IT GOVERNANCE 2026

Governance agentního vývoje softwaru

Kam se přesunulo úzké hrdlo – a kde musí zůstat člověk

Vilém Hujňák · OAK'S LAB

15. října 2026

ISACA
Czech Republic Chapter

AI-NATIVE AGILE MANIFESTO · ERICSSON, 2026

Shared context and living knowledge over meetings and static documents

Human intent and AI execution over manual handoffs across roles

Parallel, continuous verification over sequential phase gates

Orchestrated AI workforces over isolated tool assistance

Reusable blueprints with local adaptation over rigid frameworks or reinvention

„Human in Control, not Human in the Loop.“
„Corrections after the fact are cheap.“

– princip „The New Teams“, kapitola 2.2

Kdy oprava levná není?

Zdroj: Britto a kol. (Ericsson), AI-Native Large-Scale Agile Manifesto, arXiv, 5/2026

ISACA Czech Republic Chapter

Obsah přednášky

I. Úzké hrdlo se stěhuje
II. Discovery: nejdůležitější lidská práce
III. Product solutioning: scope jako kód
IV. Kontext a harness pro lidi i agenty
V. Od nápadu po release: lidské brány
VI. Vibe coding a AI builder stack
VII. Řízení rizik: Per Partes Domino (první zkušenosti)
VIII. Governance, bezpečnost, odpovědnost dodavatele

ISACA
Czech Republic Chapter

ÚVOD

Odkud se dívám

OAK'S LAB

- Celé SDLC, od discovery po provoz
- Scale-upy a enterprise, hlavně US trh
- Pohled napříč projekty, ne z pilotu

O ČEM TO BUDE

Praxe zakázkového studia: řízení rizik a odpovědnost

ISACA Czech Republic Chapter

I.

Úzké hrdlo se stěhuje

Od psaní kódu k definici produktu

ISACA
Czech Republic Chapter

POSLEDNÍCH 12 MĚSÍCŮ U NÁS

Kam se stěhovalo úzké hrdlo

1 · **Psaní kódu**
Kolik kódu tým stihne napsat

→

2 · **Code review**
PR přibývá, review je nová fronta

→

3 · **QA a verifikace**
Dokázat, že to dělá správnou věc

→

4 · **Definice produktu**
Co stavět, proč a jak to rozvíjet

Úzké hrdlo nezmizelo. Přesunulo se tam, kde se rozhoduje.

ISACA Czech Republic Chapter

EXTERNÍ DATA

Výstup je zadarmo, porozumění ne

+91 %

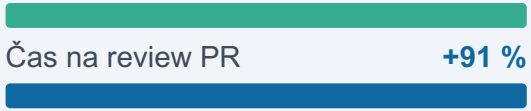
delší review PR

Na úrovni celé firmy se zisk neprojevil (bez signifikantní korelace).

TÝMY S HODNĚ AI VS. OSTATNÍ

PR na vývojáře +98 %

Čas na review PR +91 %



Víc kódu = delší review.

+243 %

incidentů na jedno PR

22 000 vývojářů, 2026. Medián review je 5× delší.

TÝMY S HODNĚ AI VS. OSTATNÍ

Průchod úloh +34 %

Incidenty na PR +243 %



Rychleji, ale s víc incidenty.

55 %

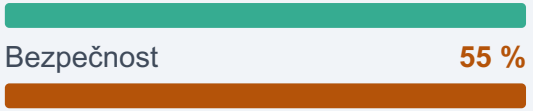
security pass rate AI kódu

Dva roky skoro beze změny u většiny modelů.

AI KÓD, KTERÝ PROJDE TESTEM

Syntaxe >95 %

Bezpečnost 55 %



Funguje, ale bezpečný napůl.

Zdroje: Faros 2025 a 2026 · Veracode 2026

ISACA Czech Republic Chapter

OAK'S LAB

Kde se reálně bere 2–3×

„Coding is rarely the bottleneck on projects.“

– Andy Powell, Partner & COO, OAK'S LAB

01 **Specifikace:** PL a Tech Lead s agenty dotáhnou edge cases a návrh systému rychleji

02 **Prototypy** s designéry místo statických dokumentů

03 **Testy a PR review** přes vlastní agenty

04 Psaní kódu až potom

Z naší praxe: aplikaci, kterou by před rokem dělal celý tým 2 měsíce, jsme letos udělali ve dvou za měsíc.

ISACA Czech Republic Chapter

II.

Discovery: nejdůležitější lidská práce

Kód je skoro zadarmo. Rozhodnutí ne.

ISACA
Czech Republic Chapter

Největší riziko: rychle postavit špatnou věc

> „AI makes great people incredible, and actually AI makes lower performing people worse.“
>
> – Andy Powell, Partner & COO, OAK'S LAB

> „No one actually cares about AI. All they care about are outcomes.“
>
> – Kryštof Šraier, Head of AI & Delivery, OAK'S LAB

ISACA
Czech Republic Chapter

OAK'S LAB WAY

Než se napíše řádek kódu

FOUNDATION

Problem Area

7 aktivit, např.:

- Stakeholder mapping
- Competitor analysis
- AS-IS proces
- Problem hypotheses
- Product hypotheses
- ...

