

Governance for AI-agenter: fra usynlig arbejdskraft til styret system

*En praktisk model for virksomheder,
der har flere AI-agenter end de tror.*

Fem søjler, ét konkret værktøj (agent-passportet), ét arkitekturprincip (kontekst med review) og en tjekliste at starte på i denne måned. Ikke for at bremse agenterne, men for at kunne sige ja til flere af dem, hurtigere, uden at miste nattesøvnen.

Din virksomhed har allerede AI-agenter i drift. Nogle har du selv sat i gang. Andre fulgte med i sidste opdatering af jeres SaaS-værktøjer. Og nogle har medarbejdere selv koblet til, med adgang til rigtige data og uden at nogen har skrevet det ned.

Gartner forudser at 40 procent af enterprise-applikationer har task-specifikke agenter inden udgangen af 2026, op fra under 5 procent i 2025. Skiftet er ikke på vej. Det er sket.

De fleste organisationer kan i dag ikke besvare fem enkle spørgsmål: Hvilke agenter kører? Hvem ejer dem? Hvad har de adgang til? Hvordan slukker vi én af dem, nu? Og kan vi bevise alt det overfor en revisor?

FORMÅLET MED GOVERNANCE

Ikke at bremse agenterne, men at kunne sige ja til flere af dem, hurtigere, uden at miste nattesøvnen.

Den nye risikoklasse har hænder

Skygge-IT var i mange år et overskueligt problem: en afdeling købte et værktøj udenom IT, og værste konsekvens var som regel spildte licenskroner og et datasæt det forkerte sted.

Skygge-agenter er en anden kategori. En agent med skriveadgang kan oprette, ændre og slette. Den kan handle på tværs af systemer via API'er og MCP-forbindelser. Den kan blive prompted til noget dumt af en velmenende kollega. Og den efterlader kun spor, hvis nogen har sørget for logning.

Branchens egen litteratur er bemærkelsesværdigt enig om diagnosen: en stor del af organisationerne monitorerer efterhånden deres AI-brug, men langt færre kan afgrænse hvad en agent må røre, og færre endnu kan slukke en konkret agent med det samme. Gabet mellem "vi kan se det" og "vi kan styre det" er 2026's mest undervurderede driftsrisiko.

Agenterne er den bedste produktivitetsnyhed i årevis. Problemet er at de fleste organisationer har givet en ny type medarbejder adgang til produktionssystemer uden ansættelseskontrakt, uden chef og uden personalemappe.

De fem søjler i agent-governance

På tværs af AgentOps-tænkningen udkrystalliserer fem søjler sig. De er ikke eksotiske. De er klassisk god IT-drift, anvendt på en ny arbejdsstyrke:

- **Inventar.** Man kan ikke styre det, man ikke kan se. Alle agenter, interne, indlejrede i SaaS, og tredjeparts, registreres ét sted, med formål og ejer. Ikke i et regneark, men i en model der ved hvad agenten er forbundet til.

- **Identitet.** Hver agent har sin egen identitet og sine egne nøgler. Delte servicekonti er governance-mørke: når alle skriver som "system", har ingen skrevet noget.
- **Mindst mulig adgang.** En agent får adgang til det, dens formål kræver, og ikke mere. Formålet er bindende: en agent der beriger systemkortet, har intet at gøre i lønsystemet.
- **Observérbarhed.** Alt en agent læser, foreslår og udfører, logges. Loggen er den evidens, alle senere spørgsmål besvares med.
- **Løbende compliance.** Klassifikationer, adgange og ejerskab reviewes på kadence, ikke ved årsrevision. Agenter ændrer sig med hver modelopdatering; det skal tilsynet også.

Søjlerne er ikke fem projekter. I en levende model er de fem egenskaber ved samme system.

