

Samen aan het Stuur: wat bronnen zeggen over een programma digitalisering waarin een bouwteam samen met de business en de werkvloer bouwt, met privacy en security erin vanaf het begin

Dit is het onderzoeksstuk achter deze site: versie 0.4, een concept ter beoordeling. Het is deels gecontroleerd tegen de bronnotities (de bevindingen uit versie 0.3 vier keer, de nieuwe zinnen van versie 0.4 één keer) en niet tegen de oorspronkelijke bronnen. Een PDF-versie om te lezen of te printen staat in [onderzoeksstuk.pdf](#). De bronnen zelf, met leescode en type, staan op [Bronnen](#); de volledige referentielijst staat onderaan deze pagina.

Onderzoeksstuk bij een gedachtevoer-stuurmodel. Versie 0.4, 19 oktober 2026. Status: concept ter beoordeling; herkadring van versie 0.3 (zie onderzoek/wijzigingslog-v0.4.md). De bronnen en bevindingen zijn die van versie 0.3 (vier claimcontroles); de nieuwe en gewijzigde zinnen van versie 0.4 hebben nog geen eigen claimcontrole gehad. Geschreven voor bestuurders en directie van organisaties als een VVT-instelling of een gemeente. Dit stuk is geen besluit, geen implementatieplan en geen juridisch advies.

Samenvatting

Medewerkers gebruiken generatieve AI al, deels met een niet-zakelijk account op bedrijfsapparaten. Volgens het rapport wijst dat op gebruik buiten beleid (Verizon Business, 2025; een leveranciersrapport). Dit stuk onderzoekt een denkwijze, Samen aan het Stuur: een programma digitalisering waarin een eigen bouwteam, met AI-hulpmiddelen als Claude Code, samen met de business en de werkvloer nieuwe hulpmiddelen ontwikkelt. Iemand stuurt en neemt collega's mee in adoptie, veiligheid, privacy en wat wel en niet mag; privacy en security zitten er vanaf het begin in. Medewerkers bouwen niet zelf. Awareness zou dan een gevolg van samen ontwikkelen worden, geen losse les. Het is geen systematische review. Het steunt op 97 bronnotities, deels volledig en deels gedeeltelijk gelezen (hoofdstuk 2).

De bronnen beschrijven of bepleiten losse bouwstenen: betrokkenheid en coaching bij verandering, psychologische veiligheid als voorwaarde, ondersteuning die meekijkt en een risicogestuurde

controle. Voor de laatste twee is geen effectonderzoek gelezen. Enkele kleine, deels niet-peer-reviewde studies wijzen er bovendien op dat AI-hulp niet vanzelf sneller, veiliger of leerzamer is.

Geen gelezen bron toetst de kernhypothese (H3): dat samen ontwikkelen privacy-, security- en AI-gedrag beter aanleert dan een les of een loket. Er is ook geen bewijs uit VVT-instellingen of gemeenten, en veel bronnen zijn preprint, leveranciersrapport of alleen als abstract gelezen. Drie gaten zijn nadrukkelijk open: of inbouwen vanaf het begin goedkoper is dan achteraf toevoegen, hoe een bouwteam en de business in zorg of gemeenten samenwerken, en hoe beheer na oplevering verloopt. Het stuurmodel (vier fasen, zes verschuivingen en zes stappen van signaal tot delen) is daarom een voorstel; een extra bronnenronde over die drie gaten is nuttig. Een geanonimiseerd voorbeeld (casus A) illustreert het, maar bewijst niets. Het stuk sluit af met een kleine proef om H3 te toetsen en met open vragen voor de functionaris gegevensbescherming (FG) en een jurist.

1 Inleiding en vraagstelling

Uitgangspunt van dit stuk, dat hier niet met een bron wordt onderbouwd: organisaties in de zorg en bij gemeenten moeten het niveau van privacy, informatiebeveiliging en AI-gebruik verhogen. Een awarenessprogramma of campagne lijkt een veelgekozen route (ICTU, n.b.; een brochure, zonder cijfer).

Tegelijk wijzen twee leveranciersrapporten erop dat medewerkers AI al op eigen initiatief gebruiken. Volgens browsermonitoring van een datapartner van Verizon Business (2025) gebruikte 15% van de medewerkers regelmatig generatieve AI op bedrijfsapparaten; elders in het rapport staat 14%. In een enquête van Microsoft en LinkedIn (2024) nam 78% van de AI-gebruikers eigen AI-hulpmiddelen mee naar het werk.

Die cijfers gaan over alle sectoren, respectievelijk kenniswerkers wereldwijd. Ze zeggen niets specifiek over zorg of gemeenten: Verizon heeft een aparte zorgparagraaf, maar die is hier niet gebruikt. Een voorzichtige conclusie is dat niets doen niet vanzelf betekent dat er niets gebeurt. Of dit gebruik tot schade leidt, laten deze bronnen niet zien.

Het idee dat hier wordt onderzocht, is een alternatief voor de les en voor het loket (informeren en verzoeken indienen). Een programma digitalisering, of een nieuwe afdeling voor nieuwe behoeften, bouwt met AI-hulpmiddelen kleine hulpmiddelen, samen met de business en de werkvloer.

Medewerkers bouwen niet zelf: zij brengen de behoefte in, denken mee in sessies, testen en nemen over. Iemand stuurt en neemt collega's meteen mee in adoptie, veiligheid, privacy en wat wel en niet mag, en de communicatie loopt twee kanten op. Adviseurs voor privacy, security en AI kijken vanaf het begin mee, zodat die onderwerpen geen apart traject achteraf worden. Wie die adviseurs precies zijn, bepaalt elke organisatie zelf. Dat awareness hieruit volgt is onze kernhypothese (projectcontext, geen bronbevinding).

Hoofdvraag. Wat zeggen de gelezen bronnen over de bouwstenen van zo'n stuurmodel, en wat zeggen ze er niet over?

Deelvragen. (1) Wat is bekend over betrokkenheid bij verandering, zelfsturing en psychologische veiligheid (achtergrond: dit model laat de werkvloer niet zelf sturen of bouwen)? (2) Over bouwteams en ondersteunende diensten die samen met anderen ontwikkelen, en over co-creatie? (3) Over de invloed van trainingen en andere interventies op privacy- en securitygedrag? (4) Over AI als medebouwer, risico's van AI-gebruik door medewerkers en guardrails bij zelf bouwen? (5) Hoe laat zich daarop een stuurmodel formuleren, en welke proef is nodig voor wat de bronnen niet beantwoorden?

