Otázky k posouzení stavu IT ve firmě

Kompletní průvodce pro hodnocení IT zralosti organizace

Verze dokumentu: 2.0
Datum vytvoření: 26. září 2025
Architekt a iniciátor projektu: Milan Trnka

Úvod a metodika

Účel dokumentu

Tento dokument slouží jako komplexní nástroj pro posouzení stavu IT ve firmě. Otázky jsou strukturované tak, aby pokryly všechny klíčové oblasti IT governance a poskytly objektivní pohled na:

- Technickou zralost IT infrastruktury a systémů
- Organizační zralost IT jako funkce
- Strategické postavení IT v organizaci
- Připravenost na budoucí výzvy a růst

Jak používat tento dokument

Fázovaný přístup:

1. **Přípravná fáze:** Identifikace klíčových respondentů
2. **Sběr dat:** Strukturované rozhovory podle sekcí
3. **Analýza:** Vyhodnocení odpovědí a identifikace gaps
4. **Akční plán:** Prioritizace oblastí pro zlepšení

Doporučení respondenti:

- IT ředitel/manažer
- Systémoví administrátoři
- Vedoucí jednotlivých oddělení (jako uživatelé IT)
- Finanční ředitel (pro rozpočtové otázky)
- CEO/jednatel (pro strategické otázky)

Fázovaný přístup pro SME

Doporučení pro firmy s 50-500 zaměstnanci

Místo hodnocení všech 11 oblastí současně doporučujeme trojfázový přístup, který zajistí postupnou transformaci IT bez přehlcení organizace:

FÁZE 1: Operační stabilita a odolnost (3-6 měsíců)

Cíl: Zajistit spolehlivost provozu a ochranu před výpadky

Oblast	Klíčové otázky	Cílová zralost
Infrastruktura	Monitoring, dokumentace, single points of failure	Úroveň 3
Bezpečnost	MFA, přístupová práva, incident response	Úroveň 3
Zálohování	Strategie 3-2-1-1-0, testování obnovy, RTO/RPO	Úroveň 3
IT Tým	Zastupitelnost, dokumentace know-how	Úroveň 2-3

FÁZE 2: Strategická spolupráce a efektivita (6-12 měsíců)

Cíl: IT jako partner byznysu, efektivní investice a projekty

Oblast	Klíčové otázky	Cílová zralost
Organizační postavení	Vnímání IT, SLA, zapojení do vedení	Úroveň 3-4
Projekty a rozvoj	Roadmapa, prioritizace, měření ROI	Úroveň 3
Finance	Rozpočtování, optimalizace nákladů	Úroveň 3

FÁZE 3: Optimalizace a konkurenční výhoda (12+ měsíců)

Cíl: Využití dat a automatizace pro růst

Oblast	Klíčové otázky	Cílová zralost
Data a analytika	BI, data governance, GDPR	Úroveň 2-3
Digitalizace	Automatizace procesů, emerging technologie	Úroveň 2-3
Externí partneři	Optimalizace SLA, vendor management	Úroveň 3

Obsah hodnocených oblastí

1. IT infrastruktura a architektura
2. Bezpečnost a řízení přístupů
3. Zálohování a disaster management
4. Organizační a hierarchické postavení IT
5. Projekty a rozvoj
6. Stav týmu a lidských zdrojů
7. Finance a investice
8. Externí partneři a služby
9. Data a analytika
10. Digitalizace a automatizace
11. Hodnotící škály a metriky

---

1. IT infrastruktura a architektura

Základní systémy a aplikace

Aplikační portfolio:

- Jaké jsou dnes klíčové systémy a aplikace (ERP, CRM, výrobní systémy, e-shop)?
- Kolik aplikací celkem firma používá a jak jsou kategorizovány podle kritičnosti?
- Které systémy jsou považovány za business-critical?
- Existuje mapa závislostí mezi aplikacemi?

Technologická architektura:

- Jak je řešena technologická architektura (on-premise, cloud, hybrid)?
- Existuje dokumentovaná IT architektura a aktuální schémata?
- Jak staré jsou klíčové systémy a jaká je jejich technologická udržitelnost?
- Existuje technický dluh a jak je řešen?

