

Managing risks with ZOTY Risk management software

Zdeněk Kocourek
October 17, 2018



Agenda

1. IDS Advisory Introduction
2. Introduction to ZOTY Risk
3. ZOTY concept - about the approach
4. Managing risks with ZOTY
5. Questions & Answers

1 IDS Advisory

Introduction



IDS Advisory - Who we are?



The company implementing
BPM and Risk Management with
ARIS & ZOTY software support



IDS Scheer

The company where ARIS
was born in the 1990s



While IDSA team keeps long-term continuity in
providing of ARIS support we belongs to the top
centers of ARIS Excellence in the whole EMEA region



Recently we're launching a brand new software
ZOTY - best of breed GRC solution connecting
risks and processes in ARIS

2 ZOTY Risk

Introduction



ZOTY - Risk management environment

Zoty **Kalendář** **Schválení**

Přehled

- Úkoly
- Incidenty
- RISK
- Požadavky
- Cíle
- Aktiva
- Hrozby a zranitelnosti
- Rizika
- Hodnocení
- Skupiny
- Opatření
- Audit
- Uživatelé
- Koš
- Nastavení

ZOTY is Risk & Compliance Management software

Support of many standards (ISO 27001, ISO 31000, ETL, Stride, Linddun...)

Offer of dedicated modules for key topics: Risk, Compliance, Audit, Incident management ...

Configurable method by users (no customization needed)

Open API for 3rd parties system integration

Fully logged user activities, No backward actions allowed (Traceable, Transparent & Auditable)

ZOTY Environment will encompass Risk & Compliance, BPM and other topics in one source of truth

Czech software with Czech/Slovak full support

ZOTY Risk management environment

ZOTY is not empty piece of software!

ZOTY offers both basic and sophisticated Evaluation Methods

ZOTY Contains valuable know-how: Threats, Vulnerabilities, Risk Catalogs, Law requirements...

STAV	TYP	METRIKY	METODY
Vytvořeno	evaluationA	3 / 0 / 0	Kyber zákon
Publikováno	evaluationR	2 / 0 / 0	ISO 27001
Publikováno	evaluationR	2 / 0 / 0	ISO 31000
Publikováno	evaluationA	3 / 0 / 0	ISO 27001
Publikováno	evaluationA	3 / 0 / 0	ISO 31000
Publikováno	evaluationA	15 / 0 / 0	Tatra banka
Publikováno	evaluationR	3 / 0 / 0	Kyber zákon
Publikováno	evaluationR	0 / 0 / 3	Tatra banka
Publikováno	evaluationR	5 / 0 / 1	Tatra banka
Publikováno	evaluationV	2 / 0 / 0	Tatra banka
Publikováno	evaluationT	2 / 0 / 0	Tatra banka
Publikováno	evaluationR	3 / 0 / 0	ISO 27001

Evaluation Methods (Schemes) could be fast adapted, derived or the new one introduced

ZOTY Risk management tool

Technical Capabilities & Architecture

Web-based solution

Build-in Social collaboration

Open API for 3rd parties System Integration

Scalable to fit both your current and future requirements

The screenshot displays the ZOTY Risk management tool dashboard. The top navigation bar includes links for 'ZOTY', 'Kalendář', 'Schválení', and a search icon. The user 'Zdeněk Kocourek' is logged in. The left sidebar contains a menu with 'Přehled', 'Úkoly', 'Incidenty', 'RISK', 'Uživatelé', 'Koš', and 'Nastavení'. The main content area shows a 'Přehled' (Overview) section with four summary cards: 'Aktiva 3 / 60', 'Rizika 119', 'Opatření 14', and 'Cíle 0'. Below these is a table for 'Zdeněk Kocourek' with columns for 'NÁZEV', 'KLÍČ', 'DŮLEŽITOST', 'SPRÁVCE', 'STAV', 'DOKONČIT DO', 'ČASOVÝ PRŮBĚH', and 'VYTVOŘENO'. The table lists two tasks: 'Test úkolů a riziky 2' (TASK12, Archivováno, 28. září 2018) and 'Úkol' (TASK14, Přřazeno, 15. listopad 2018). Below this is a 'Nejnovější záznamy' (Latest records) section with a similar table listing records like 'Hodnocení aktiv v rámci provozu a údržby budov (dle ISO 27001)' (E364, RiskOwner Oliver, Přřazeno, 27. září 2018) and 'Riziko test' (R127, Humpolíček Petr, Přřazeno, 11. říjen 2018).