Hypothese H3. Samen ontwikkelen binnen kaders (bouwteam, business en werkvloer) leert medewerkers privacy-, security- en AI-gedrag beter aan dan een les of een loket. Dit is een hypothese; niets in dit stuk toont aan dat zij klopt.

Begrippen. 'Bouwteam': de afdeling of het programma dat de hulpmiddelen ontwikkelt. 'Stuurder': het aanspreekpunt dat de richting bewaakt en collega's meeneemt. 'Business en werkvloer': de collega's die behoeften inbrengen, meedenken, testen en overnemen; zij bouwen niet zelf. 'Adviseurs': privacy, security en AI, in een invulling per organisatie. 'Bouwer': wie het hulpmiddel maakt (in dit model het bouwteam). 'Bestuur': bestuurders en directie, ongeacht organisatietype.

Kader: Hoe sterk is dit bewijs?

Kernregel. Hoe sterker de opzet van een bron, hoe meer een cijfer zegt over oorzaak en gevolg. Bij een zwakke opzet, een alleen-abstractlezing of een bron met een belang is een cijfer een aanwijzing en geen bewijs. In de tekst staat bij een bron wat het cijfer betekent en waar het ophoudt. Wat voor bron het is, staat in dit kader. Een voorbehoud dat de richting van een zin verandert, zoals 'zelfselectie kan dat verklaren', staat altijd in de zin zelf.

Soort bron	Wat het kan laten zien	Wat het niet laat zien	Voorbeelden in dit stuk
Onderzoek met controle (gerandomiseerd of vergelijkende opzet)	Een verschil tussen groepen, mits klein en goed opgezet ook een oorzaak	Of het buiten de onderzochte groep, taak en periode ook geldt	Ho e.a.; Lain e.a. (preprint); J. Becker e.a. (preprint); Perry e.a.; Shen en Tamkin (preprint); Zhao e.a. (modellen, geen mensen)

Soort bron	Wat het kan laten zien	Wat het niet laat zien	Voorbeelden in dit stuk
Onderzoek zonder controle (interviews, enquêtes, casussen, reviews van zulke studies)	Wat mensen ervaren of zeggen; patronen en voorwaarden	Effect: zonder vergelijking is oorzaak niet vast te stellen	Weerheim e.a.; Demjaha e.a.; Q-Consult; Li e.a.; Kunnen e.a.; Clarke e.a.; Hegedüs e.a.
Alleen abstract of recordpagina gelezen	Wat de auteurs zelf als hoofdresultaat melden	Methode, effectgrootte, vergelijkingsgroep en beperkingen	Silic en Lowry; Deng e.a.; Viljoen e.a.; Salvatore; Bennion e.a.
Preprint	Een voorlopig resultaat dat nog beoordeeld moet worden	Dat het resultaat de beoordeling doorstaat	J. Becker e.a.; Lain e.a.; Shen en Tamkin; Spracklen e.a.; Ong e.a.; Deng e.a.
Leveranciersrapport (bedrijf met een commercieel belang)	Dat een verschijnsel voorkomt	Onafhankelijke omvang, oorzaak of gevolg; zorg en gemeenten	Verizon; IBM/Ponemon; Microsoft en LinkedIn; DORA (Google Cloud); Microsoft Learn; Anthropic
Journalistiek	Een voorbeeld of signaal	Hoe vaak iets voorkomt; volledigheid	NOS; Binnenlands Bestuur; Fortune; The Register
Overheidsdocument of richtlijn	Wat een toezichthouder of overheid vindt of verwacht	Dat de aanpak werkt: een standpunt is geen effectonderzoek	AP; NCSC; VNG; Bennink en Drukarch (JenV); wetteksten

De tweede tabel geeft per kernbron de opzet, de sterkte en wat de bron niet laat zien. De sterkte-oordelen zijn een eigen inschatting op basis van de bronnotities.

Bron	Opzet en omvang	Sterkte	Wat het niet laat zien
Ho e.a. (2025)	Gerandomiseerd veldexperiment, 19.500 medewerkers, één zorgbedrijf, acht maanden	Sterk voor klikgedrag op phishing	Controle voor jaarlijkse training; samen bouwen
Lain e.a. (2022)	Gerandomiseerd veldexperiment, ruim 14.000 medewerkers, één bedrijf, 15 maanden; preprint	Sterk voor waarschuwingen en meldknop	Verplichte training; waarschuwingen buiten gesimuleerde mails
Silic en Lowry (2020)	Veldstudie, 420 deelnemers, zes maanden, één organisatie; alleen abstract	Zwak	Effectgrootte, vergelijking met klassieke training, aard van de meting
Freeman e.a. (2014)	Meta-analyse, 225 studies, bachelor-STEM-onderwijs	Sterk, maar andere context	Werkgedrag; bouwen
J. Becker e.a. (2025)	RCT, 16 ervaren ontwikkelaars, 246 taken; preprint	Matig: klein	Niet-programmeurs; veiligheid
Perry e.a. (2023)	Experiment, 47 deelnemers, vooral studenten; model uit 2022	Matig: samengestelde $p = 0,056$	Actuele agents; zorgcontext
Shen en Tamkin (2026)	Experiment, 52 ontwikkelaars; preprint, auteurs aan Anthropic verbonden	Matig: kleine groepen per gebruikspatroon, achteraf ingedeeld	Werkresultaat; menselijke hulp
Zhao e.a. (2026)	Benchmark, 186 taken, agents zonder mens	Sterk voor modellen, geen mensen	Review door een mens; kleine interne hulpmiddelen
Weerheim e.a. (2018)	18 interviews, twee teams, één ggz-organisatie	Zwak: mogelijk positieve selectie, geen uitkomsten	Effect; vergelijking

Bron	Opzet en omvang	Sterkte	Wat het niet laat zien
Verizon, IBM, Microsoft en LinkedIn	Leveranciersrapporten, alle sectoren	Alleen aanwijzing dat gebruik bestaat	Zorg, gemeenten, schade

2 Werkwijze

Zoeken. De bronnen komen uit meerdere zoekrondes in het project (verkenning 1 tot en met 4, de laatste met circa 230 kandidaten, met overlap) en uit gerichte zoekopdrachten naar wetenschappelijke artikelen, toezicht- en overheidsdocumenten, bedrijfsrapporten en nieuws. Er was geen vooraf geregistreerd zoekprotocol en geen dubbele selectie. Dit is dus geen systematische review. Kandidaten die alleen als zoekresultaat zijn gezien (code C) of niet bereikbaar waren (X) zijn niet als onderbouwing gebruikt.

