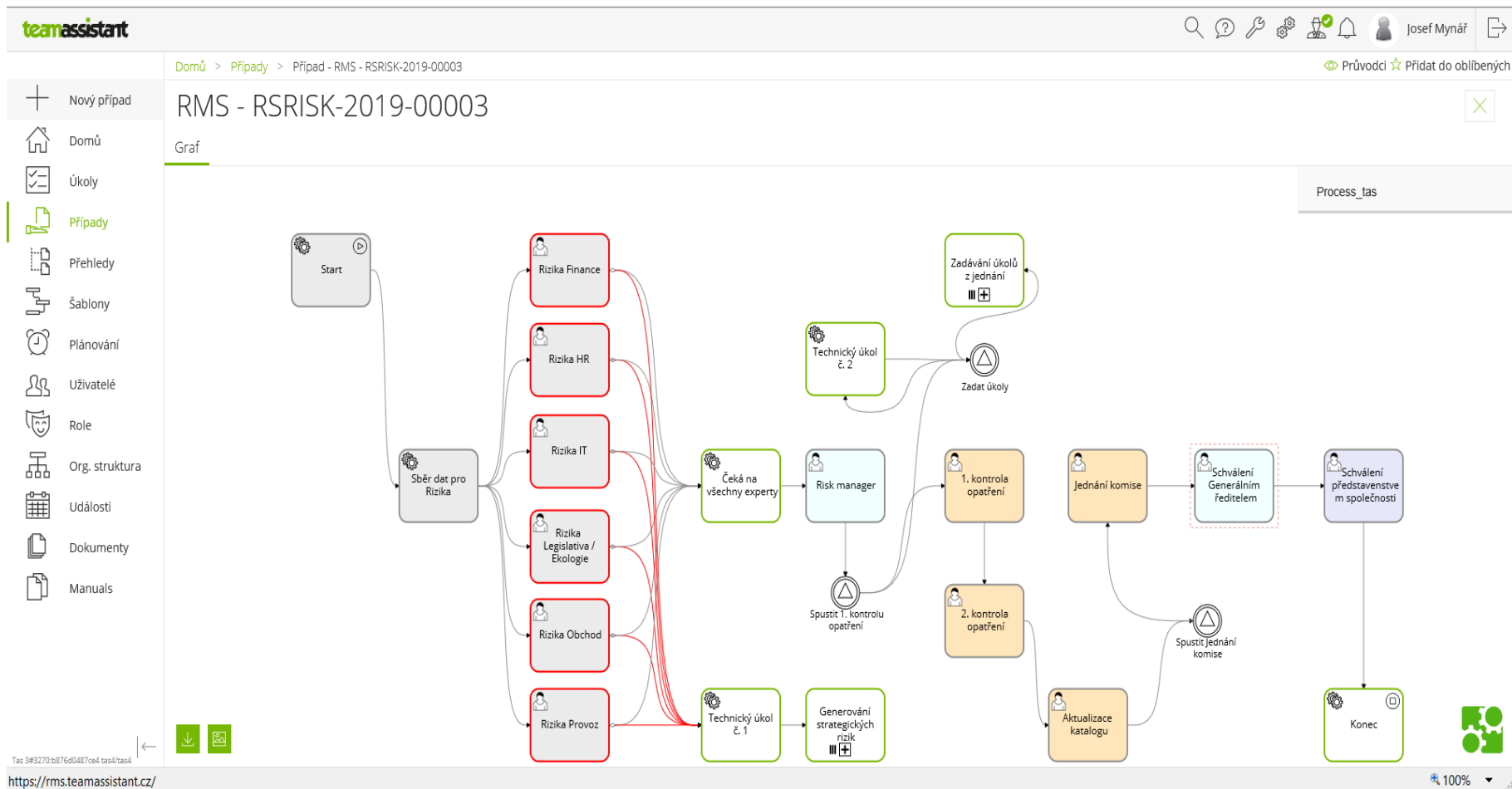
100%

Tas 3#3270:b876d0487ce4 tas4/tas4

RMT - Řízení strategických rizik

- Otevření rizika
 - Práce s rizikem a jeho hodnocení
 - Návrh mitigace rizika
 - Reporting
-

