

CONCEPTICA



itop.

iAktiva

Řízení IT aktiv a dodavatelů v kontextu
kybernetické bezpečnosti



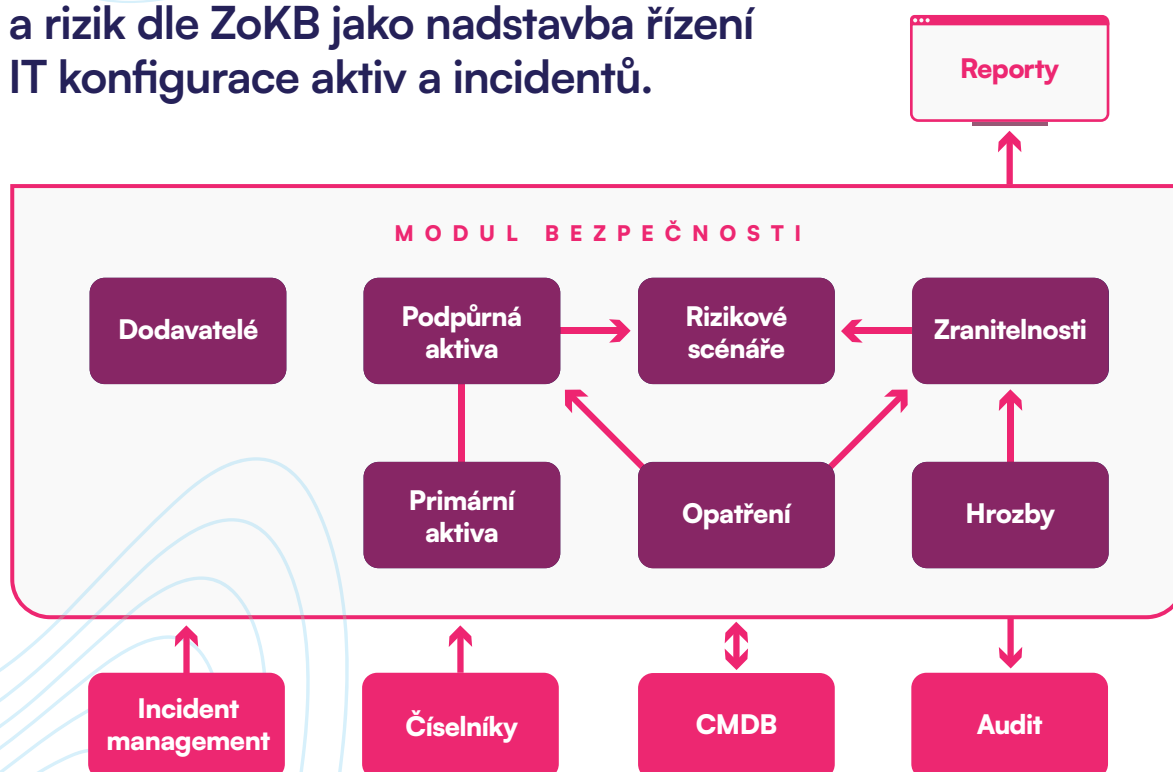
Governance platforma pro podporu souladu
se zákonem o kybernetické bezpečnosti
a směrnicí NIS2.

conceptica.cz

Kybernetická bezpečnost



Architektura řešení modulu správy aktiv a rizik dle ZoKB jako nadstavba řízení IT konfigurace aktiv a incidentů.



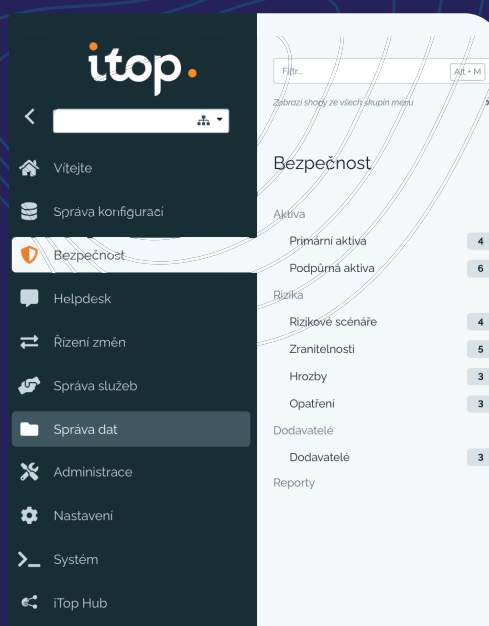
Co je iAktiva?

iAktiva je modul řízení informačních aktiv, rizik a dodavatelů vyvinutý jako licencovaná nadstavba nad platformou iTop.