Lezen. Elke gebruikte bron heeft een bronnotitie met bibliografische gegevens, kernpunten met pagina of sectie, methode en beperkingen. De meeste notities bevatten ook korte teruggezochte citaten; bij een aantal notities (onder meer Demjaha, Bennion, Salvatore en enkele nieuwsberichten) ontbreken die, en bij Li zijn ze nog te controleren. Dit stuk is geschreven op basis van die notities en niet op een nieuwe lezing van de oorspronkelijke bronnen.

De notities zijn met AI-hulpmiddelen opgesteld: meerdere vermelden dat een samenvattend model de tekst leverde. Er is geen log van een steekproefcontrole, dus de omvang van eventuele controle is niet vast te stellen. Fouten in de notities werken door.

Leescodes. De bibliotheek telt 97 bronnen.

Code	Betekenis	Gebruik hier
A	Volledige tekst zelf gelezen	Onderbouwing
B	Deels gelezen	Onderbouwing met voorbehoud, in de tekst gemarkeerd met (B)
C / X	Alleen zoekresultaat / niet bereikbaar	Niet gebruikt

Telling	Code A	Code B
Volgens de index (bibliotheek/index.md)	40	57
Volgens de notities (indicatief)	44	53

De telling volgens de notities is de index, gecorrigeerd voor zes afwijkingen tussen notitie en index. Becker e.a. (2017), Freeman e.a., Ong e.a., Vandekerckhove e.a. en Voorberg e.a. zijn A in de notitie en B in de index; DORA (2026, Platform engineering) is B in de notitie en A in de index. Niet elke notitie noemt een expliciete code (43 niet), dus beide tellingen zijn indicatief.

'Deels gelezen' betekent drie dingen.

Soort	Bronnen
Alleen abstract of recordpagina	Deng e.a. (2026); Viljoen e.a. (2024); Binzer en Winkler (2022); Ajimati e.a. (2025); Salvatore (2024); Bennion e.a. (2024); Silic en Lowry (2020)
Tekst door een ophaaltool samengevat	De nieuwsberichten (NOS, Binnenlands Bestuur, Fortune, The Register); Li e.a. (2026); Alqheedan en Alzughaibi (2026); Demjaha e.a. (2024)
Gedeeltelijk gelezen hoofdtekst	Onder meer J. Becker e.a. (2025); Perry e.a. (2023); Shen en Tamkin (2026); Zhao e.a. (2026); Edmondson en Bransby (2023); Hegedüs e.a. (2022); Verizon Business (2025); IBM (2025)

Selectiecriteria. Een bron kwam in aanmerking als zij iets zegt over een bouwsteen van het stuurmodel, met code A of B. Zwakke bronnen zijn niet geweerd maar benoemd. Bedrijfsrapporten en leveranciersdocumentatie zijn vendor-gelieerd en tellen niet als onafhankelijk bewijs. Ze gelden alleen als aanwijzing, niet als onafhankelijk bewijs (zie het kader in hoofdstuk 1). Nieuws is alleen anekdotisch gebruikt.

Beperkingen. De bewijsbasis is divers en vaak indirect: software-ontwikkelaars, studenten, kenniswerkers, medewerkers van bedrijven, een Amerikaans zorgbedrijf en ziekenhuizen, Britse overheidsdiensten en een Nederlandse ggz-organisatie. Overdracht naar VVT en gemeenten is een aannname. Meerdere bronnen zijn preprints. Cijfers zijn overgenomen uit de bronnotities, met eenheid en groep waar de notitie die noemt. In versie 0.1 waren enkele cijfers te ruim geformuleerd (onder meer Freeman, Bennion, Verizon en Ho); dat is hersteld. De notities zelf zijn niet opnieuw aan de oorspronkelijke bronnen getoetst.

Het eigen kaderwerk (risicoladder 0 tot 3, PDCA met kaderstappen) komt uit het strategievoorstel voor de VVT (strategie/strategie-vvt.md, een eigen projectdocument). Het is een voorstel en geen bronbevinding.

3 Bevindingen

Leeswijzer bij versie 0.4. Een deel van deze bronnen gaat over teams die zelf sturen (3.1) of medewerkers die zelf bouwen (3.6, 3.8). Dit model kiest daar bewust niet voor: het bouwteam bouwt. De bronnen zijn behouden om wat ze zeggen over betrokkenheid, risico's en kaders, en over wat er misgaat als niet-professionals of AI zonder controle bouwen.

3.1 Teamgestuurde verandering en zelfsturing

Een kwalitatieve review van 24 studies in zorgorganisaties over het volhouden van lean (continu verbeteren) vond 21 bevorderende en 17 belemmerende factoren (Kunnen e.a., 2023). Bevorderend waren een verbeter- en leercultuur, meer verantwoordelijkheid voor medewerkers bij besluiten en lokale verandertrekkers. Belemmerend waren onder meer overbelasting, weinig middelen en leiders zonder betrokkenheid. In drie studies gaf een strikt top-down aanpak weerstand die de betrokkenheid verlaagde (Resultaten, thema 1b). De studies zijn niet op kwaliteit beoordeeld en de review gaat over volhouden, niet over effect.

Over zelfsturing zijn de bronnen voorzichtiger. Weerheim e.a. (2018) interviewden 18 medewerkers in twee teams van een Nederlandse ggz-organisatie. Duidelijke taakverdeling, goede relaties en een coachtraject golden als succesfactoren. Medewerkers ervoeren meer invloed en leren, maar ook meer werkdruk. Het bestuur had de zelfsturing ingevoerd en had moeite de controle los te laten (p. 8-10). De regiomanager koos de teams; er zijn geen uitkomstmaten.

Een scoping review van 25 publicaties over Buurtzorg-afgeleide modellen buiten Nederland meldt vooral hoge tevredenheid. Kosten zijn niet conclusief, uitkomsten voor patiënten worden zelden onderzocht en er is 'no quick fix' (Hegedüs e.a., 2022). Het zijn veelal niet-peer-reviewde casusbeschrijvingen, deels geschreven door de invoerende organisaties zelf.

Het opdrachtonderzoek van KPMG Plexus (2015; 606 aanbieders, data van 2013, Buurtzorg in de begeleidingscommissie) vond voor Buurtzorg iets lagere totale kosten per cliënt: 15.357 euro tegen gemiddeld 15.856 euro per jaar, gecorrigeerd voor zorgzwaarte. De curatieve kosten waren hoger (7.787 tegen 5.187 euro, huisarts en ziekenhuis). Het meet de organisatie, niet het mechanisme zelfsturing.