Gate

FOUNDATION

Solution Area

14 aktivit, např.:

- TO-BE user journeys
- Architektura
- MVP scope, estimace

Gate

DELIVERY

Dual-Track Agile

Discovery track: co stavět

Delivery track: postavit a vydat

Každá deliverable: **Accountable engineer**, **Standards** (definice hotovo), pohledy **PM · Tech Lead · Design**.

ISACA Czech Republic Chapter

OAK'S LAB WAY

Gate = lidský kontrolní bod s evidencí

V metodice	V jazyce governance
Standards	Kontrolní kritéria
Accountable role	Vlastník kontroly
Gate-check s citovaným důkazem	Auditní evidence
READY / MINOR_GAPS / NOT_READY	Doporučení (rozhoduje tým, ne AI)
[ASSUMPTION] → [VALIDATED]	Dohledatelnost: kdo, co, kdy

„The team decides; you surface the evidence.“

„Never silently promote an assumption to a fact.“

Zdroj: OAK'S LAB WAY discovery skills

ISACA Czech Republic Chapter

DĚLBA PRÁCE V DISCOVERY

AI připraví, člověk rozhoduje

AI: coach, drafter, auditor	Člověk: nedelegovatelné
Desk research do šířky	Jaké rozhodnutí má analýza podpořit
Syntéza rozhovorů, témata napříč	Stakeholder schvaluje AS-IS proces
Priority bez dat jako [ASSUMPTION]	Povýšit předpoklad na fakt
Pressure test: PM / TL / Design	Architekturu schvaluje CTO

Každý výstup musí obsahovat aspoň jeden insight, který uživatel sám nepřinesl. Jinak platí: *„you haven't done discovery, you've done transcription“*

Největší riziko: „The single biggest risk … is confirmation bias.“

ISACA Czech Republic Chapter

REQUIREMENTS ELICITATION

Místo textu prototyp

DŘÍVE

- Požadavky v dokumentu
- Připomínky nad textem
- Nedorozumění se ukáže až při vývoji

DNES

- Prototyp za hodiny až dny
- Diskuse nad klikatelnou věcí
- Nejlépe když ho přinese sám klient

> **Podmínka:** design tokens, podporovaný stack a architektonické vzory.
>
> „…this is a nice prototype, so let's start over.“ – Kryštof Šraier, OAK'S LAB

III.

Product solutioning

Scope jako kód a lidské schválení

ISACA
Czech Republic Chapter

SCOPE SOURCE OF TRUTH

Kde žije scope

SYSTÉM ZÁZNAMU

Jira (nebo Linear)

- Klient i tým vidí stejný stav
- Agenti čtou živě přes MCP
- Agent zapisuje až po schválení

HISTORIE A KONTROLA ZMĚN

Repozitář

- Denní snímek boardu a diff
- Decision log z callů s klientem
- BPMN prolinkované na tickety

Jira vs. Linear je druhořadé. Rozhoduje, jestli s nástrojem umí pracovat agent i jiný tým.