Implementation scenarios

ZOTY on-premise

ZOTY cloud



Accessible by common Web-browsers

ZOTY Risk is ready to use

- The first releases have been launched
- Proven by first customers
- Robust solution ready for wide range of customers & industries
- Support and updates are available



Mendelova
univerzita
v Brně



3

ZOTY Concept

About the
approach



Risk management

Risk identification - Supported starting points

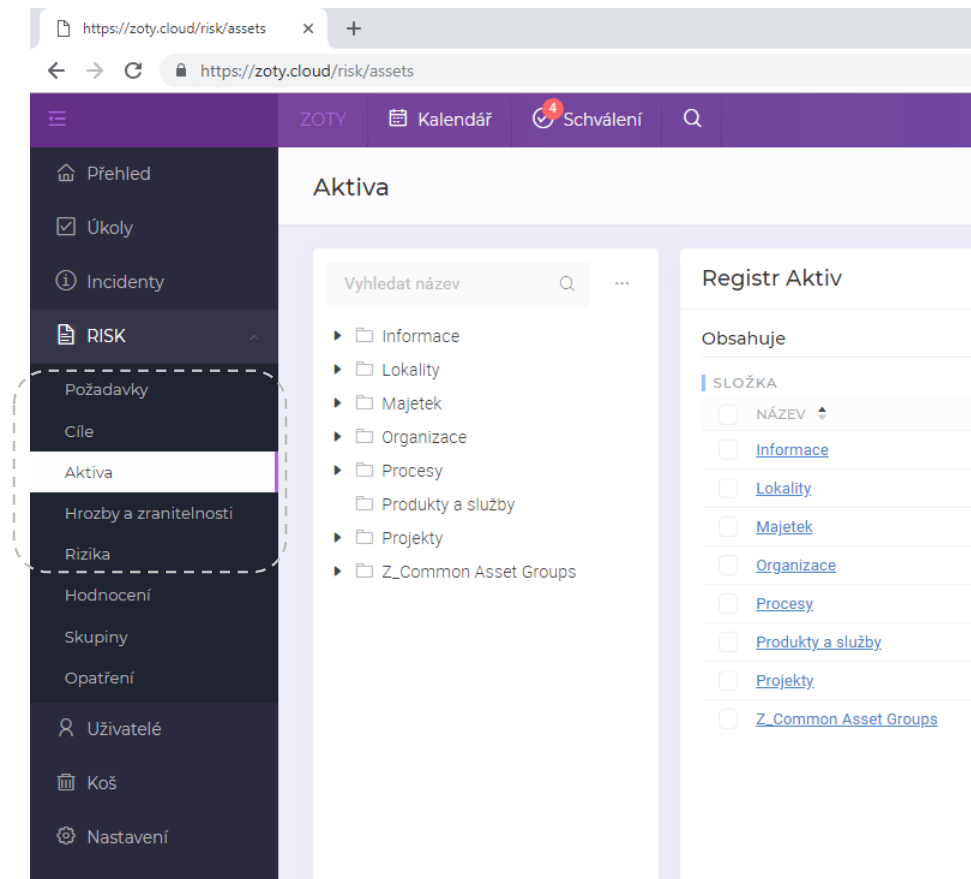
Requirements
(legal, agreements, norms)