03 · KAPITEL 3

Agent-passportet

Det konkrete værktøj, der gør søjlerne operationelle, er passportet: en struktureret profil pr. agent, som first-class borger i arkitekturmodellen på linje med systemer og data. Et agent-passport i Atlas indeholder:

- **Formål** (purpose binding): hvad agenten er sat i verden for, formuleret så en revisor kan læse det.
- **Ejer:** et menneske med navn og ansvar. Ingen ejer, ingen agent.
- **Tilladte systemer og data:** relationer i grafen til de applikationer, integrationer og datasæt agenten må røre. Ikke prosa, men faktiske koblinger.
- **Kill-switch-status:** hvordan agenten standses, og hvornår det sidst er efterprøvet.
- **Review-kadence:** hvornår passportet sidst er bekræftet, og hvornår det forfalder.
- **Provenance:** hvor agenten kommer fra, og hvilken AI-model den kører på.

Fordi passportet bor i grafen og ikke i et dokument, kan det svare på det spørgsmål intet regneark kan: **hvad er blast-radius?** Vælg en agent, og se hele kæden: hvilke systemer den når, hvilke data de systemer rummer, hvilke processer de data driver. "Hvad kan denne agent røre?" bliver et opslag med et billede, ikke en workshop.

Og fordi modellen er levende, opdager den selv kandidater: nye AI-features i eksisterende systemer, usage-signaler der ligner en ikke-registreret assistent, forbindelser ingen har meldt ind. Skygge-agenter flyttes fra anekdote til indbakke.

04 · KAPITEL 4

Vend arkitekturen om: kontekst med review

Standardmønstret i markedet er at gøre alle systemer læsbare for agenter: hver leverandør udstiller en MCP-server, hver agent kobler sig på, og konteksten flyder frit. Det løser produktivetsproblemet og skaber governance-problemet: hundrede forbindelser, ingen samlet viden om hvem der spurgte om hvad.

Det omvendte mønster er stærkere: **giv agenterne ét sted at spørge, og lad det sted have regler.** I Atlas hedder det MCP Context Hub. Organisationens agenter spørger Atlas om organisationens sandhed: hvilket

system ejer kundedata, hvem godkender ændringer i betalingsflowet, hvilke apps understøtter denne kapabilitet. Og reglerne er indbygget:

- **Læsninger** besvares fra den typede graf, med kildehenvisninger. Agenten citerer modellen, den digter ikke.
- **Skrivninger** bliver aldrig udført direkte. De bliver til ændringsforslag, der lander i Verify-indbakken og venter på et menneske. Write-with-review er standardindstillingen, ikke en tilvalgs-feature.
- **AI trafik logges** pr. agent-identitet og bliver automatisk til evidens i agentens passport. Agenter der bruger hubben, er pr. definition synlige.

Atlas governer agenterne og serverer dem, i samme bevægelse. Governance er ikke et gebyr agenterne betaler. Det er infrastrukturen der gør dem brugbare.

05 · KAPITEL 5

Politikker, der arbejder i realtid

Årshjuls-governance er designet til et tempo, hvor mennesker laver ændringerne. Agenter laver flere, mindre ændringer, hele tiden. Tilsynet må derfor flytte fra kalenderen til hændelsesstrømmen.

I Atlas evaluerer arkitektur-politikker forslagene, når de opstår: ufarlige forslag (en berigelse af metadata, en åbenlys dubletmarkering) kan auto-godkendes med log. Følsomme forslag (nye adgange, ændringer i kritiske systemer, alt der rører persondata) flagges og kræver menneskelig godkendelse.

Og det vigtigste, som forbløffende få systemer har: **et sted hvor nej'et bor**. En agent, hvis forslag konsekvent afvises, er et signal. En agent uden aktivitet i tre måneder er et signal. En agent hvis adgang vokser stille, er et signal. Politiklaget samler signalerne, så mennesket med ansvaret faktisk kan udøve det.

Resultatet er kontinuerligt review i stedet for årlig arkæologi: ugens delta pr. domæne, genereret af systemet, behandlet af mennesker på en halv time.

06 · KAPITEL 6

Evidens: fra “stol på os” til “se selv”

Governance uden evidens er stemning. Tre modtagere skal kunne betjenes direkte fra systemet:

Tilsyn og revision.