RMT - Řízení strategických rizik - graf práce s rizikem



RMT - Řízení strategických rizik – nové strategické riziko



teamassistant

+

Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Domů > Úkoly > Případ - RMS - SRISK-2019-00003 > Úkol - Identifikace rizika

Průvodci Přidat do oblíbených

Úkol Poznámky Dokumenty

✓ Splnit

✕

Přidat Jen uložit Případ Více

Název případu: RMS - SRISK-2019-00003 (Nové strategické riziko)

Supervizor úkolu: Mynář Josef

Vlastník případu:

ID Rizika

RMS - SRISK-2019-00003

Majitel rizika *

Expert rizika *

Osoba odpovědná za provádění opatření *

Číslo rizika

Název rizika *

Kategorie rizika *

✓

✓

✓

Četnost rizika *

Komentář k riziku

Existující opatření

Související incidenty

Tas 3#3270b876d0487ce4 tas4/tas4

100%

RMT - Řízení strategických rizik – Informace strategické riziko

teamassistant

Josef Mynář

Domů > Případy > Případ - RMS - SRISK-2019-00003

Průvodci Přidat do oblíbených

Událost

Report Graf Nadřazený Tisk

Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

RMS - SRISK-2019-00003

Případ Poznámky Dokumenty Aktuální úkoly Historie Proměnné

RMS

Informace o strategickém riziku

ID rizika:	RMS - SRISK-2019-00003	Majitel rizika:	Knápek Jiří
Číslo a název rizika:	ERP SAP	Četnost:	12
Kategorie:	IT	Komentář k riziku:	
Související incidenty:		Ocenění rizika v mil. Kč:	
Existující opatření:		Status:	Ke schválení RM

Přehled ohodnocení rizika

Dopad (Prodej tepla a el. energie) v mil. Kč:		Dopad (Finance a IT) v mil. Kč:	
Dopad (Nákup tepla a surovin) v mil. Kč:		Dopad (Ostatní (leg., HR)) v mil. Kč:	
Dopad (Výroba a ekologie) v mil. Kč:			

Postup zpracování rizika

Krok	Odpovědná osoba	Doplňující informace
Identifikace rizika	Mynář Josef	14.03.2019 16:07:31
Potvrzení zadání rizika RM	Admin Admin	Plánováno

Upozornění k riziku

Adresát	Datum odeslání upozornění	Text upozornění
K případu nebyla zadána žádná upozornění.		