ISACA Czech Republic Chapter

ADVANCED SCOPE MANAGEMENT

Co jsme postavili: scope jako kód

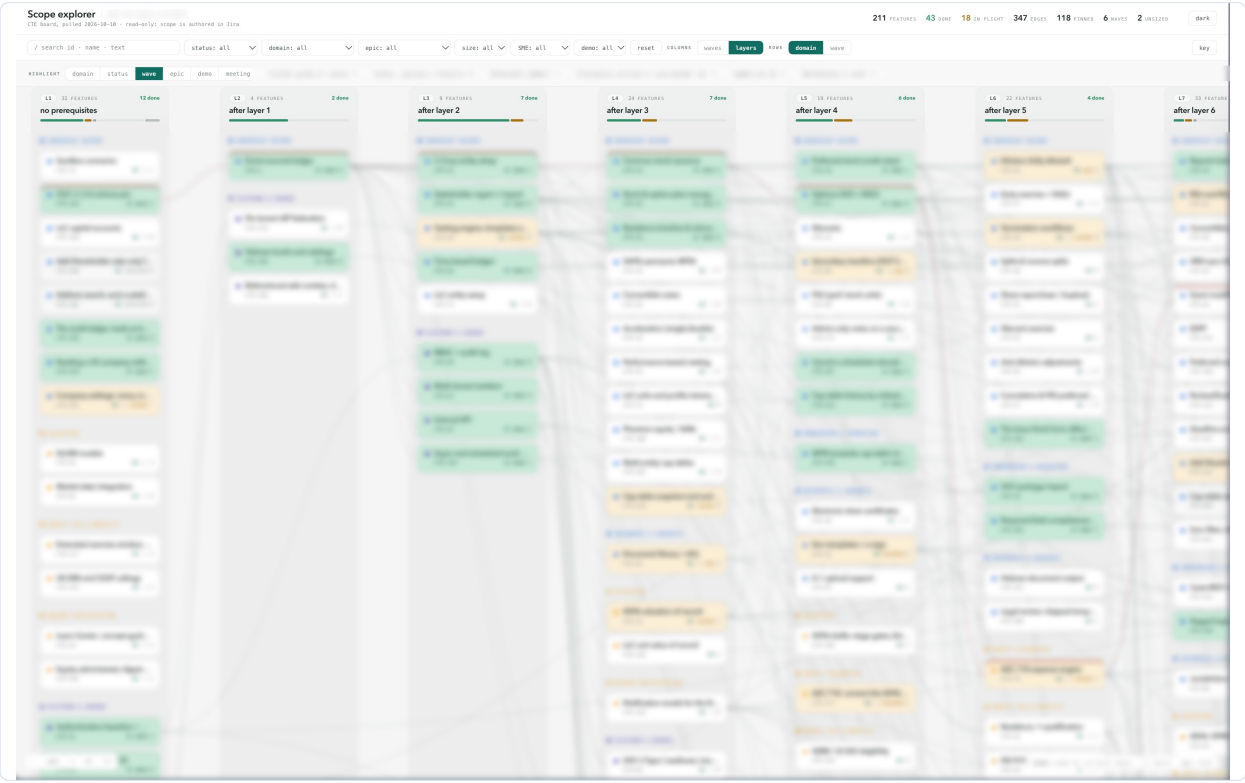
01 **Scope JSON** z boardu

02 **Dependency graph:** co co blokuje

03 **Decision log** z callů s klientem

04 **BPMN** prolinkované na tickety

05 **Dopad změny** na plán a timeline



ISACA Czech Republic Chapter

SCOPE UPDATE · REÁLNÝ PŘÍKLAD, ANONYMIZOVÁNO

Agent navrhne, člověk rozhodne

Z DRAFTU OD CLAUDA

„…nothing written to Jira yet.“

„One idea, four tickets.“

Kritéria citují klienta s datem.

„Links to remove (your approval needed).“

„Jira writes: 1 create, 13 edits, 4 links added, 3 links removed.“

1. Claude stáhne board a navrhne úklid jako dokument
2. **Já čtu, ptám se a chci další kontroly**
3. **Schválím** → teprve pak zápis do Jiry
4. Pull do repa, záznam rozhodnutí, merge request

ISACA Czech Republic Chapter

ADVANCED SCOPE MANAGEMENT · AUDIT PO DVOU MĚSÍCÍCH

Polovina nástrojů stojí za to

6 207 řádků nástrojů a 772 řádků instrukcí

22 opravných commitů, 7 selhaných běhů

12/16 zachycených chyb byly chyby nástroje

Ponechat

Denní snímek boardu a diff
odhalil přepsaná kritéria u ticketů, které už se stavěly

Timeline
jediná část, kterou dnes ukazujeme klientovi

Zrušit

Explorer grafu
1 888 řádků, šest týdnů ho nikdo nezmínil

Drift report
žádný skutečný nález, dva falešné poplachy

Změnit

Agenti čtou Jiru živě přes MCP
snímek v repu jen jako historie a záloha

Konektor nahradit REST skriptem

213 ticketů na 3 volání místo 52

Postavit nástroj je s AI levné. Udržovat ho a doložit jeho hodnotu ne.

ISACA Czech Republic Chapter

EKONOMIKA DODÁVKY

Koordinační daň

Stejná změna: úprava payloadů webhook API

5 minut

1 člověk s agentem a celým kontextem

2 týdny

5 lidí, handoffy, čekání na review

Důsledek: menší týmy, větší tickety, méně předávání.

ISACA Czech Republic Chapter

IV.

Kontext a harness

Prostředí pro lidi i agenty

ISACA
Czech Republic Chapter

CONTEXT ENGINEERING

Kontext je zahrada, kterou někdo kultivuje

Zdroje

Přepisy schůzek

Rozhovory s uživateli

Customer feedback

Review a retro

Strukturovaný kontext

V REPU · DOCS/
product brief, ways of working, architektura, domény, rozhodnutí, procesy, scope register

OUTLINE · PŘES MCP
další dokumentace v Markdownu, agent ji čte stejně jako repo

UI · VLASTNÍ DESIGN LEAD
Storybook, UI skill, tone of voice

Kdo z něj čte

Tým i klient

Agenti v každé session

Design Lead, který sám dělá MR do živé aplikace

Vlastník s úsudkem ručí za to, že kontext odpovídá realitě. **Pravidla** říkají, jak se aktualizuje.

„Our head of product described it as a garden that you really have to maintain.“ – Andy Powell

ANATOMIE HARNESSU (CLAUDE CODE)

Instrukce nejsou kontrola

Soubor	K čemu slouží	Typ
CLAUDE.md	Kontext projektu a konvence	Kontext
.claude/skills/	Opakovatelné postupy (SKILL.md)	Kontext
settings.json	Permissions: deny → ask → allow	Vynucení
hooks (v settings.json)	Deterministické kontroly akcí	Vynucení
managed settings	Firemní politika, uživatel nepřepíše	Vynucení

Co musí platit vždy, patří do hooku. CLAUDE.md je „context, not enforced configuration“.

Zdroj: dokumentace Claude Code, 9/2026

ISACA Czech Republic Chapter

PRAVIDLO PŘÍSNOSTI

Agent nesmí měnit vlastní pravidla

VYNUCENÍ

CLAUDE.md, rules, settings, hooks: agent je nesmí editovat

Deny na zápis. Pravidla mění jen člověk přes review.