Objectives
(Enterprise / project)

Assets

Threats & Vulnerabilities

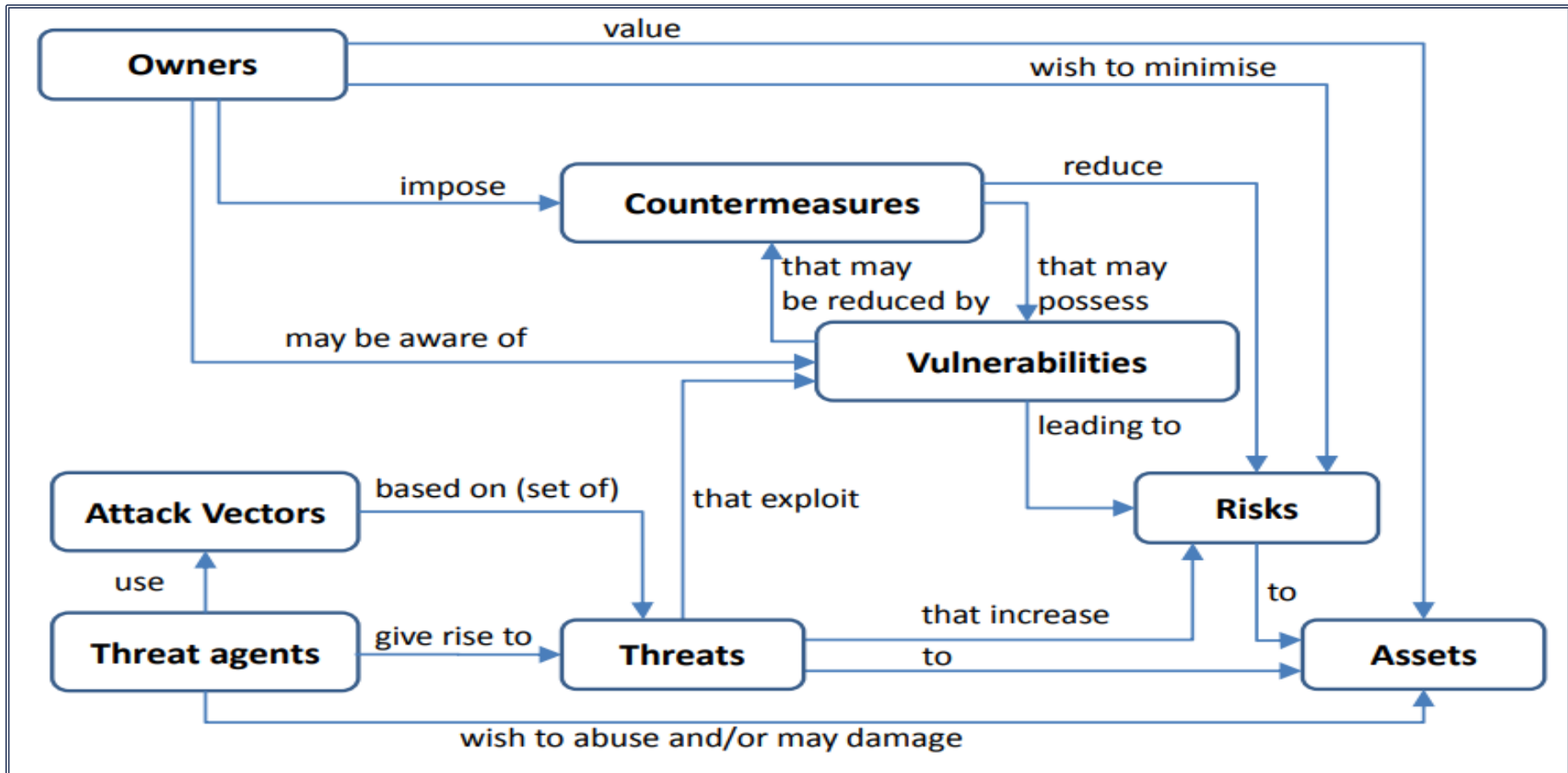
Empirical based approach
(from practice)



What is ZOTY Method?