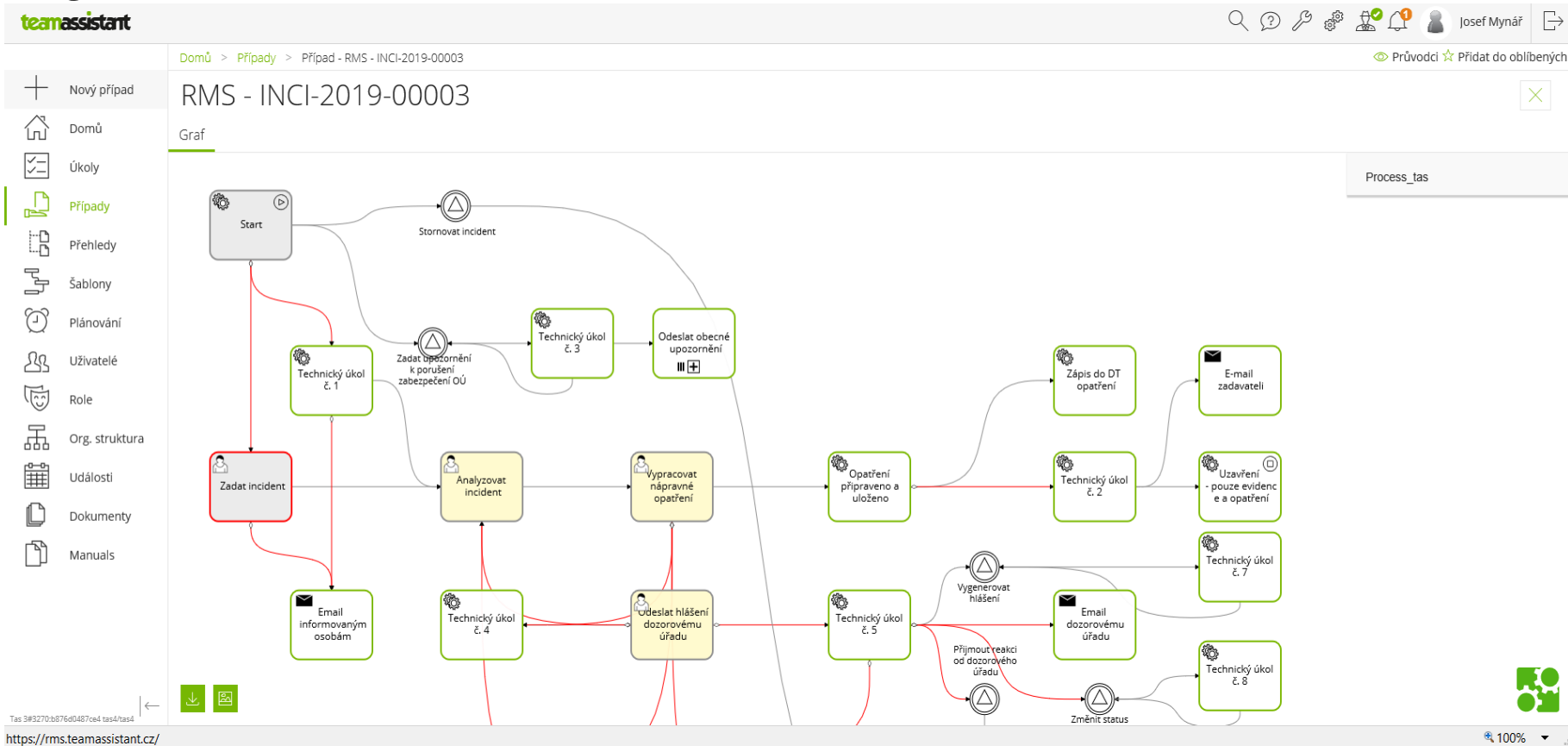
Tas 383270-b876d0487ce4-tas4/tas4

100%

RMT – Práce s incidenty (řízení a evidence incidentů)

- Nový incident
- Práce s incidenty
- Reporting

RMT – Práce s incidenty (řízení a evidence incidentů) – graf



RMT – Práce s incidenty – zadání incidentu

teamassistant

+

 Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Domů > Úkoly > Případ - RMS - INCI-2019-00003 > Úkol - Zadat incident

Průvodci

Přidat do oblíbených

✓ Splnit

✕

Přidat

Jen uložit

Případ

Více

Zadat incident

Úkol Poznámky Dokumenty

Název případu:

RMS - INCI-2019-00003 (Nový bezpečnostní incident)

Supervizor úkolu:

Vlastník případu:

Mynář Josef

Číslo hlášení incidentu

② RMS - INCI-2019-00003

Datum zadání incidentu

② 14.03.2019 16:13

Společnost zadavatele incidentu

② Risk Management System

Datum a čas zjištění incidentu *

②

Typ společnosti

② správce

Název incidentu *

②

Zadavatel incidentu

② Mynář Josef

Popis incidentu *

②

Tas 3f93270-b876d0487ce4-tas4/tas4

100%

RMT – PRÁCE S INCIDENTY (řízení a evidence incidentů)

teamassistant

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Domů > Případy > Případ - RMS - INCI-2019-00002 - Spam

Průvodci

Přidat do oblíbených

Událost

Report

Graf

Nadřazený

Tisk

RMS - INCI-2019-00002 - Spam

Případ

Poznámky

Dokumenty

Aktuální úkoly

Historie

Proměnné

Porušení zabezpečení osobních údajů

Číslo hlášení incidentu:	RMS - INCI-2019-00002	Typ společnosti:	správce
Název společnosti zadavatele porušení:	Risk Management System	Jméno odpovědné osoby:	Admin Admin
Jméno zadavatele:	Knápek Jiří	Kont. údaje odp. osoby:	Pražská 999, 110 00 Praha +420 000 000 000; kontakt@osoba.cz
Název incidentu:	Spam	Další kroky:	
Popis události:	přišel spam	Vazba na agendu:	
Související incident:		Odesílat hlášení DÚ:	
Priorita:		Odesílat hlášení SÚ:	
Aktuální stav řešení:		Status:	Otevřený