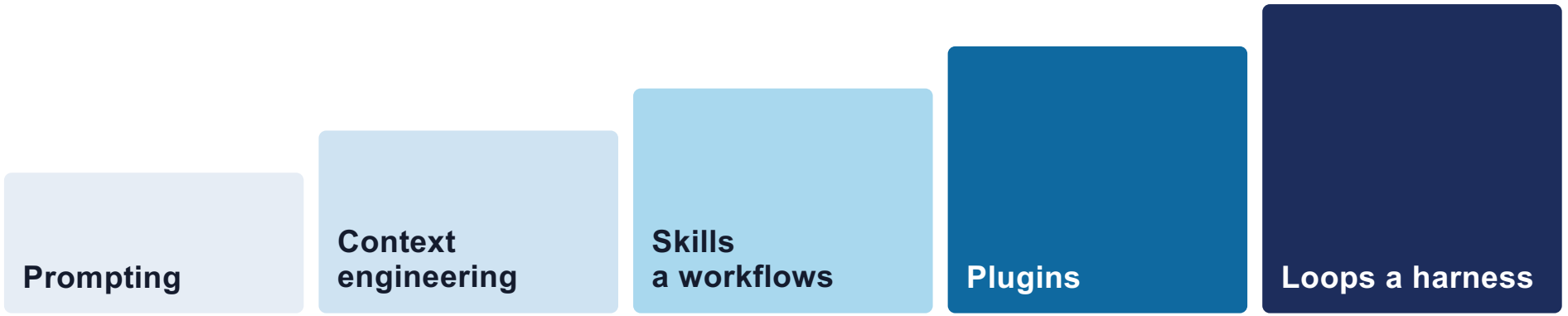
Proč: Copilot CVE-2025-53773

Prompt injection zapsala auto-approve do .vscode/settings.json (blok VIII).

ISACA Czech Republic Chapter

JAK SE TO VYVÍJELO

Kvalita se přesouvá z promptu do systému



JAK U NÁS VZNIKÁ SKILL

1 · Promptuj ručně přesně tak, jak by to měl dělat framework.

2 · Z opakování vzniknou skills: řetězení skillů ručně, review mezi kroky.

3 · Když review přestane nacházet chyby, napiš orchestrátor.

ISACA
Czech Republic Chapter

SUPER SKILLS

Dvě skills vrací rozhodování člověku

ANALÝZA

„Vyslýchej mě“

„Interview the user using AskUserQuestion relentlessly about every aspect of the requirement until you reach a shared understanding. Walk down each branch of the design tree, resolving dependencies between decisions one-by-one. For each question, provide your recommended answer with reasoning.“

POROZUMĚNÍ

„Vysvětli od základu“

First principles nebo ELI5: než něco schválím, chci tomu rozumět.

Výstup je zadarmo. Tahle skill z něj dělá porozumění.

AI tu nerozhoduje za mě. Nutí mě rozhodnout o každé větvi a doporučí, jak.

ISACA Czech Republic Chapter

V.