Volgens een alternatieve visie (Ford & Ford, 2009, aangehaald in Stalker, 2024) kan weerstand worden gelezen als informatie over het ontwerp van de verandering en niet als eigenschap van medewerkers. Dat is de visie van de besproken auteurs en geen eigen bevinding van Stalker. Het is

een zwakke secundaire bron, en Stalker merkt zelf op dat die visie een managementperspectief blijft.

Voor het model: betrokkenheid, tijd en coaching zijn herhaaldelijk genoemde voorwaarden. Een strikt top-down aanpak gaf in drie lean-studies weerstand. In de ggz-casus van Weerheim e.a. (2018) was dat niet zo: de opgelegde zelfsturing werd, ook zonder duidelijke reden, door de medewerkers als verbetering ervaren. Dat teamgestuurd beter werkt dan top-down is niet aangetoond. Zelfsturing is geen automatische vorm van 'van onderaf': in die ene casus noemt de bron de moeite van het bestuur om controle los te laten als spanning.

3.2 Psychologische veiligheid

Edmondson en Bransby (2023) overzagen 185 empirische artikelen (2013-2021), 153 kwantitatief; zorg is met 33 artikelen de grootste afzonderlijke setting (p. 58-59). De auteurs vinden aanzienlijk kwantitatief bewijs dat psychologische veiligheid samenhangt met leren en kennisoverdracht en dat zij dit bemiddelt of modereert (p. 63), vooral bij gedrag met interpersoonlijk risico zoals fouten melden (p. 63-64). Het bewijs is overwegend correlatieel. Het grootste hiaat is hoe je psychologische veiligheid creëert (p. 71); zij is 'not the goal but rather a factor for enabling other goals' (p. 73).

Een systematische review van interventies in zorgteams vond 14 studies, vooral onderwijs (simulatie, video, casussen) met gemengde uitkomsten. Slechts drie mat psychologische veiligheid zelf (O'Donovan & McAuliffe, 2020).

Het Britse National Cyber Security Centre (NCSC, 2025) vraagt om incidentonderzoek om te leren en niet om te beschuldigen (principe 2). De NCSC zegt de principes met partners uit industrie en overheid te hebben ontwikkeld, maar toont geen onderbouwing of effectonderzoek.

Voor het model: een klimaat waarin teams durven te zeggen dat iets niet werkt hangt samen met het delen van fouten (Edmondson & Bransby, 2023; correlatieel). Of het zich met een korte les laat ontwerpen, is niet aangetoond. De gelezen review met interventies (O'Donovan & McAuliffe, 2020) vond gemengde uitkomsten van vooral onderwijsinterventies en meldt weinig onderzoek; over korte lessen specifiek is niets gevonden. Dat samen verbeteren dat klimaat versterkt, is een veronderstelling.

3.3 Ondersteunende diensten die meebouwen

Het idee van een team dat anderen helpt en zich dan terugtrekt, zoals een bouwteam dat collega's laat zien hoe AI-hulpmiddelen werken, sluit gedeeltelijk aan bij het enabling team uit Team Topologies, een model voor softwareteams. Een enabling team laat vaardigheden in andere teams groeien en schrijft geen normen om ze af te dwingen (Fowler, 2023), en is bedoeld als tijdelijk (Team Topologies, n.b.). Een enabling team bouwt niet zelf voor andere teams; de aansluiting bij

een bouwteam is daarom beperkt en geldt alleen voor het laten groeien van collega's. De vertaling naar ondersteunende afdelingen als ICT, privacy en security is onze eigen lezing. Het is een praktijkmodel zonder onderzoek.

DORA (2026), een programma van Google Cloud, noemt poortwachters in plaats van enablers een antipatroon dat tot schaduw-IT-omwegen kan leiden. Dat is een waarschuwing en niet gemeten. De cijfers op die pagina hebben geen steekproef en worden hier niet overgenomen.

Uit de zorg zelf is beperkter materiaal. Coaches en backoffice (ICT, administratie) worden bij Buurtzorg-afgeleide modellen als even belangrijk beschreven (Hegedüs e.a., 2022). Waarmee precies is vergeleken, is niet vastgelegd. Bij co-design in acute zorg hielden betaalde facilitators projecten op koers en hinderde werk in eigen tijd (Clarke e.a., 2017, p. 6-8). Dat waren geen softwarebouwers.

Een factsheet van Q-Consult Zorg (n.b.), zelf aanbieder van digicoach-trainingen, meldt dat ± 1.000 medewerkers uit meer dan 200 zorgorganisaties zijn opgeleid. Als uitdaging uit interviews noemt het onder meer ontbrekend draagvlak bij directie en MT (aantal interviews onbekend).

In een interviewstudie bij een Britse universiteit gaf administratief personeel aan zich meer te laten leiden door collega's, leidinggevend en lokale ondersteuning dan door beleid (Demjaha e.a., 2024). Het ging om 14 administratief medewerkers en 7 ondersteuners; het is zelfrapportage zonder gedragsmeting.

Als achtergrond (dit model kiest niet voor zelfbouw door medewerkers): voor zelf bouwen is een Center of Excellence (CoE) in de gelezen bronnen het meest uitgewerkte voorbeeld: kernrollen, sandbox-omgevingen en het opsporen van apps zonder eigenaar (Microsoft, 2026a, 2026b; de Starter Kit wordt niet meer onderhouden). Een proefschrift (Salvatore, 2024) beschrijft een CoE met governance en fusion teams van business en IT. Een interviewstudie met 30 interviews (Viljoen e.a., 2024) benadrukt de rol van technische experts. Bij de apothekersstudie ondersteunde één IT-facilitator (Li e.a., 2026).

In Engeland reageerden 191 van 226 NHS-trusts op een verzoek om informatie. Van die 191 had 84% (161) een team voor software-, website- of innovatieontwikkeling, en 93% van die teams (150) werkte met klinisch personeel (Bennion e.a., 2024; data 2020-2021). Dat zegt niets over zelfbouw door zorgmedewerkers.

Voor het model: meebouwende ondersteuning en een centraal team met een eigen werkwijze (een gids van het International Growth Centre over het Britse i.AI-team, een ervaringsdocument in concept; het team groeide van drie of vier naar ongeveer zestig mensen en noemt overdracht aan afdelingen zonder eigenaar als hoofdbarière) worden in praktijkmodellen beschreven, maar geen enkele gelezen bron vergelijkt samenwerking tussen een bouwteam en de business met een loketmodel op een uitkomst. Dat is een van de drie open gaten.