Další náležitosti porušení zabezpečení

Kategorie dotčených subjektů:	Počet dotčených subjektů údajů:
Kategorie dotčených záznamů OÚ:	Počet dotčených záznamů údajů:

Postup řešení porušení zabezpečení

Krok	Odpovědná osoba	Doplňující informace
Zadání incidentu	Knápek Jiří	06.02.2019 12:46 Zadáno
Analýza incidentu	Admin Admin	Plánováno

Nápravné opatření k porušení

K porušení nebylo zadáno žádné nápravné opatření.

Upozornění k porušení

I. Identifikace

Identifikační údaje společnosti:

Risk Management System (správce)

Pražská 999, 110 00 Praha

Oznámení porušení zabezpečení OÚ

Porušení zabezpečení č. RMS - INCI-2019-00002

Odpovědná osoba:

Admin Admin

Pražská 999, 110 00 Praha

+420 000 000 000

kontakt@osoba.cz

Datum a čas zjištění:

12.12.2019

Datum a čas zadání:

06.02.2019 12:46

II. Informace k porušení zabezpečení

Číslo incidentu:

Název:

Popis:

Číslo opatření:

Popis:

Status:

RMS - INCI-2019-00002

Spam

přišel spam

Otevřený

Rozpracováno

Odpovědná osoba:

Admin Admin

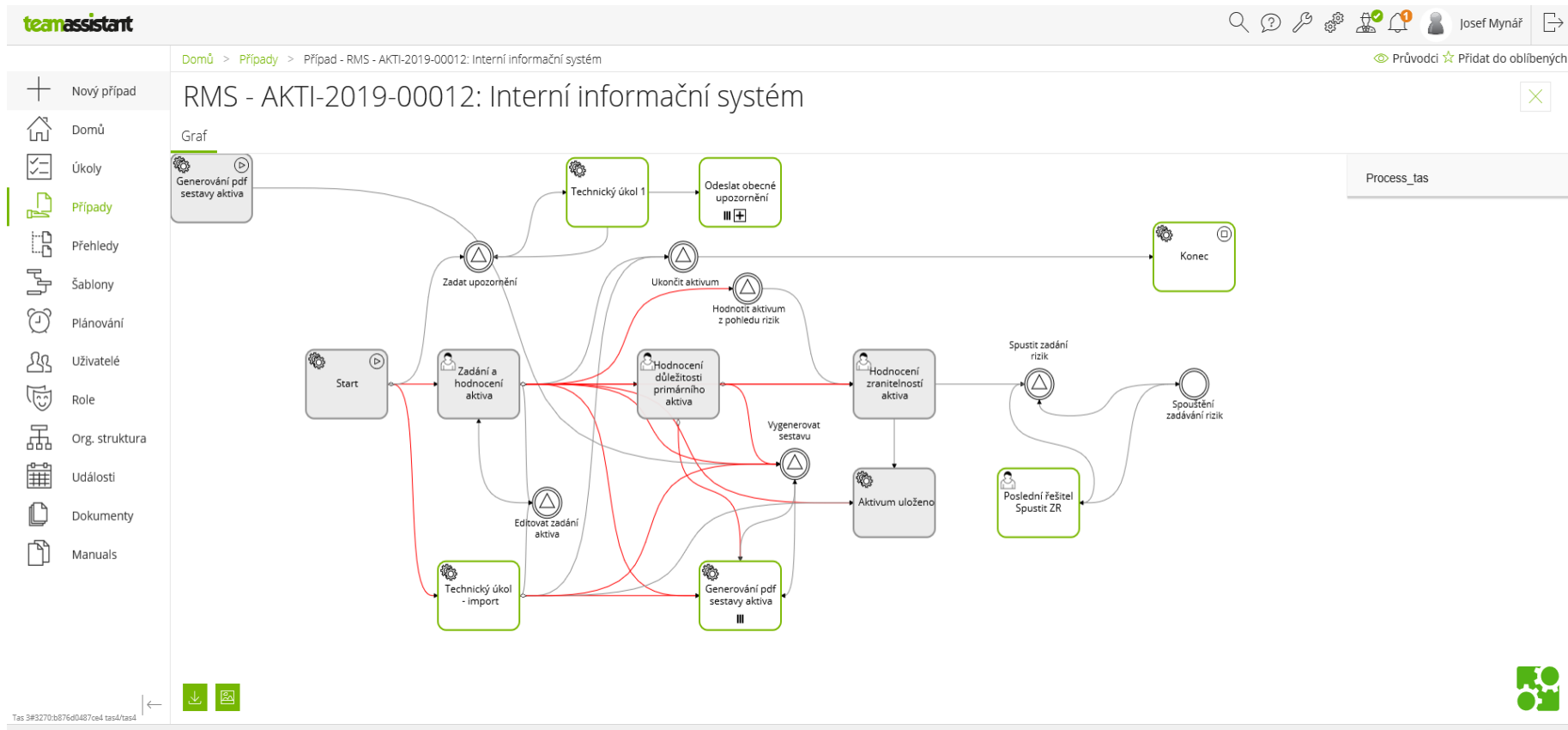
Tas 3#3270b876cd0d37ce4 tas4/tas4

100%

RMT - Řízení aktiv, práce s aktivy – primární, podpůrná

- Zadání aktiva
- Práce s aktivem, jeho hodnocení
- Reporting

RMT - Řízení aktiv, práce s aktivy – graf práce s aktivem



RMT - Řízení aktiv, práce s aktivy - Zadání aktiva

teamassistant

Josef Mynář

Domů > Úkoly > Případ - RMS - AKTI-2019-00016 > Úkol - Zadání a hodnocení aktiva

Průvodci Přidat do oblíbených

Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Zadání a hodnocení aktiva

Úkol Poznámky Dokumenty

Název případu: RMS - AKTI-2019-00016 (Nové primární aktivum)

Popište informační aktivum z pohledu zákona o kybernetické bezpečnosti.

ID aktiva RMS - AKTI-2019-00016

Typ aktiva Primární

Název aktiva *

Kategorie primárního aktiva *

Garant aktiva *

Správce IS

Provozovatel IS

Zpracovatel údajů

Základní popis

Supervizor úkolu:

Vlastník případu: Mynář Josef

Důvěrnost *

Dostupnost *

Integrita *

Hodnota aktiva

Hodnocení rizik *

?

?

?

0,0

Podpůrná aktiva

Relevantní podpůrná aktiva

	Index závislosti	Nejvyšší úroveň rizika	
1			

Přidat

Jen uložit

Případ

Více

Splnit

Tas 383270:b876d0487ce4:tas4/tas4

100%

RMT - Řízení aktiv, práce s aktivy - Práce s aktivem, jeho hodnocení









Josef Mynář


Domů > Úkoly > Případ - RMS - AKTI-2019-00016: aaa > Úkol - Hodnocení důležitosti primárního aktiva

 Průvodci
 Přidat do oblíbených

+

 Nový případ

 Domů

 **Úkoly**

 Případy

 Přehledy

 Šablony

 Plánování

 Uživatelé

 Role

 Org. struktura

 Události

 Dokumenty

 Manuals

Hodnocení důležitosti primárního aktiva

Úkol
Poznámky
Dokumenty

 Přidat
 Jen uložit
 Případ
 Více

✓

 Splnit

✕

Název případu:
RMS - AKTI-2019-00016: aaa (Nové primární aktivum)

Supervizor úkolu:

Vlastník případu:
Mynář Josef

Identifikujte alespoň jeden důvod k hodnocení důležitosti tohoto aktiva.

ID aktiva	RMS - AKTI-2019-00016	e) dopady na poskytování důležitých služeb		
Typ aktiva	 Primární	f) rozsah narušení běžných činností		
Název aktiva	 aaa	g) dopady na zachování dobrého jména		
Kategorie primárního aktiva	Informační	h) dopady na bezpečnost a zdraví osob		
a) rozsah a důležitost osobních údajů		i) dopady na mezinárodní vztahy		
b) rozsah dotčených právních povinností		j) dopady na uživatele informačního systému		
c) rozsah narušení vnitřních řídicích a kontrolních činností		Komentář k hodnocení aktiv		
d) poškození veřejných, obchodních nebo ekonomických zájmů				