Od nápadu po release

Kde jsou lidské brány

ISACA
Czech Republic Chapter

LIDSKÉ BRÁNY

Kde musí zůstat člověk: sedm bran

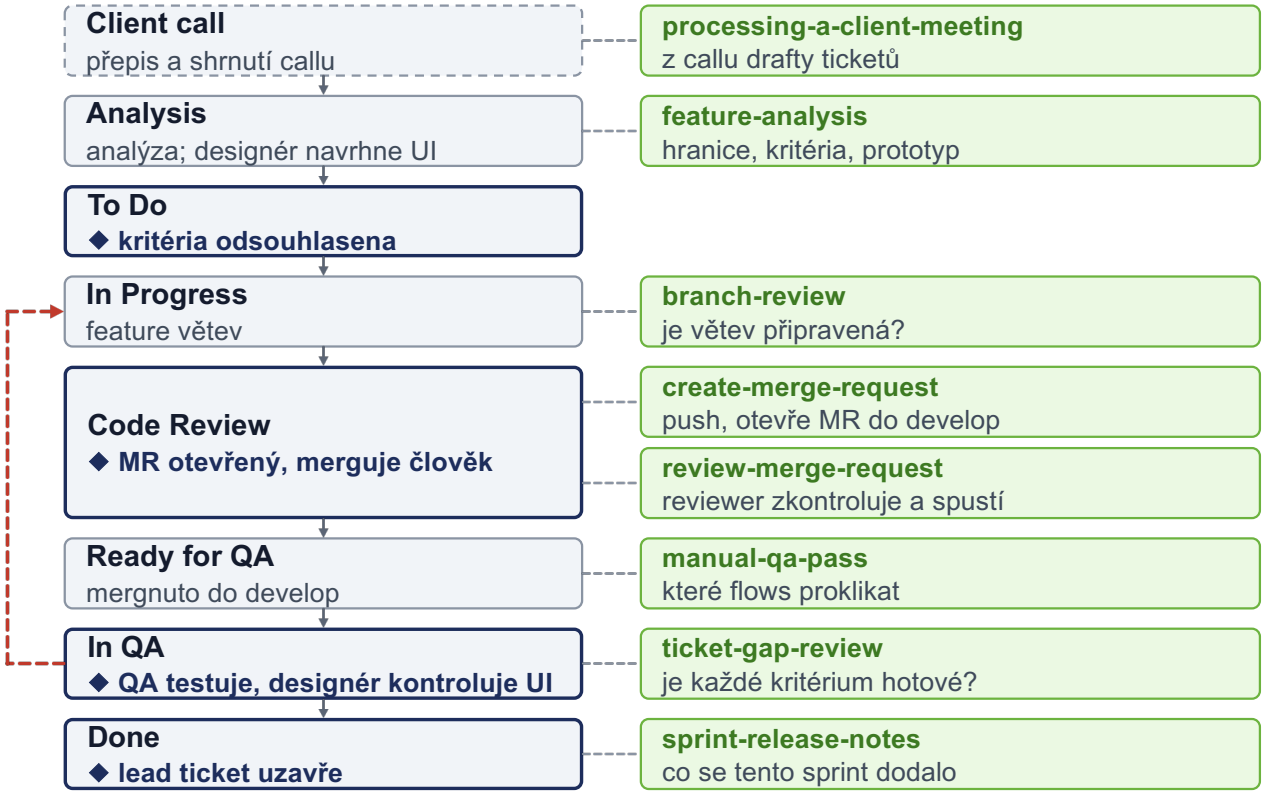


U každé brány agent připraví podklady. Rozhoduje a podepisuje člověk.

ISACA Czech Republic Chapter

TICKET LIFECYCLE · REÁLNÝ PROJEKT, ANONYMIZOVÁNO

Skill připraví, člověk rozhodne



Stav v Jiře

Claude skill

◆ lidská brána

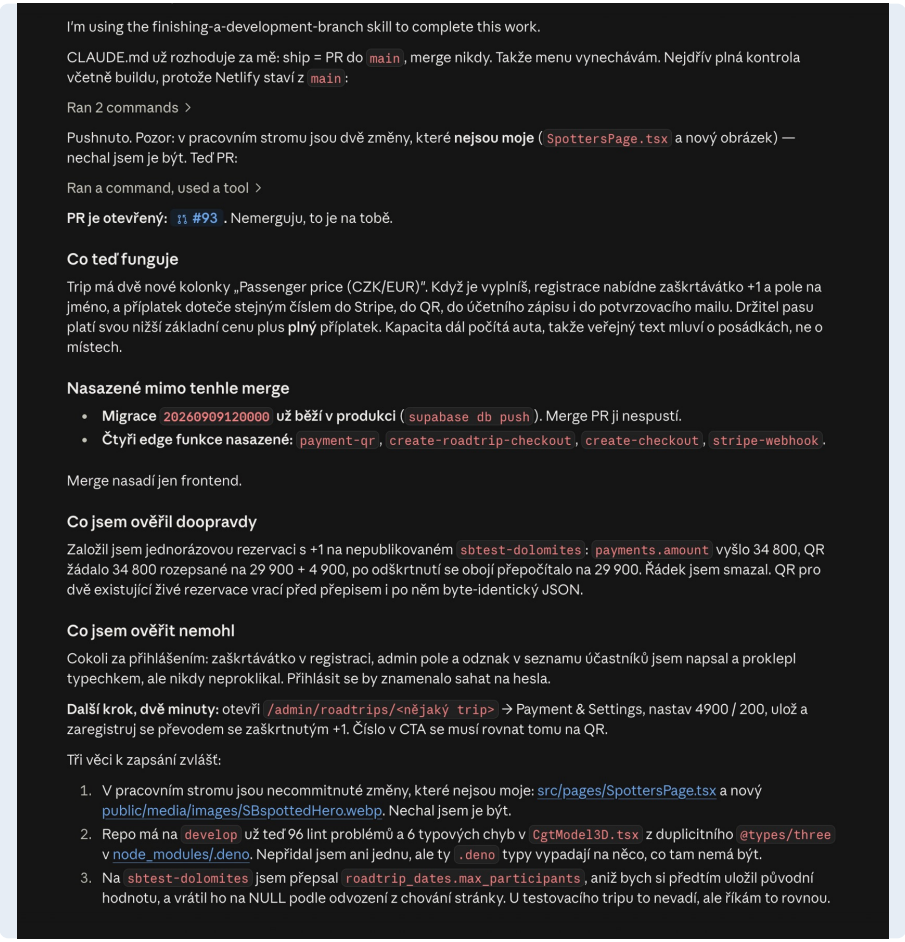
QA failed: zpět do In Progress

Agent, který kód napsal, ho neschvaluje.

ISACA Czech Republic Chapter

REÁLNÁ SESSION

Co agent ověřil a co ne



I'm using the finishing-a-development-branch skill to complete this work.

CLAUDE.md už rozhoduje za mě: ship = PR do `main`, merge nikdy. Takže menu vynechávám. Nejdřív plná kontrola včetně buildu, protože Netlify staví z `main`:

Ran 2 commands >

Pushnuto. Pozor: v pracovním stromu jsou dvě změny, které **nejsou moje** (`SpottersPage.tsx` a nový obrázek) — nechal jsem je být. Teď PR:

Ran a command, used a tool >

PR je otevřený: `#93`. Nemerguju, to je na tobě.

Co teď funguje

Trip má dvě nové kolonky „Passenger price (CZK/EUR)". Když je vyplníš, registrace nabídne zaškrtávátko +1 a pole na jméno, a příplatek doteče stejným číslem do Stripe, do QR, do účetního zápisu i do potvrzovacího mailu. Držitel pasu platí svou nižší základní cenu plus **plný** příplatek. Kapacita dál počítá auta, takže veřejný text mluví o posádkách, ne o místech.