Role iAktiva ↗

iAktiva je komerčně licencovaná nadstavba.

- ↗ rozšiřuje CMDB o bezpečnostní vrstvu
- ↗ podporuje metodiku řízení aktiv dle ZoKB
- ↗ umožňuje systematické řízení rizik
- ↗ zavádí řízení bezpečnosti dodavatelského řetězce
- ↗ podporuje auditní dohledatelnost a řízení přístupů



iTop tvoří technologický základ — CMDB, workflow engine, auditní logiku a integrační vrstvu.

Role iTop ↗

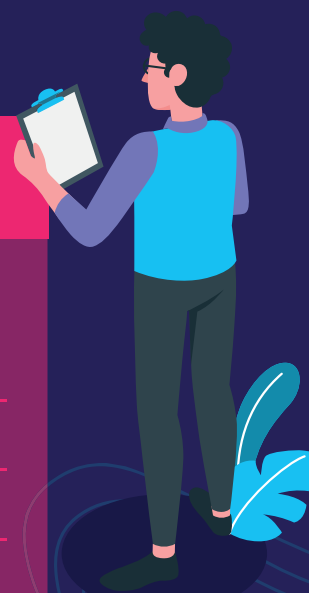
iTop je robustní ITSM a CMDB platforma společnosti Combodo. Je dostupná ve dvou variantách:

Open source verze

- ↗ komunitní edice
- ↗ otevřený zdrojový kód
- ↗ možnost vlastních úprav
- ↗ bez licenčních poplatků za jádro

Enterprise verze

- ↗ oficiální podpora výrobce
- ↗ garantované aktualizace
- ↗ rozšířené bezpečnostní funkce
- ↗ SLA a dlouhodobá udržitelnost



Jak iAktiva funguje

iAktiva

Cílem je zavést jednotnou klasifikaci aktiv organizace a řízené posuzování jejich vazeb a dopadů s auditní dohledatelností.

Primární aktiva

- ↗ služby a informace organizace
- ↗ hodnocení Důvěrnosti, Dostupnosti a Integrity (D+D+I) dle ZoKB

Podpůrná aktiva

- ↗ technická infrastruktura, personální zdroje, podpůrné systémy
- ↗ vazby na primární aktiva a vyhodnocení jejich dopadu

Automatizace a integrace

- ↗ napojení na CMDB iTop umožňuje automatické načítání a aktualizaci dat



Náhled na typickou situaci výsledku posuzování konkrétního rizika.

Poskytování informací občanům kraje formou webového portálu

• Aktiva (Primární aktiva)

Základní informace Provozní informace **Hodnocení** Podpůrná aktiva

Hodnotící tabulka

Oblasti hodnocení	Důvěrnost				Dostupnost				Integrity			
	Nizka	Střední	Vysoká	Kritická	Nizka	Střední	Vysoká	Kritická	Nizka	Střední	Vysoká	Kritická
Soubor osobních údajů	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Práva osobnosti / občanská tajemství	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Vnitřní kontrolní činnosti	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Vnější, ekonomické a finanční zájmy	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Poskytování služeb	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Báňské činnosti	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Pověř / dobré jméno	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Bezpečnost a zdraví osob	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Mezinárodní vztahy	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Uživatelé regulované služby	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Termín hodnocení: 31.12.2025
Termín kdy má být hodnocení provedeno

Datum hodnocení: 04.12.2025
Datum provedení hodnocení

Hodnotitel: marek.nagman
Osoba provádějící hodnocení

Poznámka:
Digitální komentář k hodnocení

POUŽÍT JAKO NOVÉ HODNOCENÍ

Historie hodnocení

Termín hodnocení	Datum hodnocení	Hodnotitel	Důvěrnost	Dostupnost	Integrity
2025-12-31	2025-12-04	marek.nagman	KRITICKÁ	VYSOKÁ	VYSOKÁ
2025-12-31	2025-12-04	martin.jarecka	KRITICKÁ	VYSOKÁ	KRITICKÁ

Rizika ↗

Cílem je kvantifikovat rizika a systematicky řídit jejich vazby na aktiva, hrozby, zranitelnosti a přijatá opatření včetně sledování jejich účinnosti.