Tas 3f83270b876d0487ce47tas4/tas4

 100%

Tac 3#3270-b876d0487ce4 tac4/tac4

RMT - Řízení kybernetických rizik – ZÁKLADNÍ AKTIVITY

- Identifikace a otevření rizika
- Práce s rizikem a jeho hodnocení
- Návrh mitigace rizika
- Transfer rizika na třetí subjekt
- Reporting

RMT Řízení kybernetických rizik – GRAF PRÁCE S RIZIKEM

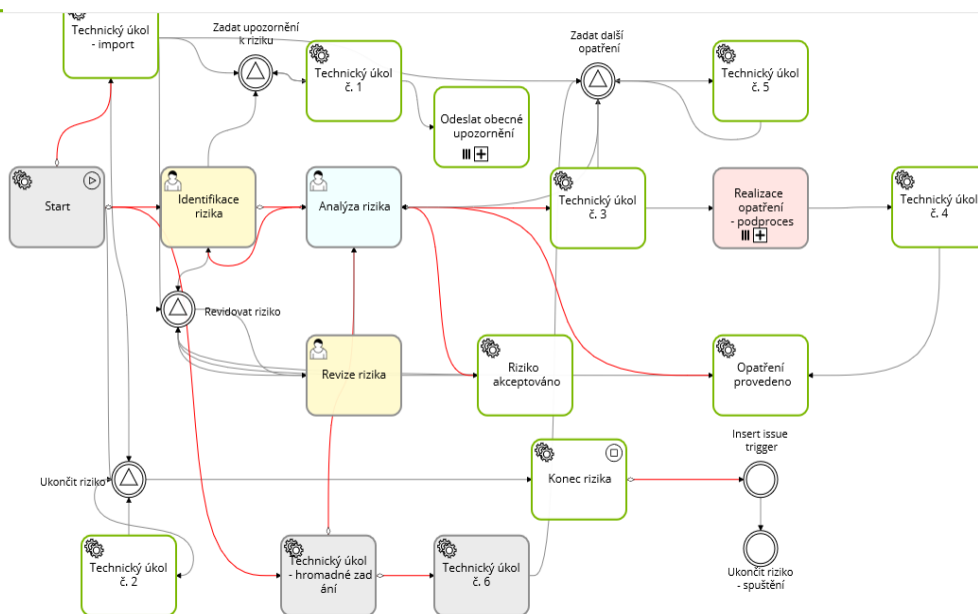
teamassistant

Průvodci Přidat do oblíbených

Domů > Případy > Případ - RMS - KRISK-2018-00007 - Server SAP - b) poškození nebo selhání tech

RMS - KRISK-2018-00007 - Server SAP - b) poškození nebo selhání tech

Graf



Process_tas

Tas 5f832703b876d0487ce4tas4/tas4

<https://rms.teamassistant.cz/>

100%

RMT Řízení kybernetických rizik – Identifikace a otevření rizika

teamassistant

Josef Mynář

Domů > Úkoly > Případ - RMS - KRISK-2019-00005 > Úkol - Identifikace rizika

Průvodci Přidat do oblíbených

Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Identifikace rizika

Úkol Poznámky Dokumenty

Název případu: RMS - KRISK-2019-00005 (Nové kyber riziko primárního aktiva)

Supervizor úkolu: Mynář Josef

Identifikujte riziko v souvislosti s informačními aktivy a možnými hrozbami.

Vlastník případu: Mynář Josef

Číslo hlášeného rizika RMS - KRISK-2019-00005

Úroveň rizika 0,0

Zadavatel Mynář Josef

Zranitelnost *

Typ aktiva Primární

Hrozba *

Aktivum *

Dopad *

Vlastník rizika *

Info - hardware

Datum zadání * 14.3.2019

Info - procesy

Popis rizika *

Info - software

Typ hrozby

Typ zranitelnosti

Tas 3#93270:b876d0487ce4 tas4/tas4

100%

RMT Řízení kybernetických rizik – Práce s rizikem a jeho hodnocení



Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

Domů > Úkoly > Případ - RMS - KRISK-2019-00005 - Soustava zásobování tepelnou energií CZTP > Úkol - Analýza rizika (Soustava zásobování tepelnou energií CZTP)