3.4 Co-creatie en participatie

Een snelle synthese van 11 co-designstudies in acute ziekenhuiszorg vond waardering, ideeën en kleine praktische verbeteringen. Slechts één studie had een gevalideerde uitkomstmaat, één had een kostenanalyse en geen enkele evalueerde duurzaamheid (Clarke e.a., 2017, p. 1, 5, 9). De auteurs wijzen op publicatiebias en een 'dark side' (gedwongen deelname, goedkope arbeid).

Een review over co-creatie met burgers in de publieke sector vond 'hardly any empirical material' over uitkomsten (Voorberg e.a., 2013, p. 33). Het is een conferentieversie met inconsistente aantallen (49 of 59 artikelen).

Van 69 eHealth-studies met participatief ontwerp beoordeelden 50 hun uitkomst volgens de oorspronkelijke auteurs als in lijn met eerdere bevindingen of (na een test) effectief. Slechts 22 daarvan rapporteerden uitkomstmaten (Vandekerckhove e.a., 2020; aantallen niet nagerekend). Slupska e.a. (2022) lieten 32 migrante huishoudelijke werkers zelf bedreigingen modelleren; kwalitatief, zonder gedragsmeting, niet in een werkorganisatie.

Voor het model: co-creatie is gangbaar en wordt gewaardeerd, maar bewijs voor uitkomsten, duurzaamheid en leer- of gedragseffecten is dun. Dat past bij een bescheiden claim.

3.5 Privacy- en securitygedrag

Deze bronnen staan het dichtst bij de vraag of een les werkt.

Ho e.a. (2025) deden een gerandomiseerd veldexperiment bij meer dan 19.500 medewerkers van een groot Amerikaans zorgbedrijf: acht maanden, tien gesimuleerde phishingcampagnes, vier trainingsvormen en een controlegroep. Het is één organisatie en de maat is klikgedrag.

Er was geen significant verband tussen hoe recent iemand de jaarlijkse training deed en de kans te falen. Dat is een niet-gerandomiseerde vergelijking; een controlegroep zonder training bestond hiervoor niet. Embedded training (na een gesimuleerde klik) gaf een kleine verbetering: 9,5% lagere odds op falen (odds ratio 0,905, geen kans), gemiddeld ongeveer 1,7 procentpunt lager faalpercentage. Bij 37% tot 51% van de sessies werd de pagina direct gesloten en 24,0% werd afgerond (p. 1, 9-11).

Wie een interactieve training afrondde had 19% lagere odds later te falen, maar zelfselectie kan dat verklaren (p. 12). De auteurs: 'better phishing lures increase failure rates much more than the training approaches decrease them' (p. 9). Technische maatregelen als hardware-MFA leveren volgens hen waarschijnlijk meer op (p. 14); zij hebben dat niet getest.

Lain e.a. (2022; ruim 14.000 medewerkers van één bedrijf, 15 maanden) vonden dat waarschuwingen in de mail het klikken sterk verlaagden. Het waren waarschuwingen op gesimuleerde phishingmails. Er waren 3.964 klikken zonder waarschuwing tegen 1.427 (korte) en

1.289 (gedetailleerde), in groepen van vergelijkbare omvang. Vrijwillige embedded training verbeterde de detectie niet en ging samen met meer herhaald falen; verplichte training is niet getest. Een meldknop werd 15 maanden gebruikt, met ongeveer 1,5 handmatig te beoordelen mail per dag bij meer dan 21.000 melders (p. 9-12).

Becker e.a. (2017; enquête bij 608 medewerkers van één bedrijf) schrijven dat beleid alleen werkbaar is 'if employees are involved in shaping it' (p. 9). Dat is een aanbeveling en geen gemeten effect. De Wegwijzer Informatieveilig Gedrag (ICTU, n.b.) is een gedragsgerichte methode voor de zorg; de gelezen brochure heeft vier gebruikersquotes en geen effectcijfers. De Autoriteit Persoonsgegevens (AP, 2025) noemt trainingen een uitvoeringsmaatregel voor AI-geletterdheid zonder te onderbouwen dat die werken.

Een voorbehoud bij het beeld dat training weinig oplevert: Silic en Lowry (2020; B) melden uit een veldstudie van zes maanden met 420 deelnemers dat gegamificeerde securitytraining volgens het abstract tot 'statistically significant positive behavioral changes' kan leiden. Effectgrootte, vergelijking met klassieke training en aard van de gedragsmeting zijn uit het abstract niet te halen. Het is één organisatie, en gamification is niet hetzelfde als samen bouwen.

Als analogie, niet als bewijs: een meta-analyse van 225 studies in bachelor-STEM-onderwijs vond dat actief leren de scores op examens en andere toetsen met gemiddeld 0,47 standaarddeviatie verhoogde ten opzichte van hoorcollege (Freeman e.a., 2014, p. 8410). Het ging om 158 vergelijkingen voor examenscores en 67 voor zakpercentages. Examens zijn geen werkgedrag.

Voor het model: de bronnen steunen de scepsis over gangbare, passieve of losse trainingen (met het voorbehoud van Silic en Lowry), niet de stelling dat samen doen beter werkt. Embedded training kan als een vorm van leren door doen worden gelezen (onze lezing; het is een pagina na een klik, ver van bouwen) en werkte beperkt of niet.

Het sterkst komt in deze bronnen ontwerp naar voren, maar smal. Waarschuwingen op het moment van handelen en een eenvoudige meldknop deden het in één veldexperiment goed (Lain e.a., 2022). Technische maatregelen zijn een vermoeden van de auteurs van Ho e.a. (2025), in geen van beide studies getest. Dat past bij verschuiving 4 en minder bij H3.

3.6 AI als medebouwer

Snelheid. In een RCT met 16 ervaren open-sourceontwikkelaars en 246 taken in hun eigen repositories duurden taken met toegestane AI gemiddeld 19% langer, terwijl de deelnemers achteraf 20% tijdswinst schatten (J. Becker e.a., 2025, p. 1; B). Nakijken en opschonen van AI-uitvoer kostte 9% van de tijd (p. 11). Winst is volgens de auteurs wel mogelijk bij kleine nieuwe projecten of onbekende codebases (p. 12). Het ging niet om medewerkers die een klein intern hulpmiddel bouwen.