Monitoring a dohled

Hodnotící indikátory (1-5):

- **Úroveň 1:** Žádný monitoring, reaktivní řešení problémů
- **Úroveň 2:** Základní monitoring, většina alertů od uživatelů
- **Úroveň 3:** Strukturovaný monitoring s alerting systémem

- **Úroveň 4:** Proaktivní monitoring s dashboardy a SLA tracking
- **Úroveň 5:** Komplexní monitoring s AI-driven insights a automatickou remediation

Klíčové otázky:

- Jak je řešeno monitorování dostupnosti a výkonu?
- Jaké nástroje se používají pro monitoring infrastruktury a aplikací?
- Jsou definovány SLA pro dostupnost jednotlivých služeb?
- Jak probíhá incident management a eskalace?

Kapacitní plánování:

- Jak se plánuje růst kapacit (výpočetní výkon, úložiště, síť)?
- Jsou sledovány trendy využití zdrojů?
- Jak se řeší špičky a seasonal peaks?
- Existuje disaster recovery pro hardware selhání?

---

2. Bezpečnost a řízení přístupů

Bezpečnostní politiky a governance

Strategické řízení bezpečnosti:

- Má firma definovanou bezpečnostní politiku a kdo ji schvaluje?
- Jak často se bezpečnostní politika aktualizuje?
- Existuje pozice CISO nebo bezpečnostního manažera?
- Jak je bezpečnost řízena na úrovni představenstva/vedení?

Compliance a regulatorní požadavky:

- Kterým regulatorním požadavkům firma podléhá (GDPR, ISO 27001, odvětvové předpisy)?
- Jak je zajišťována compliance s těmito požadavky?
- Probíhají interní nebo externí audity bezpečnosti?
- Jak se řeší nalezené non-compliance situace?

> **Doporučení:** Pro české organizace doporučujeme jako referenční rámec **Minimální bezpečnostní standard** vydaný NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost).

Správa identit a přístupů

Identity and Access Management (IAM)

Hodnotící indikátory (1-5):

- **Úroveň 1:** Manuální správa účtů, sdílená hesla, žádná centrální správa
- **Úroveň 2:** Základní AD/LDAP, manuální onboarding/offboarding
- **Úroveň 3:** Centralizovaná správa identit, základní MFA
- **Úroveň 4:** Pokročilé IAM s automatizovaným provisioning, role-based access
- **Úroveň 5:** Zero-trust architektura, adaptive authentication, privileged access management

Klíčové otázky:

- Jak je řešena správa uživatelských účtů a přístupových práv?
- Je implementováno MFA (vícefaktorové ověřování)?
- Jak je řešen princip nejmenších oprávnění (least privilege)?
- Jak probíhá audit přístupových práv?

Bezpečnostní opatření

Technická ochrana:

- Jaká je úroveň ochrany perimetru (firewall, IDS/IPS)?
- Jak je řešena ochrana koncových zařízení (endpoint protection)?
- Je implementována segmentace sítě?
- Jak je řešeno šifrování dat (at rest, in transit)?

Bezpečnostní kultura:

- Jak zaměstnanci vnímají bezpečnostní opatření?
- Existují jasné postupy pro hlášení bezpečnostních incidentů?
- Jak se řeší balance mezi bezpečností a uživatelským komfortem?
- Jsou definovány consequence za porušení bezpečnostních politik?

---

3. Zálohování a disaster management

Strategie zálohování

Zálohování dat

Hodnotící indikátory (1-5):

- **Úroveň 1:** Nepravidelné zálohy, pouze lokálně, netestované
- **Úroveň 2:** Pravidelné zálohy, ale pouze lokálně nebo netestované
- **Úroveň 3:** Strategie 3-2-1-1-0 implementována, základní testování
- **Úroveň 4:** Automatizované zálohy s monitoringem, pravidelné testy obnovy

- **Úroveň 5:** Immutable backups, automated disaster recovery, kontinuální validace

Klíčové otázky:

- Jak často se dělají zálohy a kde jsou uchovávány?
- Jaká je strategie zálohování (3-2-1-1-0 rule, incremental vs. full)?
- Jak jsou zabezpečeny záložní data (šifrování, access control)?
- Existuje geografická distribuce záloh?

Testování a obnova:

- Jsou zálohy pravidelně testovány (obnova)?
- Jak často se testuje úplná obnova systémů ze záloh?
- Jaké jsou zkušenosti se skutečnou obnovou dat?
- Jsou dokumentovány postupy pro obnovu?

Business Continuity a Disaster Recovery

Plánování kontinuity:

- Má firma funkční Disaster Recovery Plan a Business Continuity Plan?
- Kdy byl naposledy aktualizován a testován DRP/BCP?
- Jsou definovány RTO (Recovery Time Objective) a RPO (Recovery Point Objective)?
- Existuje krizový tým a jsou definovány role při incidentu?