- Method is a logical container for ZOTY artifacts (Asset types, Threat types, Risk types...) that requires the same logic / applied approach
 - The corresponding attributes
 - Way of measuring (relevant risk metrics)
 - Connection types among artifacts
 - & evaluation logic (e.g. $A \rightarrow V \rightarrow T \rightarrow \text{Risk}$; $A \rightarrow \text{Risk scenario}$...)
- It let you see the relevant artifacts and bind it together
- Enable you to filter data and to reduce the complexity of tool 😊

Example of sophisticated Method (One of many)



Risk management

The same data vs a lot of points of views

The screenshot displays the IDS A Risk Management interface. The left sidebar shows a navigation menu with various sections, including 'Aktiva' which is currently selected. The main content area is titled 'Aktiva' and contains a search bar and a list of asset categories. The 'Registr Aktiv' option is highlighted in yellow. On the right, the 'Registr Aktiv' section shows a list of assets under the heading 'Obsahuje' and 'SLOŽKA'.

Create your own catalogues
and assign related artifacts.

The objects will be re-used
from the Register in place of
creating new definitions =
redundancies!

4

Managing risks with ZOTY in details

What's inside?



Entry points Artifacts Management

Aktiva

Vyhledat název

- Informace
- Lokality
- Majetek
- Organizace
 - Externí subjekty
 - Organizační struktura
- Procesy
 - Hlavní procesy
 - Podpůrné procesy
 - Řídicí procesy
- Produkty a služby
- Projekty

Registr Aktiv

Obsahuje

SLOŽKA

NÁZEV		
Informace	FOLDER121	...
Lokality	FOLDER124	...
Majetek	FOLDER122	...
Organizace	FOLDER140	...
Procesy		
Produkty a služby		
Projekty		
Z_Common Asset Groups		

The Register of assets contains the structured list of artifact types (e.g. Processes, Information, Locations, Properties, Persons, Departments etc.)

Methods and its Attributes are related to the artifact types

The **content** could be imported or **synchronized** from external data source

Risk evaluation related to the Method being used

The screenshot displays the ZOTY risk evaluation interface. The top navigation bar includes links for ZOTY, Kalendář, Schválení (with a red notification badge), a search icon, and the user name Zdeněk Kocourek. The left sidebar contains a menu with options: Přehled, Úkoly, Incidenty, RISK (expanded), Požadavky, Cíle, Aktiva, Hrozby a zranitelnosti, Rizika, Hodnocení (selected), Skupiny, and Opatření. The main content area is titled 'Hodnocení / Hodnocení rizika v rámci provozu a údržby bud...' and features a green 'Vytvořit hodnocení' button. Below this, a sub-header 'Hodnocení' has an 'Ohodnotit' button. The main section is titled 'Hodnocení rizik dle ISO 27001 (základní 3 parametry)'. It shows a table with columns: NÁZEV, STAV, SKÓRE, and a date column. A row is highlighted with a dashed box around the 'Cíl' status and a score of 3 - Střední. A callout box explains: 'Target state represents the Objectives in numbers (Planned values)'. Below this, a 'HISTORIE' section shows a table of past evaluations with columns: NÁZEV, STAV, SKÓRE, OPATŘENÍ, PLATNOST OD, and PLATNOS. A row is highlighted with a dashed box around the 'Skutečnost' status and a score of 11 - Vysoké. A callout box explains: 'Current state represents the real collected values'.