Veiligheid. Vier studies, per studie samengevat.

Studie	Wat is gemeten	Resultaat	Let op
Perry e.a. (2023), p. 1, 6-7	47 deelnemers, vooral studenten; bestandspad- en SQL-taak	Bestandspad: 12% met AI-assistent veilig tegen 29% zonder. SQL: 36% met AI een injectiekwetsbaarheid tegen 7% zonder. Deelnemers met AI geloofden vaker dat hun code veilig was	Over alle taken samen net niet significant ($p = 0,056$); model uit 2022
Zhao e.a. (2026), p. 1, 7-8	Agents voeren 186 functieverzoeken uit echte open-sourceprojecten uit	Beste combinatie: 57,0% functioneel correct, slechts 11,8% correct én veilig; extra beveiligingshints hielpen nauwelijks	Zonder mens in de lus
Deng e.a. (2026), alleen abstract	200 uitgerolde, publieke applicaties gebouwd met AI-hulpmiddelen	91,0% minstens één kwetsbaarheid; 65,77% van de 1.186 kwetsbaarheden kritiek of hoog	Methode en definitie van kwetsbaarheid niet gelezen; de applicaties zijn mogelijk niet representatief voor interne hulpmiddelen
Spracklen e.a. (2025)	16 codemodellen van 2023-2024, 576.000 codevoorbeelden	Gemiddeld ten minste 5,2% (commercieel) tot 21,7% (open-source) verzonden softwarepakketten	Volgens de bronnotitie een percentage van de aanbevolen pakketten

Leren. In een experiment met 52 ontwikkelaars die een nieuwe Python-bibliotheek leerden, scoorde de groep met AI-assistent 17% lager op een quiz zonder AI. Wie uitleg vroeg behield de leerwinst; wie code liet genereren leerde het minst (Shen & Tamkin, 2026, p. 2, 9-14). Het is een preprint met Anthropic-auteurs en de aantallen per gebruikspatroon zijn klein. 'AI-enhanced productivity is not a shortcut to competence' (p. 1).

Niet-programmeurs. Dit model kiest er bewust niet voor dat medewerkers zelf bouwen; de volgende bronnen laten zien wat er dan gebeurt en zijn achtergrond. Clinici beschrijven hoe zij zelf kleine hulpmiddelen bouwen, met een risicoladder in drie lagen (Ong e.a., 2026; deels commerciële belangen, niets gemeten). Apothekers in een Chinees ziekenhuis bouwden met een

low-codeplatform een voorraadapp. Het foutpercentage in de voorraadtelling daalde tussen de basislijn en de nameting (studieduur 12 maanden) van 8,7% naar 2,1% bij 22 apothekers, zonder controlegroep en met de bouwers als evaluatoren (Li e.a., 2026). De notitie meldt inconsistenties in het artikel en raadt aan de cijfers eerst na te lezen; ze gelden hier alleen als illustratie.

Voor het model: AI als medebouwer lijkt geen vanzelfsprekende versneller en niet vanzelf veilig of leerzaam. Het hangt vermoedelijk af van wie bouwt en hoe de AI wordt gebruikt. Of een controlestap het risico verkleint, is door geen studie getoetst (hypothese).

De experimenten met mensen (METR, Perry, Shen en Tamkin) betreffen ontwikkelaars of studenten. Zhao, Spracklen en Deng meten modellen of applicaties zonder deelnemers. De studies bij zorgprofessionals (Li, Ong) meten geen privacy- of securitygedrag of zijn zelfverteld; Li meet wel een werkuitkomst, het foutpercentage in de voorraadtelling. Toepassing op teams in zorg of gemeente is extrapolatie.

3.7 Risico's van AI-gebruik door medewerkers

Drie bedrijfsrapporten laten zien dat AI-gebruik buiten het zicht van de organisatie voorkomt. Het zijn leveranciersrapporten met een belang (zie het kader).

Bron	Steekproef	Cijfers	Let op
Verizon DBIR 2025 (p. 13, 20, 25, 106)	22.052 incidenten, 12.195 bevestigde datalekken	Menselijke betrokkenheid bij 60% van de datalekken, in een brede definitie. Volgens browsermonitoring van een datapartner gebruikte 15% van de medewerkers regelmatig generatieve AI op bedrijfsapparaten (elders 14%); van hen had 72% een niet-zakelijk e-mailadres als account en 17% een zakelijk adres zonder geïntegreerde aanmelding. Volgens het rapport wijst dat op gebruik buiten beleid	Auteurs: 'The best we can do is correlation'. Organisaties en aantallen achter de browsermonitoring niet gelezen

Bron	Steekproef	Cijfers	Let op
IBM/Ponemon (2025)	600 organisaties met een datalek	20% had een datalek door schaduw-AI-incidenten; 63% had geen AI- governancebeleid. Elders staat 87% zonder beleid of proces om AI-risico te beperken (groep onduidelijk)	87% en 63% zijn zonder de vraagstelling niet te verzoenen. Niet-statistische steekproef, vertekend naar volwassener beveiliging; IBM verkoopt oplossingen op dit terrein
Microsoft en LinkedIn (2024)	31.000 kenniswerkers in 31 markten	78% van de AI-gebruikers nam eigen AI-hulpmiddelen mee naar het werk (niet verstrekt door de organisatie, niet per se verboden); 52% was terughoudend te melden dat zij AI voor hun belangrijkste taken gebruiken	Zelfrapportage; kenniswerkers

De cijfers gaan over alle sectoren (bij Microsoft en LinkedIn over kenniswerkers) en zeggen niets specifiek over zorg of gemeenten. De aparte zorgcijfers in het Verizon- en IBM-rapport zijn hier niet gebruikt.

In een evaluatie van een gekocht hulpmiddel verschilde de kennis van het beleid voor acceptabel gebruik sterk (Department for Business and Trade, 2025, p. 34); gedrag is niet gemeten. DORA (2025) meldt een samenhang: de baten van AI zijn groter bij organisaties met een duidelijk gecommuniceerde AI-houding. Het onderzoek omvat bijna 5.000 technologieprofessionals, is zelfgerapporteerd en is door Google Cloud betaald.

Anekdotisch, zonder aantallen of opzet: de AP waarschuwde in 2024 na een medewerker van een huisartsenpraktijk die persoonsgegevens in een chatbot zette (NOS Nieuws, 2024). Eindhoven rapporteerde in een interne steekproef (23 september tot 23 oktober 2025) bestanden met persoonsgegevens op openbare AI-websites en liet daarna alleen Copilot toe (Hartholt, 2025). De AP zou in 2025 'tientallen' meldingen hebben ontvangen, tweedehands via het FD (Binnenlands Bestuur, 2025).