---

4. Organizační a hierarchické postavení IT

Pozice IT v organizaci

Strategické postavení:

- Kde je IT organizačně zařazeno (pod CFO, COO, samostatně)?
- Je IT reprezentováno na úrovni vedení/představenstva?
- Jak je IT vnímáno - jako nákladové středisko nebo strategický partner?
- Má IT možnost ovlivňovat strategická rozhodnutí firmy?

Governance:

- Existuje IT steering committee nebo podobný orgán?
- Jak probíhá prioritizace IT investic a projektů?
- Jsou definovány IT politiky a standardy?
- Jak je řešen shadow IT?

---

5. Projekty a rozvoj

Projektové řízení

Hodnotící indikátory (1-5):

- **Úroveň 1:** Chaotické, projekty se často nedokončují
- **Úroveň 2:** Problematické, časté zpoždění
- **Úroveň 3:** Průměrné projektové řízení
- **Úroveň 4:** Dobré projektové řízení s metodikou
- **Úroveň 5:** Vynikající, metodické a efektivní

Klíčové otázky:

- Existuje IT roadmapa a jak je aktualizována?
- Jak jsou IT projekty prioritizovány a schvalovány?
- Jaká metodika se používá pro projektové řízení?
- Jak se měří úspěšnost IT projektů?

Metriky projektů:

- Project success rate (%)
- Project on-time delivery (%)
- Project budget variance (%)
- User adoption rate for new systems (%)
- ROI of IT projects

---

6. Stav týmu a lidských zdrojů

Struktura a velikost týmu

Organizace IT týmu:

- Jak velký je IT tým a jaké má role (infrastruktura, aplikace, podpora, vývoj)?
- Jak je tým organizován (podle technologií, služeb, projektů)?
- Existují jasně definované role a odpovědnosti?
- Jak je řešena koordinace mezi různými IT týmy?

Reporting a hierarchie:

- Jaká je hierarchická struktura IT týmu?
- Kdo jsou klíčoví lidé (team leads, architekti, senior specialisté)?
- Jak probíhá reportování v rámci IT týmu?
- Existují cross-functional týmy nebo centra kompetencí?

Kompetence a dovednosti

Hodnotící indikátory (1-5):

- **Úroveň 1:** Ad-hoc skills, žádná mapa kompetencí, reaktivní řešení skill gaps
- **Úroveň 2:** Základní přehled o skills, sporadické školení
- **Úroveň 3:** Skills matrix existuje, pravidelné hodnocení gaps, plánované školení
- **Úroveň 4:** Systematický rozvoj skills, career paths, mentoring programy
- **Úroveň 5:** Proaktivní skills development, internal training programy, knowledge sharing kultura

Klíčové otázky:

- Jaké jsou silné stránky týmu a kde chybí kompetence?
- Existuje skills matrix nebo inventory kompetencí?
- Jak se identifikují skill gaps?
- Jaké jsou plány pro rozvoj chybějících kompetencí?

Zastupitelnost a kontinuita

Operační kontinuita:

- Jak je zajištěna zastupitelnost (absence, dovolené)?
- Existují backup osoby pro kritické role?
- Jak se řeší emergency situations při nedostupnosti klíčových lidí?
- Jsou definovány escalation paths pro různé oblasti?

Knowledge management:

- Jak probíhá znalostní transfer a dokumentace know-how?
- Existují single points of knowledge v týmu?
- Jak jsou dokumentovány procesy a postupy?
- Probíhá cross-training mezi členy týmu?

Motivace a spokojenost

Work environment:

- Má tým přístup k moderním nástrojům a technologiím?

- Jak jsou hodnoceny pracovní podmínky IT týmu?
- Existuje možnost home office nebo flexible work?
- Jak je řešen work-life balance?

Development a kariérní růst:

- Jaké jsou možnosti professional development?
- Existuje rozpočet na školení a certifikace?
- Jak probíhají performance reviews?
- Jaká je fluktuace a motivace IT zaměstnanců?