Target state represents the Objectives in numbers (Planned values)

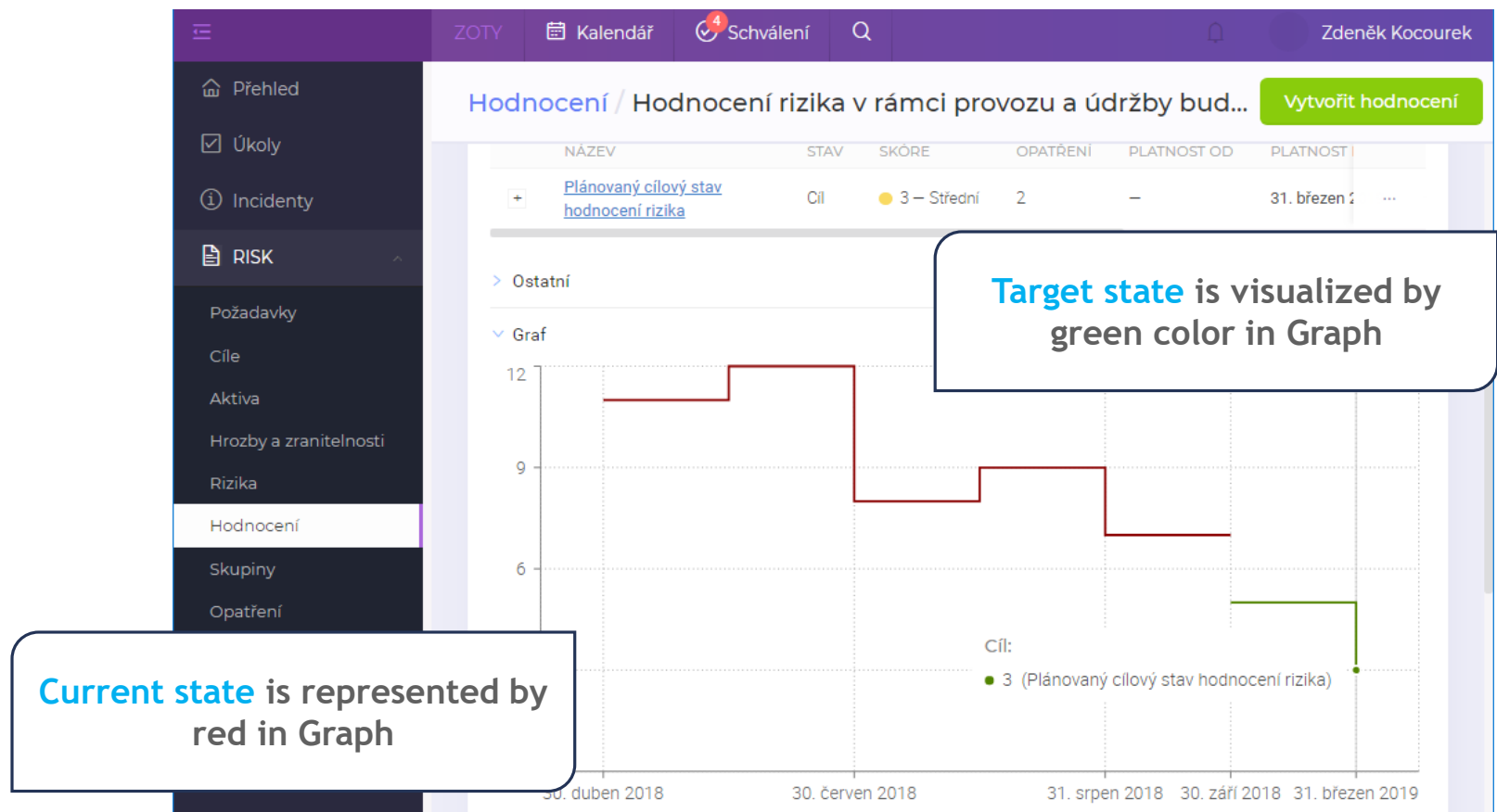
NÁZEV	STAV	SKÓRE	OPATŘENÍ	PLATNOST OD	PLATNOS
Plánovaný cílový stav hodnocení rizika	Cíl	3 – Střední	2	–	31. března 2018