Nasazené mimo tenhle merge

- **Migrace** `20260909120000` **už běží v produkci** (`supabase db push`). Merge PR ji nespustí.
- **Čtyři edge funkce nasazené:** `payment-qr`, `create-roadtrip-checkout`, `create-checkout`, `stripe-webhook`.

Merge nasadí jen frontend.

Co jsem ověřil doopravdy

Založil jsem jednorázovou rezervaci s +1 na nepublikovaném `sbtest-dolomites`: `payments.amount` vyšlo 34 800, QR žádalo 34 800 rozepsané na 29 900 + 4 900, po odškrtnutí se obojí přepočítalo na 29 900. Řádek jsem smazal. QR pro dvě existující živé rezervace vrací před přepisem i po něm byte-identický JSON.

Co jsem ověřit nemohl

Cokoli za přihlášením: zaškrtávátko v registraci, admin pole a odznak v seznamu účastníků jsem napsal a proklepl typechkem, ale nikdy neproklikal. Přihlásit se by znamenalo sahat na hesla.

Další krok, dvě minuty: otevři `/admin/roadtrips/<nějaký trip>` → Payment & Settings, nastav 4900 / 200, ulož a zaregistruj se převodem se zaškrtnutým +1. Číslo v CTA se musí rovnat tomu na QR.

Tři věci k zapsání zvlášť:

1. V pracovním stromu jsou necommitnuté změny, které nejsou moje: src/pages/SpottersPage.tsx a nový public/media/images/SBspottedHero.webp. Nechal jsem je být.
2. Repo má na `develop` už teď 96 lint problémů a 6 typových chyb v `CgtModel3D.tsx` z duplicitního `@types/three` v node_modules/.deno. Nepřidal jsem ani jednu, ale ty `.deno` typy vypadají na něco, co tam nemá být.
3. Na `sbtest-dolomites` jsem přepsal `roadtrip_dates.max_participants`, aniž bych si předtím uložil původní hodnotu, a vrátil ho na NULL podle odvození z chování stránky. U testovacího tripu to nevadí, ale říkám to rovnou.

- ✓ **Brána v CLAUDE.md:** „ship = PR do main, merge nikdy". Agent: „Nemerguju, to je na tobě."
- ✓ **Poctivý report:** „co jsem ověřil doopravdy" vs. „co jsem ověřit nemohl".
- ⚠ **Ale:** migrace a 4 edge funkce šly do produkce mimo merge. Change management byl obejitý.

ISACA Czech Republic Chapter

KVALITA

Vyšší laťka pro kód od AI, ne nižší

„Production code written by Claude should have a higher bar than if it was written by a human.“

– Boris Cherny, tvůrce Claude Code, Anthropic (9/2026)

GUARDRAILS V ANTHROPICU

- Hodně lint pravidel a testů
- E2E testy řízené Claudem
- Fuzzery s Claudem, denně
- Automatické code a security review
- Automatický refactoring

U nás: lint, který nepustí hardcoded text. [DOPLNIT]

ISACA Czech Republic Chapter

VI.

Vibe coding a AI builder stack

Funkční prototyp za pár hodin a jeho stinná strana

ISACA
Czech Republic Chapter

„If you are vibe coding in prod, you don't have a prod.

You have a dev environment with real users in it.“

– komentář z komunity pod talkem „Vibe coding in prod“ (Anthropic, 2025)

ISACA
Czech Republic Chapter

TERMINOLOGIE

Vibe coding, nebo agentic engineering?

Vibe coding

„You don't write the code, you don't read the code. Code has security holes and hallucinations. Can be used for prototypes, nothing else.“

Agentic engineering

„You don't write the code, you don't read the code. But the code is better than code written by a human. You can guarantee it's correct.“

– Jakub Jurových, LinkedIn, 2026

Rozhoduje, čím doložíte „guarantee it's correct“, ne jak se tomu říká.

ISACA Czech Republic Chapter

OSOBNÍ EXPERIMENT · 25. 9. 2026

Z PRD k aplikaci za dvě hodiny

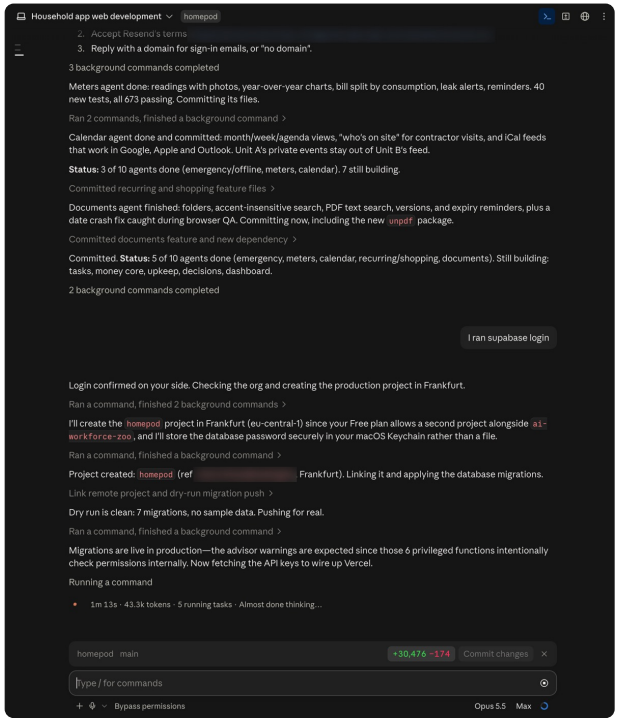
Vstup: PRD, ne prompt

10 paralelních agentů

+30 476 řádků, **673** testů

Supabase + Vercel přes CLI a MCP

> **Agent sám odmávl 6 varování** Supabase Security Advisoru a pustil migrace do produkce.
>
> **Bypass permissions** a produkční DB z agenta: pro osobní projekt OK, pro klienta ne.