Benchmark pro IT tým (200 zaměstnanců)

Typická struktura IT týmu SME:

- IT Manager/Ředitel (1) - 80-120k Kč/měsíc
- System Admin/Infrastructure (1-2) - 45-65k Kč/měsíc
- Application Support/Developer (1-2) - 50-75k Kč/měsíc
- Help Desk/User Support (1-2) - 35-50k Kč/měsíc
- External/Freelance projekty - 800-1500 Kč/hod

---

7. Finance a investice

IT rozpočet - detailní analýza

Hodnotící indikátory (1-5):

- **Úroveň 1:** Žádný strukturovaný IT rozpočet, ad-hoc výdaje
- **Úroveň 2:** Základní rozpočet, převážně OPEX, minimum plánování
- **Úroveň 3:** Strukturovaný rozpočet CAPEX/OPEX, roční plánování
- **Úroveň 4:** Detailní rozpočet s měsíčním sledováním, TCO analýzy
- **Úroveň 5:** Zero-based budgeting, activity-based costing, continuous optimization

Doporučené alokace rozpočtu:

- 60% Personální náklady (platy, benefity, školení)
- 25% Technologie (HW, SW licence, cloud)
- 10% Služby (externí support, consulting, projekty)
- 5% Reserve (emergency, nepředvídané výdaje)

Finanční metriky:

- IT spend as % of revenue
- Cost per user
- ROI of IT investments
- Budget variance (%)
- Cost optimization savings

---

8. Externí partneři a služby

Vendor management

Klíčové otázky:

- Jaké externí služby firma využívá (outsourcing, managed services)?
- Jak jsou řízeny vztahy s dodavateli IT služeb?
- Jsou definovány SLA a jak se měří jejich plnění?
- Existuje vendor risk assessment?

---

9. Data a analytika

Data governance

Klíčové otázky:

- Jak je řízena kvalita a integrita dat?
- Existují definovaní data owners a data stewards?
- Jak je zajištěna compliance s GDPR?
- Využívá firma BI nástroje pro analytiku?

---

10. Digitalizace a automatizace

Stav digitalizace

Klíčové otázky:

- Které procesy jsou již digitalizovány?
- Jaké jsou plány pro další automatizaci?
- Sleduje firma emerging technologie (AI, IoT, RPA)?
- Jak je řízena digitální transformace?

11. Hodnotící škály a metriky

Univerzální hodnotící škála (1-5)

Úroveň	Popis	Charakteristika
1	Initial/Ad-hoc	Nepředvídatelné, reaktivní, závislé na jednotlivcích
2	Developing	Základní procesy existují, ale nejsou standardizované
3	Defined	Procesy jsou dokumentovány a standardizovány
4	Managed	Procesy jsou měřeny a řízeny pomocí metrik
5	Optimized	Kontinuální zlepšování, best practices

KPIs pro jednotlivé oblasti

Infrastruktura:

- System availability (%)
- Mean time to recovery (MTTR)
- Planned vs unplanned downtime ratio
- Infrastructure cost per user

Bezpečnost:

- Number of security incidents
- Mean time to detect (MTTD)
- Mean time to respond (MTTR)
- Compliance audit score
- Security training completion rate (%)

Praktické tipy pro týmový management v SME

Týdenní team management checklist:

- One-on-one s klíčovými lidmi (15-30 min týdně)
- Workload monitoring - kdo je přetížený/nedostatečně vytížený
- Skill development tracking - progres v plánovaném učení

- Knowledge sharing - co se naučil tým tento týden

Měsíční team health review:

- **Projekt load:** Jsou lidé přetížení nebo mají prostor na development?
- **Skill gaps:** Objevily se nové potřeby kompetencí?
- **Motivation pulse:** Krátký neformální chat o spokojenosti
- **Training opportunities:** Nadcházející kurzy, konference, certifikace

Čtvrtletní strategic review:

- Career development conversations s každým členem týmu
- Compensation review - jsou platy stále competitive?
- Team structure assessment - potřebujeme nové role/pozice?
- Culture assessment - funguje komunikace a spolupráce?

Warning signs pro SME IT management:

- 🚨 Jeden člověk zná >70% systémů = kritické riziko
- 🚨 Žádné školení >12 měsíců = zaostávání za trendy
- 🚨 Overtime >15% pravidelně = špatné capacity planning
- 🚨 Fluktuace >20% ročně = systémový problém s motivací/kulturou

---

Doporučená metodika pro SME

Přizpůsobení pro firmu s 200 zaměstnanci

Klíčové charakteristiky střední firmy:

- IT tým: 3-8 lidí
- IT rozpočet: 2-5% obratu
- Systémy: 10-30 aplikací
- Potřeba: rychlý ROI, praktická řešení

Zjednodušený assessment proces

Týden 1-2: Cílené rozhovory

Místo rozhovorů s každým vedoucím vyberte 4-5 klíčových reprezentantů:

- IT Manager/Ředitel: Technické otázky, rozpočet, strategie
- CEO/Jednatel: Strategické vnímání IT, investiční rozhodování

- Zástupce byznysu: 2-3 vedoucí (Obchod, Výroba, Finance) - vnímání IT služeb

---

Závěrečné doporučení

Klíčové principy úspěšného IT assessment

1. Holistický přístup

- Nehodnoťte pouze technologie, ale i procesy, lidi a kulturu
- Zohledněte business kontext a strategické cíle organizace
- Balancujte současné potřeby s budoucími requirements

2. Objektivita a transparentnost

- Používejte data a fakta, ne pouze opinions
- Zapojte různé perspektivy a stakeholders
- Buďte otevření k uncomfortable findings

3. Praktičnost doporučení

- Doporučení musí být implementovatelná s dostupnými zdroji
- Prioritizujte podle business impact a feasibility
- Poskytněte konkrétní kroky, ne pouze high-level guidance

4. Change management

- Připravte organizaci na změny vyplývající z assessment
- Komunikujte value proposition jasně
- Zajistěte buy-in od key stakeholders

Časté úskalí a jak se jim vyhnout

Příliš technické zaměření

- ❌ Risk: Ztráta business perspective
- ✅ Mitigation: Zapojte business stakeholders do celého procesu

Paralýza analýzou

- ❌ Risk: Nekonečné analyzování bez action
- ✅ Mitigation: Stanovte jasné deadlines a decision points

Nedostatečný follow-up

- ❌ Risk: Skvělý report, který skončí v šuplíku
- ✅ Mitigation: Establish accountability a regular review cycles

Ignorování kulturních aspektů

- ❌ Risk: Technicky správná doporučení, která organizace neakceptuje
- ✅ Mitigation: Assess organizational readiness for change

Podcenění prevence

- ❌ Risk: Jeden incident stojí více než rok prevence
- ✅ Řešení: Začněte s free/low-cost řešeními (MFA, školení)

> Úspěšný IT assessment je začátek journey, ne konec. Klíčem je transformovat insights do actionable improvements, které skutečně posílí IT capabilities organizace a její schopnost dosáhnout business cílů.

Slovníček pojmů

Zkratka	Význam	Popis
RTO	Recovery Time Objective	Maximální přípustná doba výpadku systému – jak rychle musí být systém obnoven po havárii
RPO	Recovery Point Objective	Maximální přípustná ztráta dat – jak staré mohou být poslední zálohy (např. RPO 1 hodina = ztráta max. 1 hodiny dat)
BCP	Business Continuity Plan	Plán kontinuity podnikání – strategie pro udržení chodu firmy během a po incidentu
DRP	Disaster Recovery Plan	Plán obnovy po havárii – technické postupy pro obnovu IT systémů
SLA	Service Level Agreement	Dohoda o úrovni služeb – definuje očekávanou kvalitu a dostupnost služby
MFA	Multi-Factor Authentication	Vícefaktorové ověřování – kombinace více metod přihlášení (heslo + SMS/aplikace)
IAM	Identity and Access Management	Správa identit a přístupů – řízení kdo má přístup kam
MTTR	Mean Time To Recovery	Průměrná doba obnovy – jak dlouho trvá oprava po výpadku
MTTD	Mean Time To Detect	Průměrná doba detekce – jak dlouho trvá zjištění problému

Zkratka	Význam	Popis
TCO	Total Cost of Ownership	Celkové náklady vlastnictví – všechny náklady spojené s provozem systému
ROI	Return On Investment	Návratnost investice – poměr přínosu k nákladům
CAPEX	Capital Expenditure	Kapitálové výdaje – jednorázové investice (nákup HW, SW)
OPEX	Operational Expenditure	Provozní výdaje – průběžné náklady (licence, cloud, údržba)
KPI	Key Performance Indicator	Klíčový ukazatel výkonnosti – metrika pro měření úspěšnosti
SME	Small and Medium Enterprise	Malé a střední podniky (typicky 50-500 zaměstnanců)
3-2-1-1-0	Backup Strategy	3 kopie dat, 2 různá média, 1 offsite, 1 offline/immutable, 0 chyb při ověření obnovy
BI	Business Intelligence	Nástroje pro analýzu dat a reporting
GDPR	General Data Protection Regulation	Obecné nařízení o ochraně osobních údajů (EU)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost	Česká autorita pro kybernetickou bezpečnost, vydává standardy a doporučení