Current state represents the real collected values

NÁZEV	STAV	SKÓRE	OPATŘENÍ	PLATNOST OD	PLATNOS
Hodnocení rizika - Q2	Skutečnost	11 – Vysoké		1. duben 2018	30. duben 2018
	Skutečnost	12 – Vysoké		1. květen 2018	31. květen 2018
	Skutečnost	8 – Vysoké		1. červen 2018	30. červen 2018
	Skutečnost	9 – Vysoké		1. červenec 2018	31. červenec 2018
	Skutečnost	7 – Vysoké		1. srpen 2018	31. srpen 2018

Risk evaluation related to the Method being used

- The progress of Risk shall be monitored and targeted



Risk control is about relevant Risk mitigation

Mitigation plan is set of the Processes, Tasks & Projects arranged as a real Plan (Work Breakdown Structure)

Projects & Process are stored in Asset and could be synchronized / imported

- Přehled
- Úkoly
- Incidenty
- RISK**
- Požadavky
- Cíle
- Aktiva
- Hrozby a zranitelnosti
- Rizika
- Hodnocení
- Skupiny

Hodnocení / Hodnocení rizika v rámci

Přehled Aktivita Propojení Hodnocení Opatření

Opatření

Vytvořit opatření

Hodnocení rizik dle ISO 27001 (základní 3 parametry)

PLÁNOVANÝ CÍLOVÝ STAV HODNOCENÍ RIZIKA, 16. ZÁŘÍ 2018 - 31. BŘEZEN 2019

NÁZEV	VYTVOŘIL	STAV	TYP	PŘEDCHŮDCE	V
Předat k posouzení Risk boardem	RiskOwner Oliver	Schváleno	Úkol	—	1 ...

ČEKÁ NA SCHVÁLENÍ

NÁZEV	VYTVOŘIL	STAV	TYP	PŘEDCHŮDCE
Provoz a údržba budov	RiskOwner Oliver			

All Initiatives are stored in ZOTY repository (one definition) and **re-used** here

Managers wants to see the **Risk value & Mitigation Costs** in one placed (needs to compare)!

Nastavení

Komentáře

Task management

Tasks are created due to further risk management needs (e.g. Audits, Incident management issues, or ZOTY workflow tasks)

The screenshot displays the ZOTY task management interface. The top navigation bar includes 'ZOTY', 'Kalendář', 'Schválení', and a search icon. The left sidebar shows a menu with 'Přehled', 'Úkoly' (selected), 'Incidenty', 'RISK', 'Požadavky', 'Cíle', 'Aktiva', 'Hrozby a zranitelnosti', 'Rizika', 'Hodnocení', 'Skupiny', 'Opatření', 'Uživatelé', 'Koš', and 'Nastavení'. The main content area is titled 'Úkoly' and shows 'Celkem: 9' tasks. A table lists the tasks with the following columns: NÁZEV, KLÍČ, DŮLEŽITOST, SPRÁVCE, STAV, DOKONČIT DO, ČASOVÝ PRŮBĚH, UPRAVENO, and VYTVOŘENO. The tasks are as follows:

NÁZEV	KLÍČ	DŮLEŽITOST	SPRÁVCE	STAV	DOKONČIT DO	ČASOVÝ PRŮBĚH	UPRAVENO	VYTVOŘENO
Definovat metodiku řízení rizik v TB > 2018	TASK1	●●	RiskManager Martina	Přirazeno	31. srpen 2018	<div></div>	11. říjen 2018	28. srpen 2018
Identifikovat Informační aktiva	TASK5	●●●	ProcessOwner Patrik	Dokončeno	30. září 2018	<div></div>	15. září 2018	6. září 2018
Poslat k review OPRIC	TASK4	●●	Auditor Adam	Dokončeno	1. říjen 2018	<div></div>	15. září 2018	3. září 2018
Předat k posouzení Risk boardem	TASK9	●●●	RiskManager Martina	Přirazeno	16. září 2018	<div></div>	16. září 2018	12. září 2018
Revidovat metodický pokyn pro nakládání s citlivými osobními údaji s ohledem na identifikovaná rizika	TASK7	●●●●	RiskManager Martina	Probíhá	30. listopad 2018	<div></div>	10. září 2018	6. září 2018
Review to OPRIC	TASK6	●●	Auditor Adam	Dokončeno	10. září 2018	<div></div>	15. září 2018	6. září 2018
UAT systému ZOTY - Testovací prostředí v TB	TASK2	●●●	ProcessOwner Patrik	Přirazeno	28. září 2018	<div></div>	16. září 2018	28. srpen 2018
Úkol	TASK14	●●●	Kocourek Zdeněk	Přirazeno	15. listopad 2018	<div></div>	15. říjen 2018	15. říjen 2018
Úkol Zoty+	TASK13	●●●	Humpolíček Petr	Probíhá	31. říjen 2018	<div></div>	15. říjen 2018	15. říjen 2018

Tasks are related to the **mitigation plan** (WBS activities)

Calendar view - presents task in time manner / schedule form. Accessible form Calendar icon in top bar/menu.

Incident management

Incidents are whatever issues that organization are facing. Only risks or BPM related risks shall be managed here.

ZOTY | Kalendář | Schválení | Q

Zdeněk Kocourek

Vytvořit incident

Incidenty

Celkem: 2

<input type="checkbox"/> NÁZEV	DŮLEŽITOST	STAV	SPRÁVCE	VTVOŘENO
<input type="checkbox"/> Podvodný e-mail vymáhající pohledávku se zavírovanou .zip přílohou	●●●	Vytvořeno	RiskOwner Oliver	9. září 2018
<input type="checkbox"/> Výpadek datového připojení (WAN)	●●●	Vytvořeno	RiskOwner Oliver	28. srpen 2018

Incidents could be synchronized on the request for the specific incident management system.

Incidents - can arise from Audits - Audit findings subtype is used in this case. The new Task or Risk shall be interconnected.

Audit trail in practice

Rizika / Narušení střeženého objektu

Přehled Aktivity

Aktivita

27. ZÁŘÍ 2018

- Narušení střeženého objektu: Entita byla upravena uživatelem Humpolíček Petr. 9:43
- Narušení střeženého objektu: Entita byla upravena uživatelem Humpolíček Petr. 9:34
- Narušení střeženého objektu: Entita byla upravena uživatelem Humpolíček Petr. 9:34
- Související entity
- Bylo vytvořeno propojení "Rodič → Potomek" mezi Narušení střeženého objektu a Budova 1 v sektoru A. 9:31
- Bylo vytvořeno propojení "Vztah" mezi Narušení střeženého objektu a Budova 2 v sektoru A. 9:30
- Bylo odebráno propojení "Rodič → Potomek" mezi Budova 2 v sektoru A a Narušení střeženého objektu. 9:30

	Aktivum	23. září 2018 21:19	...
<input type="checkbox"/> T13.Unintentional damage / loss of information or IT assets.Damage caused by a third party due to the Lack of monitoring mechanisms for asset A1	Riziko	19. září 2018 16:04	...
<input type="checkbox"/> T61.Nefarious Activity/ Abuse.Brute force due to the Lack of audit trail Abuse of rights for asset A1	Riziko	19. září 2018 16:04	...
<input type="checkbox"/> T56.Nefarious Activity/ Abuse.Compromising confidential information (data breaches) due to the Lack of monitoring mechanisms for asset A1	Riziko	19. září 2018 16:04	...
<input type="checkbox"/> T66.Legal.Abuse of personal data due to the Lack of monitoring mechanisms for asset A1	Riziko	19. září 2018 16:04	...
<input type="checkbox"/> T61.Nefarious Activity/ Abuse.Brute force due to the Lack of monitoring mechanisms for asset A1	Riziko	19. září 2018 16:04	...
<input type="checkbox"/> T08.Unintentional damage / loss of information or IT assets.Accidental leaks due to the Lack of monitoring mechanisms for asset A1	Riziko	19. září 2018 16:04	...
	Složka	20. září 2018 18:03	...
	Složka	20. září 2018 18:03	...
	Složka	19. září 2018 15:46	...