EU AI Act er blevet mere overkommelig for midtfeltet: Digital Omnibus (godkendt af Europa-Parlamentet 16. juni 2026) udså high-risk-forpligtelserne til 2. december 2027 og udvidede lempelsesregimet til virksomheder op til 750 ansatte eller 150 millioner euro i omsætning. Men overkommelig er ikke det samme som frivillig: inventar, klassifikation og dokumentation skal stadig findes. I Atlas genereres AI Act-dokumentationen fra registret og passporterne, med provenance-stemplet rationale pr. klassifikation.

Bestyrelsen.

Boards beder i stigende grad om ét samlet narrativ: hvad har vi af AI, hvad koster det, hvad gør det ved risikoen, og hvad får vi ud af det. Boardroom views og board pack trækker fortællingen direkte fra modellen, og ROI-ledgeren kobler hver use-case til en værdihypotese og realiseret værdi over tid, i enheder en CFO

accepterer. Relevant baggrundstal, verificeret: kun omkring en tredjedel af CIO'er kan i dag konsekvent bevise finansielle AI-outcomes, mens AI-forbruget vokser cirka 35 procent årligt. Den der møder op med en ledger i stedet for en fornemmelse, ejer samtalen.

Organisationen selv.

Den undervurderede modtager. Når medarbejdere kan se hvilke agenter der findes, hvad de må, og hvem der ejer dem, falder både frygten og fristelsen til at bygge udenom. Synlighed er den billigste adfærdsregulering, der findes.

07 · KAPITEL 7

Kom i gang: tjeklisten

Governance-programmer dør af omfang. Start med det, der kan gøres i denne måned:

- **Lav inventaret, sjusket.** Skriv de agenter ned, I kender: købte, byggede, indlejrede. Accepter at listen er ufuldstændig; det er den hos alle.
- **Giv hver agent en ejer.** Ét navn pr. agent. De agenter, ingen vil eje, har lige fortalt jer noget vigtigt.
- **Skriv formålet ned.** Én sætning pr. agent. Kan formålet ikke formuleres, kan adgangen ikke begrundes.
- **Find kill-switchen.** Ved I, hvordan hver agent standses? Prøv det på én af dem. Alvorligt talt: prøv det.
- **Kanalisér konteksten.** Beslut at agenter fremover henter organisationsviden ét sted, og at skrivninger går gennem review. Det er dagen, governance holder op med at være et dokument.
- **Sæt kadencen.** Kvartalsvis passport-review pr. agent. En halv time. Kalenderen er halvdelen af al governance.

Kan I sætte flueben ved de seks, er I foran de fleste. Og I har fundamentet, resten af rejsen bygger på: flere agenter, mere autonomi, samme ro i maven.

NÆSTE SKRIDT

Se hele flowet: opdagelse, passport, review og evidens.

Atlas' demo-workspace indeholder en realistisk AI-portefølje, inklusive et Annex III-højrisiko-eksempel og en skygge-agent, så du kan se hele flowet fra opdagelse til evidens.

Prøv Atlas

Tal med os om EA

ATLAS.SPEKIR.COM · HELLO@SPEKIR.COM

OM SPEKIR

Spekir er et dansk produkthus med ét fokus: at give virksomheder i midtfeltet den arkitektur-kapacitet de store køber sig til med dedikerede teams. Atlas er Spekirs platform: det governede kontekstlag for den agentiske virksomhed.

KILDER

Gartner (26/8-2025): 40% af enterprise-apps får task-specifikke agenter ultimo 2026, fra <5% i 2025.
Europa-Parlamentet, Digital Omnibus (16/6-2026): Annex III udskudt til 2/12-2027; lempelsesregime udvidet til 750 ansatte / EUR 150M (Travers Smith, Latham & Watkins, Morgan Lewis, Stibbe, DLA Piper).
Gartner CIO Agenda 2026: 33% beviser konsekvent finansielle AI-outcomes; AI-spend ca. +35% YoY.
MCP-adoption 2026: 97M installationer; 78% af enterprise AI-teams i produktion. Kvalitative udsagn om monitorerings- og containment-gab bygger på AgentOps-brancheanalyser og er gengivet uden procenttal.