- | | |
|--|--|
| ↗ identifikace rizik | ↗ risk matrix (dopad × pravděpodobnost) |
| ↗ rizikové scénáře | ↗ automatizovaný výpočet risk score |
| ↗ evidence hrozeb (externí příčiny) | ↗ heat mapa rizik |
| ↗ evidence zranitelnosti (interní slabiny) | ↗ evidence a vyhodnocení efektivity opatření |

Dodavatelé ↗

Cílem je zajistit prokazatelné řízení rizik třetích stran pomocí centrální evidence a bezpečnostního hodnocení dodavatelů.

- | | |
|---------------------------------------|--|
| ↗ vazba dodavatelů na aktiva a služby | ↗ vazba na incidenty |
| ↗ bezpečnostní hodnocení | ↗ řízení bezpečnostních aspektů dodavatelského řetězce |
| ↗ auditní historie | |

Reporting, audit a kontrola

Dashboard TOP rizik

Trendové grafy

Heat mapa scénářů

Exporty
PDF / CSV / XLSX

Auditní logování
všech změn

Role-based access
control (RBAC)

Verzování číselníků
a historická dohledatelnost

Validace vazeb
mezi objekty

Systém eviduje všechny operace nad objekty včetně uživatele, data a typu akce.

Organizace je průběžně
připravena na audit.

IT překážky, které řeší iTop

iTop je standardní nástroj, který organizaci pomáhá překonávat časté překážky spojené s řízením provozu a rozvoje IT systémů.

- ✓ fragmentované IT procesy a data
- ✓ nedostatečně řízené incidenty
- ✓ chybějící kontrolu nad změnami
- ✓ nízkou efektivitu provozu
- ✓ nedostatečné zabezpečení a auditní dohledatelnost
- ✓ nedostatečnou automatizaci
- ✓ obtížnou integraci s jinými systémy

CMDB jako srdce řízení IT

- ↗ centrální databáze konfigurací
- ↗ mapování vztahů mezi systémy
- ↗ vizualizace závislostí
- ↗ dopadová analýza změn

ITSM procesy

- ↗ incident Management
- ↗ problem Management
- ↗ change Management
- ↗ SLA monitoring
- ↗ workflow engine
- ↗ integrace přes API

Strategická hodnota kombinace iTop + iAktiva

Bezpečnost musí vycházet z reálné znalosti infrastruktury, protože řízení IT kybernetických rizik nemá být oddělené.

Přínos iAktiva pro organizaci ↗

↗ podpora souladu s NIS2, ZoKB a ISO 27001

↗ integrované řízení aktiv, rizik, opatření a dodavatelů

↗ automatizovaný výpočet rizik

↗ řízení přístupů podle rolí

↗ auditní dohledatelnost

↗ jednotná metodika díky centralizovaným číselníkům

Ukázka typického výstupu posouzení konkrétního rizika.

The screenshot displays the iAktiva web application interface for risk assessment. The title bar shows 'Únik citlivých dat přes zneužitou zranitelnost v DB serveru' (Data leak via exploited vulnerability in DB server) and a status 'Do řešení (Rizikový scénář)'. The interface is divided into two main sections: 'Základní informace' (Basic information) and 'Podpůrná aktiva (1)' (Supporting assets (1)). The 'Základní informace' section contains a table with the following data:

ID	1
Název *	Únik citlivých dat přes zneužitou zranitelnost v DB serveru
Popis *	Externí útočník zneužije známou, avšak neoprávněnou zranitelnost v operačním systému nebo databázovém softwaru serveru SQL-FINANCE-01. Získá přístup k databázi ISÚ a exfiltruje finanční výkazy a citlivé osobní údaje zaměstnanců (mzdy).
Typ *	Externí
Kategorie *	Technická
Oblast dopadu *	Důvěrnost
Dopad (Dr) ?	1.20
Reziduální riziko (Rr) ?	2.40
Finanční jednotka dopadu (Fj) ?	5000000.00
Měna ?	CZK
Finanční dopad (Fd) ?	750000.00
Stav *	Do řešení
Garant *	Change Implementor
Vlastník (uživatel) *	martin.jurecka
Datum vytvoření	2025-12-08 07:39:09
Poslední aktualizace	2025-12-09 13:15:43
Kdo provedl poslední úpravu	admin

Scénář využití iTop: CMDB

(Configuration Management Database)

Co je CMDB?