Fortune (Lazzaro, 2025) en The Register (Sharwood, 2025) beschrijven kwetsbaarheden in AI-codeertools volgens beveiligingsbedrijven en een door één gebruiker gemelde verwijderde productiedatabase, onbevestigd.

Voor het model: ongestuurd AI-gebruik bestaat al en kan gegevens in gevaar brengen. IBM meldt zowel schaduw-AI-datalekken (20%) als het ontbreken van AI-governancebeleid (63%); een verband daartussen is in de notitie niet getoetst. In de gelezen bronnen meet geen studie of bouwen binnen kaders dit risico verkleint.

3.8 Gecontroleerd bouwen en guardrails

De bronnen hieronder gaan deels over medewerkers die zelf bouwen. Voor het bouwteam in dit model zijn ze mogelijk bruikbaar als kader: dat ook professionele bouwers met AI baat hebben bij een tweede lezer, een eigenaar en een risicogestuurde controle is een hypothese; geen studie toetst het. Verschillende bronnen stellen een risicogestuurde aanpak voor:

- Ong e.a. (2026): Tier 1 persoonlijk gebruik zonder patiëntgegevens; Tier 2 voor een team met een tweede lezer, een benoemde beheerder en melding aan IT; Tier 3 patiëntgericht met formele review (p. 8-10).
- Alqheedan en Alzughaibi (2026): vier niveaus, bepaald door vier criteria: gevoeligheid van gegevens, nabijheid van klinische beslissingen, autonomie en schaal. Het kernrisico is dat de bouwer de code niet meer begrijpt. Alleen conceptueel gevalideerd.
- NCSC (2026): de zwaarte van toezicht hangt af van wat je bouwt; interne hulpmiddelen met beperkte blootstelling en zonder gevoelige gegevens kunnen lichter, gevoelige persoonsgegevens niet (p. 2). Een blog.
- OWASP (n.b.): blind vertrouwen in AI-uitvoer, lekkende gegevens en verweesde apps zonder eigenaar (CD-SEC-01, -04, -09); een expertlijst zonder prevalentiecijfers.
- Bennink en Drukarch (2023): privacy by design vanaf het begin en in alle fasen, met een nulgesprek met medewerkers en geen afvinklijstje (p. 4, 16, 49, 51). Het gaat niet over kleine zelfgebouwde tools.
- Vereniging van Nederlandse Gemeenten (VNG, 2025): bij interne ontwikkeling van AI-toepassingen is de gemeente zelf leverancier met dezelfde eisen (p. 6). Een standpunt met een toezichtsteam, eerder top-down dan teamgestuurd.

Drie praktische punten sluiten aan bij de empirische bronnen. Het is onze eigen afleiding; geen van deze maatregelen is getoetst.

- 'Vraag de AI veilig te bouwen' is geen kader (Zhao e.a., 2026, p. 1, 8).
- Een kundige tweede lezer lijkt nodig. Shen en Tamkin (2026) wijzen op kennisbehoefte bij het beoordelen van AI-code, en deelnemers met beveiligingservaring kopieerden AI-uitvoer minder vaak (Perry e.a., 2023, p. 9). Of een controlestep het risico verkleint, is niet getoetst (hypothese).
- Een lijst met toegestane bouwstenen is zinvol, omdat 'bestaat de naam' bij verzonden pakketten niet volstaat (Spracklen e.a., 2025, p. 2). Dit is onze interpretatie.

Volgens leveranciersdocumentatie van Anthropic (n.b.) moet de gebruiker zelf voorgestelde code beoordelen en verschillen training en bewaartermijn per abonnementstype. Dat laatste is een

beheerpunt.

In de gelezen bronnen is over overdracht en beheer het minst gevonden. De apothekersstudie beschrijft volgens de ophaalsamenvatting geen onderhoudsplan (Li e.a., 2026). De citizen-development-literatuur noemt technical debt en schaduw-IT als risico (Viljoen e.a., 2024). Geen van de 11 studies in de review van Clarke e.a. (2017, p. 1) evalueerde duurzaamheid.

Juridische punten als open vragen (alleen op basis van de juridische bronnotities, geen advies).

AVG. Open vraag voor de FG en een jurist: valt een klein intern hulpmiddel onder de DPIA-plicht? Een DPIA is vereist bij een verwerking die gelet op aard, omvang, context en doeleinden waarschijnlijk een hoog risico inhoudt, in het bijzonder bij een verwerking waarbij nieuwe technologieën worden gebruikt (art. 35 lid 1). Dat laatste is voor AI-hulpmiddelen het relevante deel. Is een FG aangewezen, dan wint de verwerkingsverantwoordelijke diens advies in (art. 35 lid 2; taken van de FG in art. 39 lid 1 onder c) (Europees Parlement & Raad, 2016). De lijst van de Autoriteit Persoonsgegevens met verplichte DPIA's is niet gelezen.

AI Act. De AI-verordening (Europees Parlement & Raad, 2024) vroeg in art. 4 maatregelen voor een toereikend niveau van AI-geletterdheid van personeel. Volgens de wijziging van 2026 zijn het maatregelen om de ontwikkeling van AI-geletterdheid te ondersteunen, zonder dat een bepaald niveau gegarandeerd hoeft te worden (Europees Parlement & Raad, 2026). Open vraag: is een bouwer van een intern hulpmiddel 'aanbieder'? Dat staat niet in de gelezen bronnen (de definities in art. 3 zijn niet gelezen; AP, 2025 noemt de vraag niet).

MDR. Open vragen: (1) aan welke voorwaarden voldoet een zelfgebouwd hulpmiddel van een zorginstelling voor de uitzondering voor eigen gebruik (art. 5 lid 5), (2) geldt een VVT-instelling als 'health institution', (3) heeft tekstsamenvattende AI een medisch doel? De voorwaarden zijn onder meer:

- geen overdracht aan een andere juridische entiteit;
- een passend kwaliteitsmanagementsysteem;
- een gedocumenteerde rechtvaardiging dat de specifieke behoeften van de doelpatiëntgroep niet, of niet op het passende prestatieniveau, door een gelijkwaardig hulpmiddel op de markt kunnen worden gedekt;
- een openbare verklaring en documentatie;
- geen productie op industriële schaal.