Log of Activities is available for further activity's monitoring. ZOTY logs any activity...

Trash bin for undo actions helps not to loose your work.

ZOTY

Kalendář

Koš

Celkem: 366

NÁZEV

Budova 13 v sektoru B

Proces řízení interního auditu

T13.Unintentional damage / loss of information or IT assets.Damage caused by a third party due to the Lack of monitoring mechanisms for asset A1

T61.Nefarious Activity/ Abuse.Brute force due to the Lack of audit trail Abuse of rights for asset A1

T56.Nefarious Activity/ Abuse.Compromising confidential information (data breaches) due to the Lack of monitoring mechanisms for asset A1

T66.Legal.Abuse of personal data due to the Lack of monitoring mechanisms for asset A1

T61.Nefarious Activity/ Abuse.Brute force due to the Lack of monitoring mechanisms for asset A1

T08.Unintentional damage / loss of information or IT assets.Accidental leaks due to the Lack of monitoring mechanisms for asset A1

Koš

Nast

Role-based approach and User management

User Roles - ZOTY is based on Roles & the multi-user access (workgroup approach). Each user or user group has assigned dedicated roles in ZOTY environment

The screenshot displays the ZOTY user management interface. The top navigation bar includes 'ZOTY', 'Kalendář', 'Schválení', and a search icon. The left sidebar contains navigation links: 'Přehled', 'Úkoly', 'Incidenty', 'RISK', 'Požadavky', 'Cíle', 'Aktiva', 'Hrozby a zranitelnosti', 'Rizika', 'Hodnocení', 'Skupiny', and 'Opatření'. The main content area is titled 'Uživatelé' and shows a list of users. A green button 'Vytvořit uživatele' is in the top right. A callout box explains that LDAP is supported for user authentication. Another callout box mentions that SSO (Single Sign On) is coming soon.

Uživatelé

Celkem: 10

ZOTY JMÉNO	PŘÍJMENÍ	JMÉNO	ROLE	EMAIL	TELEFON	ODDĚLENÍ
@zdenek.kocourek	Kocourek	Zdeněk	administrator, risk-manager, auditor	zdenek.kocourek@idsa.cz	+420724328498	IDSA Delivery
@petr.humpolicek	Humpolíček	Petr	administrator, risk-owner, user	petr.humpolicek@idsa.cz	606723105	
@vilem.umlauf	Umlauf	Vilém	auditor, risk-owner	vilem.umlauf@idsa.cz		
@riskmanager	RiskManager	Martina	risk-manager	riskmanager@idsa.cz		
@riskowner	RiskOwner	Oliver	risk-owner	riskowner@idsa.cz		
@auditor@idsa.cz	Auditor	Adam	auditor	auditor@idsa.cz		
@patrik.user	user	Patrik	user, risk-owner			
@jmeno.riskmanager	risk-manager	Jmeno	risk-manager			
@jonas.riskmanager	risk-manager	Jonáš	risk-manager			
@robert.riskmanager	risk-manager	Robert	risk-manager			

LDAP is supported. The user accounts are overtaken from AD/LDAP servers. Users use their domain login credentials

SSO (Single Sign On) - automatic seamless login coming soon with next releases.

5

Questions & Answers

Any open questions?



Thank you!

IDS Advisory team



www.zoty.software | www.idsa.eu | www.idsa.cz