- CMDB je centrální databáze, která dokumentuje všechny IT komponenty (CI) a jejich vzájemné vztahy — od serverů, aplikací, síťových prvků až po smlouvy, služby či kontakty. Díky tomu poskytuje jednotný a aktuální přehled o IT infrastruktuře.

Proč je to důležité?

- kompletní přehled IT majetku a vazeb otevírá možnosti pro audit, řízení změn i compliance reporting
- vazby mezi prvky pomáhají pochopit dopady výpadků nebo změn na služby a SLA
- data z CMDB se používají napříč všemi procesy (ticketing, SLA, eskalace, reporting)

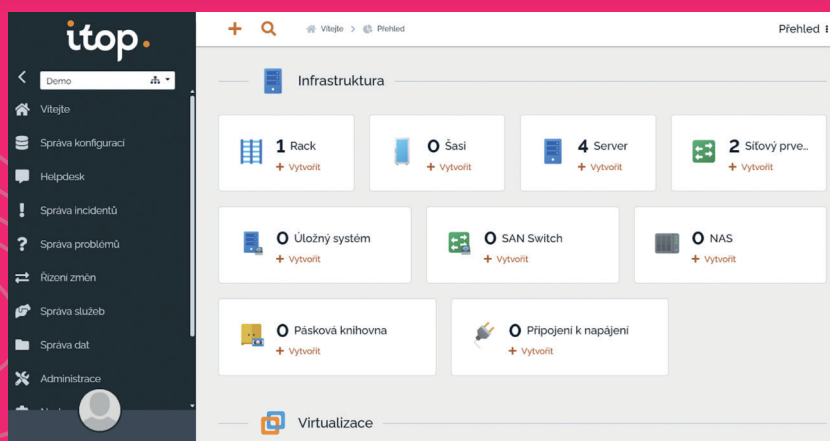
Hlavní funkce v iTop

- centralizovaná databáze všech CI objektů a jejich atributů
- vizualizace vztahů a závislostí mezi komponentami
- integrace s dalšími procesy (incidenty, SLA, workflow).
- import dat a synchronizace s externími zdroji

Výsledek pro organizaci

- lepší přehled o infrastruktuře vede k vyšší efektivitě správy
- snížení chyb při rozhodování o změnách a provozu
- auditovatelná historie a shoda s interními politikami

**Kompletní
přehled
CMDB:**



Scénář využití iTop: Incident Management

Co řeší?

- Incident Management v iTop umožňuje rychlé a strukturované řešení provozních problémů a požadavků uživatelů pomocí ITIL-orientovaného workflow.

K čemu slouží?

- centralizované řízení Incidentů a přidělování ticketů týmům
- automatické sledování SLA a eskalace, aby Incidentům byla přiřazena odpovídající reakce podle priority a SLA
- integrace s CMDB pro dopadovou analýzu — např. při selhání serveru jsou automaticky identifikovány dotčené služby

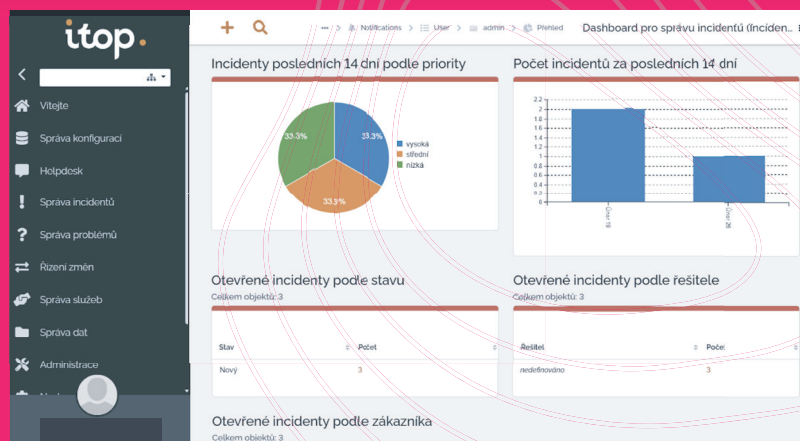
Hlavní funkce v iTop

- ticketovací systém s univerzálními poli, historií, stavy a odpovědnostmi
- možnost automatického přiřazení a eskalace dle SLA/SLT parametrů
- notifikace a komunikace s uživateli i týmy během celého procesu

Výsledek pro organizaci

- zrychlené řešení incidentů a vyšší spokojenost uživatelů
- měřitelné procesy, které lze reportovat vedení i pro potřeby auditu

Incident
Management
— přehled:



Scénář využití iTop: SLA Monitoring

Co je SLA monitoring?