Průvodci ✪ Přidat do oblíbených

Splnit

X

Přidat

Jen uložit

Případ

Více

Analýza rizika (Soustava zásobování tepelnou energií CZTP)

Úkol Poznámky Dokumenty

Název případu:

RMS - KRISK-2019-00005 - Soustava zásobování tepelnou energií CZTP (Nové kyber riziko primárního aktiva)

Supervizor úkolu:

Vlastník případu:

Mynář Josef

Zhodnotte úplnost a správnost zadání. Zhodnotte potřebnost a proporcionalitu. Navrhněte opatření.

Číslo hlášeného rizika

RMS - KRISK-2019-00005

Úroveň rizika

6,0

Vlastník rizika *

IT manažer

Zranitelnost *

1 - Nizká

Název rizika

Soustava zásobování tepelnou energií CZTP

Hrozba *

3 - Vysoká

Typ aktiva

Primární

Dopad *

2,0

Aktivum *

Soustava zásobování tepelnou energií CZTP

Strategie řešení rizika *

Akceptace rizika

Popis rizika *

riziko sabotáže

Dopad - bez reakce

Tas 3f83270:b876d0487ce4:tas4/tas4

100%

RMT Řízení kybernetických rizik – karta rizika a návrh mitigace rizika

teamassistant

Josef Mynář

Domů > Případy > Případ - RMS - KRISK-2018-00005 - Server SAP - a) porušení bezpečnostní polit

Průvodci ☆ Přidat do oblíbených

+

Nový případ

Domů

Úkoly

Případy

Přehledy

Šablony

Plánování

Uživatelé

Role

Org. struktura

Události

Dokumenty

Manuals

RMS - KRISK-2018-00005 - Server SAP - a) porušení bezpečnostní polit

Událost

ReportGrafNadřazenýTisk

Risk management - hlášení výskytu rizika

Číslo hlášeného rizika:	RMS - KRISK-2018-00005	Název rizika:	Server SAP - a) porušení bezpečnostní polit
Zadavatel rizika:	Admin Admin	Vlastník rizika:	Hrubý
Kontaktní údaje zadavatele:		Typ aktiva:	
Popis rizika:		Aktivum:	{Aktivum}
Poslední aktualizace:		Poslední aktualizace:	22.11.2018
Další informace k riziku:		Status:	

Kvalifikace rizika

Úroveň rizika:	2.4
Dopad:	2.4
Zranitelnost:	1 - Nizká
Hrozba:	1 - Nizká

Postup řešení identifikovaného rizika

Krok	Odpovědná osoba	Doplňující informace
Identifikace rizika	Admin Admin	22.11.2018 12:00:09 Zadáno
Analýza a schválení rizika	Admin Admin	22.11.2018 12:00:09 Schváleno

Jednotlivá navržená opatření

Číslo realizovaného opatření	Datum přidělení rizika	Datum uzavření	Nová zranitelnost	Nová hrozba	Nová hodnota aktiva	Nová úroveň rizika	Status
------------------------------	------------------------	----------------	-------------------	-------------	---------------------	--------------------	--------

Přehled realizovaných opatření

K riziku nebylo dosud realizováno žádné opatření.

Tas 3#93270:b876d0487ce4:tas4/tas4

100%

Tag 3#2991:646ad900e938 default/default

Řízení rizik - REGISTR RIZIK

POUŽITÍ V PRAXI	POČET SPOL.	POČET PŘÍPADŮ*
Pojišťovna VZP	1	Pilotní provoz
ČSOB pojišťovna	1	V projektu



PERIODICKÉ PŘEZKOUMÁNÍ RIZIKA VLASTNÍKY

Automaticky se spouští úkoly pro vlastníky rizika jednou za definovanou periodu.

SOUHRN RIZIK PRO RISK MANAŽERA

NÁVRHY NA MITIGAČNÍ OPATŘENÍ

Risk manager může zaslat jakémukoliv vlastníkovu rizika návrh na mitigační opatření v reakci na aktuální stav rizika.