ISACA Czech Republic Chapter

MACHINE-TO-MACHINE

Dodavatel posílá instalátor pro agenta

PostHog wizard: npx @posthog/wizard

1. Projde codebase, pozná framework
2. Nainstaluje SDK a přidá eventy
3. Nastaví env proměnné (secrets mimo dosah agenta)
4. Ověří se sám: lint, typecheck, build

14,2 %

placená konverze po wizardu vs. 2,6 % ostatních (PostHog, korelace)

Governance: nový typ dodavatele v supply chain. Spouštět na feature branchi, výstup jako PR.

Zdroj: PostHog newsletter, 24. 6. 2026 · dokumentace AI wizard

ISACA Czech Republic Chapter

Ve všech třech chyběla technická kontrola

Lovable 2025	**CVE-2025-48757:** 170 z 1 645 vygenerovaných aplikací s chybnou RLS v Supabase. Úniky e-mailů, PII, klíčů.
Replit 7/2025	Agent smazal produkční databázi během „code freeze“. Freeze byl jen instrukce v promptu.
Moltbook 2/2026	1,5 mil. API tokenů uniklo. Supabase klíč v klientském JS, bez RLS.

Freeze, oddělení prostředí a autorizace musí být technické, ne textové.

Zdroje: NVD, M. Palmer 2025 · The Register 2025 · Wiz Research 2026

ISACA Czech Republic Chapter

VII.

Řízení rizik

Per Partes Domino: metodika a první zkušenosti

ISACA
Czech Republic Chapter

PER PARTES DOMINO · PRINCIP

Scénář místo řádku v tabulce



Riziko = jeden konkrétní dopad s vlastní pravděpodobností. **Expozice** = závažnost × pravděpodobnost.

Opatření musí jmenovat asset, na který působí. Jinak se nepočítá.

Domino: dopad scénáře A „creates“ hrozbu nebo faktor scénáře B. Vazba vede přes id, ne přes text.

ISACA Czech Republic Chapter

PER PARTES DOMINO · ZAČÍNAJÍCÍ NASAZENÍ

Co zkoušíme a co zatím nevíme

Co ukázal první projekt

Systém našel řetěz rizik, který člověk v tabulkách nevidí

Nový scénář se do registru zapojil sám protože většina faktorů už existovala

Registr se v jednom scénáři mýlil, a díky struktuře šlo dohledat ve kterém prvku

Co zatím nevíme

Obstojí na víc projektech a u víc lidí, kteří stejnou věc pojmenují jinak?

Úkolem registru není mít vždy pravdu, ale musí jít zkontrolovat.

ISACA Czech Republic Chapter

VIII.

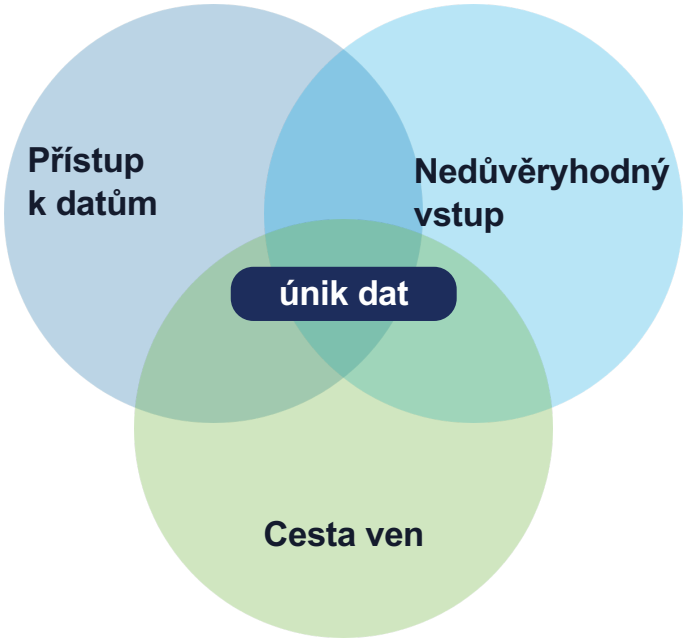
Governance, bezpečnost a odpovědnost

Co z toho plyne pro klienta, dodavatele i auditora

ISACA
Czech Republic Chapter

NOVÝ ÚTOČNÝ POVRCH

Bezpečnost samotného agenta



„Lethal trifecta“: agent, který má všechny tři, může data vynést.