- Monitoring SLA (Service Level Agreement) sleduje, zda služby poskytované IT odpovídají dohodnuté kvalitě a čase reakce/řešení. V iTop je SLA součástí datového modelu a propojena s ticketingem i katalogem služeb.

Proč je to důležité?

- měření výkonu služby dle definovaných parametrů (např. reakční časy, řešení)
- automatické sledování a eskalace, když SLA hrozí překročení
- reporting pro vedení pro posouzení kvality IT služby

Jak to funguje?

- SLA je navázáno na jednotlivé služby a zákazníky v katalogu služeb
- systém automaticky počítá splnění parametrů na základě definovaných měřítek
- výsledky lze vizualizovat a exportovat pro interní i externí reporting

Výsledek pro organizaci

- transparentní měření kvality IT služeb
- jednodušší řízení služeb a SLA s dodavateli
- podklad pro rozhodování ve vedení

Napojení SLA
na služby
a smlouvy
se zákazníky:

The screenshot displays the iTop web interface. On the left is a dark sidebar with the iTop logo and a menu of navigation items. The main panel shows the 'Standard SLA' configuration page. It includes a breadcrumb trail at the top: 'Vítejte > Přehled > Incident > Přehled > SLT > SLA > Standard SLA'. Below this, there are tabs for 'Vlastnosti', 'SLTs (2)', and 'Smlouvy se zákazníky (3)'. The 'Smlouvy se zákazníky' tab is active, showing a table with the following data:

Spojení (Smlouva se zákazníkem / Služba)	Smlouva se zákazníkem	Služba	SLA
Customer contract Demo / Computers and peripherals	Customer contract Demo	Computers and peripherals	Standard SLA
Customer contract Demo / Software	Customer contract Demo	Software	Standard SLA
Customer contract Demo / Telecom and connectivity	Customer contract Demo	Telecom and connectivity	Standard SLA

Scénář využití iTop: Vlastní workflow pro IT úkoly a provozní situace

Co je workflow v iTop?

- Workflow je logika, která řídí životní cyklus úkolů, ticketů a procesů podle definovaných pravidel — od vytvoření až po uzavření. iTop podporuje jak základní ITIL procesy, tak vlastní definice dle potřeby.

K čemu slouží?

- automatizace opakovaných úloh — přiřazování, kontrola stavu, eskalace
- custom workflow s přizpůsobenými pravidly a stavy
- notifikace a akce řízené pravidly i časovými podmínkami

Funkční příklady

- automatické přidělení ticketu týmu podle typu incidentu
- eskalace a upozornění, když úkol přesáhne definovaný časový limit
- vlastní formuláře a pole podle procesu zákazníka

Výsledek pro organizaci

- standardizované postupy napříč IT procesy
- snížení manuální správy a chyb v průběhu řešení
- lepší měřitelnost a řízení výkonnosti týmů

Konfigurace triggerů pro zasílání oznámení:

The screenshot shows the iTop web interface. On the left is a dark sidebar with navigation links: Vítání, Správa konfigurací, Helpdesk, Správa incidentů, Správa problémů, Řízení změn, Správa služeb, Správa dat, Administrace, Nastavení, and Systém. The main content area is titled 'Konfigurace upozornění' (Notification Configuration). It contains introductory text about triggers and a list of three configuration steps: 1. Defining triggers based on object type, status, or priority; 2. Defining triggers based on object type and status; 3. Defining triggers based on object type and priority. Below this is a table titled 'Dostupné trigger' (Available triggers) with columns for Trigger, Typ (Type), and Dopřijímací informace (Receiving information). The table lists three triggers: 'Aktualizace incidentu emailem' (Email incident update), 'Trigger when updated by mail' (Trigger when updated by mail), and 'class restriction Incident' (class restriction Incident).

Licencovaná nadstavba nad iTop pro řízení aktiv, rizik a souvisejících odpovědností.

Sociální sítě:



Conceptica Inovace
Aplikace Digitalizace



Conceptica s.r.o.

Kontakt:



+420 777 865 290



info@conceptica.cz

↗ **conceptica.cz**

řešení propojuje IT governance
a ITSM

itop.

do jednotné platformy pro řízení
aktiv, rizik a vazeb

iAktiva

Illustrations by StorySet

CONCEPTICA 