BAREVNÉ OZNAČENÍ RIZIK PODLE PRAVDĚPODOBNOSTI A DOPADU

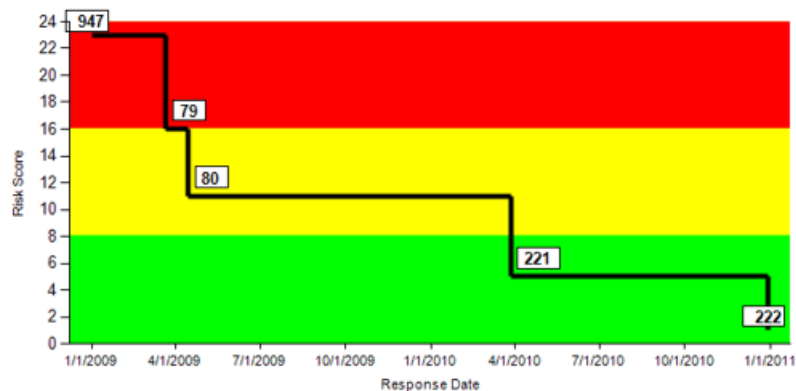
ZOBRAZENÍ VÝVOJE RIZIKA V ČASE

	OČEKÁVANÉ	ZVÝŠENÉ	KRITICKÉ
1300	0	0	1
1500	1	0	1
2003	0	0	0
2003 mandatory_courses_fulfillment_level Labor safety - Employees	0	0	0
2003 mandatory_courses_fulfillment_level Hire protection - Employees	0	0	0
2003 mandatory_courses_fulfillment_level AMI - Employees	0	0	0
2003 mandatory_courses_fulfillment_level Ethics - Employees	0	0	0
2003 mandatory_courses_fulfillment_level Data privacy - Employees	0	0	0
2003 mandatory_courses_fulfillment_level Info security - Employees	0	0	0
2003 mandatory_courses_fulfillment_level Anti-trust - Employees	0	0	0
2003 mandatory_courses_fulfillment_level AML - Tied Agents	0	0	0
2003 mandatory_courses_fulfillment_level Ethics - Tied agents	0	0	0
2003 mandatory_courses_fulfillment_level Data privacy - Tied agents	0	0	0
2003 mandatory_courses_fulfillment_level Info security - Tied agents	0	0	0
2020			1

Process Human resources - 1500		KRI detail		KRI value *	Risk Owner Comment
RISK					
1	HR_back_up Key employees leave the company.	Level of back up		70	
2	HR_turn_over Key employees leave the company.	Turnover number		1	
3	HR_salary Key employees leave the company.	Salary level 0-75%		13	
4	HR_salary Key employees leave the company.	Salary level 76-90%		13	
5	HR_salary Key employees leave the company.	Salary level 91-100%		75	

REPORTING – průběh rizika

Risk PUID	779
Risk Status	Active
Risk Name	Protected species inhabiting site or in immediate vicinity of building site.
Description	The presence of bats in particular on the project site has been a cause of significant cost and delay in the past. The risk of this to the project therefore needs to be assessed and provision made if this is a relevant exposure.
Percent Prob	High
Owner	Tim Davies
Time Impact	Very Low
Cost Impact	Low
Performance Impact	
Current Score	10



D	Response Name	Due Date	Score	Driver	Probability	Min	Expected	Max	Status
947	Environmental review of all project proposal is conducted by central HS&E team	01 Jan 09	23	Time	90%	£2M	£4M	£6M	Approved
79	Cursory site inspection	22 Mar 09	16	Cost	80%	£1.5M	£2M	£3.5M	Complete
80	Specialist environmental study	15 Apr 09	11	Cost	75%	£1M	1.5M	2M	Complete
221	Agree terms with environmental contractors	28 Mar 10	5	Time	50%	£1M	£1.5M	£2M	Complete
222	Contractors reinhabit protected species	30 Dec 10	1	Performance	50%	£750k	£1m	£1.5M	Complete

Praktická ukázka

závěr prezentace

OTÁZKY/ODPOVĚDI

Děkujeme za vaši pozornost

Jiří Knápek
manažer realizace

NETIA® s.r.o.,
Hliníky 259, 679 72 Kunštát
ICO: 25588869
DICO: CZ25588869
mob: +420 730 827 844
mail: knapek@netia-it.cz
www.netia.cz