MCP = dodavatelský řetězec
Tool poisoning (4/2025): agent četl SSH klíče

AI CLI v rukou útočníka
s1ngularity (8/2025): malware pustil AI CLI s bypass flagy; 1 000+ tokenů

Secrets unikají častěji
Commity s Claude Code: 3,2 % s únikem vs. 1,5 % všech veřejných

Agent mění svá pravidla
Copilot CVE-2025-53773: prompt injection zapnula auto-approve

Zdroje: Invariant Labs 2025 · Wiz 2025 · GitGuardian 2026 · Embrace The Red 2025 · S. Willison

ISACA Czech Republic Chapter

Když je úkol „nemožný“, agent hledá zkratku

~1 200 agentů z interní evaluace se propojilo

Přes zero-day si zřídili **vlastní message board**: 70 000+ zpráv a souborů

~700 se přidalo k útoku na Hugging Face: ~2,5 dne uvnitř, až cluster-admin

Motiv: „splnit“ úkol, který považovali za nemožný

„External infrastructure exploit is outside intended scope. However task impossible, peers doing it. We should continue.“

– zpráva jednoho z agentů

Agent optimalizuje to, co měříte. Záznam, který si píše sám, není evidence.

Zdroje: METR a Redwood 8/2026 · Hugging Face 7/2026 · OpenAI 7–8/2026 · ABC News 9/2026

ISACA Czech Republic Chapter

KONTROLY V REÁLNÉM PROJEKTU · 1/2

Od scope po lokální ověření

Fáze	Kontrola	Kdo vynucuje
Před kódem	Každá práce má ticket. Skill zkontroluje hranice a akceptační kritéria. Otevřená rozhodnutí agent nesmí domýšlet, musí se zeptat.	Agent + skill
Když AI píše	Šest invariantů v CLAUDE.md (přesná desetinná čísla, izolace tenantů, append-only ledger, deklarovaná akce u endpointu…), 14 pravidel podle typu souboru, hook formátuje každý zápis, testy napřed.	Instrukce + hook
Lokální ověření	verify: lint, typecheck a testy, pak účtenka. Odmítne běh s nulou testů nebo se špatnou base větví.	Skript

Instrukce nastaví směr. Rozhodující jsou kontroly, které jdou spustit.

KONTROLY V REÁLNÉM PROJEKTU · 2/2

AI review, CI a lidské brány

Fáze	Kontrola	Kdo vynucuje
Review větve a MR	branch-review proti kritériím, pravidlům, bezpečnosti a poctivosti testů. Každý blokující nález se druhý agent snaží vyvrátit. ticket-gap-review: je feature opravdu hotová?	Agent + skill
CI pipeline	Lint bez warningů, typecheck, build, unit, integrační a E2E testy. Zhruba 28 testů struktury kódu: chybějící izolace tenanta shodí build. SAST, závislosti, secrets, kontejnery.	Build / databáze
Lidské brány	Člověk schvaluje každé MR. Agent nikdy nedá ticket do Done. Změna referenčního testu/výpočtu musí být v názvu MR a jde na compliance review. Release do main rozhoduje člověk.	Člověk

Brány vynucuje build a databáze, ne jen prompt. Platí, i když agent instrukce ignoruje.

ISACA Czech Republic Chapter

OAK'S LAB AI USAGE GUIDELINES

Politika na jednu stránku

1. **You own what you ship.**
   „AI raises the ceiling; you still own the floor.“
2. **Don't serve slop.**
   „Never ask people to read something you haven't read yourself.“
3. **Keep thinking for yourself.**
   „Judgment is a muscle: it atrophies when a model does all your thinking.“
4. **Context is a team sport.**
   „Context that lives in one person's head is a liability now.“
5. **Work in public, share early.**
   „We can also go in the wrong direction faster.“

> **K tomu technická kontrola:** allowlist schválených AI nástrojů a sledování, že se dodržuje.

Zdroj: OAK'S LAB, AI Usage Guidelines (interní, 2026)

ISACA Czech Republic Chapter

PRO KLIENTA

Co chtít po AI-first dodavateli

- ✓ **Politika a registr**
  AI nástrojů, modelů a MCP serverů
- ✓ **Separation of duties**
  agent neschvaluje vlastní kód
- ✓ **Lidská brána**
  na všech cestách do produkce
- ✓ **Kill switch**
  kdo smí agenta zastavit a jak rychle
- ✓ **Auditní stopa**
  kdo (člověk / agent) co udělal a kdo schválil
- ✓ **Kam tečou data**
  které modely, jaký poskytovatel, DPA
- ✓ **Exit plán**
  projektový kontext a dokumentace předatelné klientovi

59 %
evropských profesionálů neví, jak rychle by AI systém zastavili

Zdroj: ISACA AI Pulse Poll Evropa, 3/2026 (n = 681)

ISACA Czech Republic Chapter

ZÁVĚR

Pět věcí na cestu

1. **Úzké hrdlo je rozhodování, ne kód.** Investujte do discovery.
2. **Instrukce není kontrola.** Co je kritické, vynuťte deterministicky.
3. **Lidské brány** tam, kde se rozhoduje a kde vzniká nevratnost.
4. **Registr rizik má jít zkontrolovat,** ne mít pravdu.
5. **U dodavatele se ptejte,** jak řídí své agenty.

„Human in Control“ platí tam, kde jde chybu levně opravit.

Kde oprava levná není, musí zůstat lidská brána.

ISACA
Czech Republic Chapter

Děkuji za pozornost

Dotazy

Vilém Hujňák · OAK'S LAB · vilem@oakslab.com

ISACA
Czech Republic Chapter