De algemene veiligheids- en prestatie-eisen van Annex I blijven ook voor zulke hulpmiddelen gelden. De gelezen bronnen noemen de voorwaarden, maar beantwoorden deze toepassing niet (Europees Parlement & Raad, 2017).

Cyberbeveiligingswet. Zorgaanbieders staan in Bijlage 1. Middelgrote en grote zorgaanbieders zijn essentiële of belangrijke entiteiten met een zorgplicht (art. 21) en goedkeuring van de maatregelen door het bestuur (art. 24). Kleine zorgaanbieders vallen er alleen onder na aanwijzing

(Staatsblad, 2026). Open vraag: is een specifieke instelling essentieel of belangrijk (dat hangt van de omvang af) en wat betekent de zorgplicht voor hulpmiddelen die een bouwteam zelf bouwt? Dat is niet vastgesteld.

Twee onderdelen zijn niet onderzocht: de positie van overheid en gemeenten (de Staatscourant-regeling voor de sector overheid is alleen gescand) en de uitzondering voor entiteiten die uitsluitend jeugdhulp of maatschappelijke ondersteuning bieden. Voor gemeenten is deze paragraaf daarom niet af.

4 Het stuurmodel (voorstel)

Het stuurmodel heeft vier fasen: **Idee**, **Bouwen**, **Neerzetten** en **Borgen**. De zes stappen (4.2) lopen daardoorheen. In elke fase zit de kaderstap (privacy, security, AI) vast ingebouwd en werkt het bouwteam samen met de werkvloer.

Fase	Wat	Vast ingebouwd	Samen met de werkvloer
Idee	Signaal en oorzaak	Welke gegevens, welk risiconiveau; adviseurs kijken mee	De werkvloer brengt de behoefte in
Bouwen	Het bouwteam ontwikkelt klein, met AI	Kaderstap; tweede lezer waar het risico dat vraagt	Co-creatie: schetsen, prototypes, feedback
Neerzetten	Oplevering, overdracht, adoptie	Eigenaar en beheerder; toegang en logging; wat wel en niet mag	Uitleg en oefenen; terugkoppeling
Borgen	Beheer, register, evaluatie, delen	Register; evaluatiemoment	Wat werkt gaat naar andere teams

De communicatie loopt twee kanten op: co-creatiesessies, een open spreekuur, demo's 'wat mag wel en niet' en een terugkoppelmoment (eigen voorstel; de vorm komt uit de HBO-ICT-methoden Workshop, Co-creation en Prototyping, de invulling voor zorg of gemeente is een eigen duiding). Rollen: stuurder, bouwteam, business en werkvloer, adviseurs en bestuur. De organisatievorm is een keuze voor het bestuur: een programma digitalisering of een vaste nieuwe afdeling; het voorstel is te beginnen als programma en te evalueren.

Het stuurmodel is een voorstel en een hypothese. De tabellen geven aan wat de bronnen wel en niet zeggen; de kolom met wat bronnen wel zeggen bevat bronclaims, de rest is voorstel. Bronnen die slechts deels zijn gelezen (leescode B, zie hoofdstuk 2) zijn met (B) gemarkeerd.

4.1 Zes verschuivingen

#	Van	Naar	Wat bronnen wel zeggen	Wat ze niet zeggen
1	Een vraag steeds opnieuw beantwoorden	Vragen waarom hij terugkomt en de oorzaak wegnemen	Voorbeelden van Ong e.a. (2026) en Li e.a. (2026; B) begonnen bij een terugkerend werkprobleem; Clarke e.a. (2017) vonden kleine praktische verbeteringen	Geen vergelijking met alternatieven; zelfverteld
2	Ondersteuning als loket	Een bouwteam dat met de werkvloer ontwikkelt en uitlegt	Coaches en backoffice worden als even belangrijk beschreven (Hegedüs e.a., 2022; B); DORA (2026; B) waarschuwt, zonder cijfers, dat poortwachters tot omwegen kunnen leiden; enabling-idee (Fowler, 2023)	Geen onderzoek in zorg of overheid dat meebouwen vergelijkt met een loket
3	Awareness als les	Awareness als gevolg van samen ontwikkelen (H3, niet getoetst)	Gangbare phishingtraining (jaarlijks, embedded) leverde weinig op (Ho e.a., 2025; Lain e.a., 2022); gedrag wordt volgens interviews mede door collega's en lokale ondersteuning bepaald (Demjaha e.a., 2024; B); een gegamificeerde training kan volgens het abstract tot gedragsverandering leiden (Silic & Lowry, 2020; alleen abstract, B)	Geen studie vergelijkt samen bouwen met een les op awareness; AI-hulp kan leren verminderen (Shen & Tamkin, 2026)

#	Van	Naar	Wat bronnen wel zeggen	Wat ze niet zeggen
4	Kaders als rem achteraf	Kaders als vaste stap tijdens het bouwen	Waarschuwingen in de flow verlaagden klikken op gesimuleerde phishing (Lain e.a., 2022); privacy by design vanaf dag een (Bennink & Drukarch, 2023); risicoladders (Ong e.a., 2026; NCSC, 2026)	Geen effectmeting van kaderstappen op gedrag
5	Verandering van bovenaf	Samen ontwikkelen; bestuur geeft mandaat, kaders en aandacht	Betrokkenheid van medewerkers komt terug als factor voor volhouden van lean; strikt top-down gaf in drie van 24 studies weerstand (Kunnen e.a., 2023)	Zelfsturing was opgelegd en werd toch positief ervaren (Weerheim e.a., 2018); over de effecten van Buurtzorg-afgeleide modellen is weinig gemeten, kosten en kwaliteit zijn niet aangetoond (Hegedüs e.a., 2022; B)
6	Aparte trajecten voor privacy, security, AI	Eén werkwijze van idee tot geborgd	De VNG (2025) bepleit een integrale aanpak; Perry e.a. (2023) en Zhao e.a. (2026) wijzen erop dat AI-hulp de beveiligingskwaliteit van gegenereerde code kan beïnvloeden	Standpunt, geen onderzoek; zegt niets over teams die zelf bouwen of over aparte versus geïntegreerde trajecten

4.2 De cyclus

Voorgesteld wordt een cyclus die de bestaande PDCA-cyclus volgt, zoals uitgewerkt in het eigen strategievoorstel (strategie/strategie-vwt.md; een eigen projectdocument, geen bron), met een startpunt dat teams herkennen:

1. **Signaal.** Een vraag of probleem komt terug; de werkvloer herkent en brengt het in. In de voorbeelden uit de literatuur begon het bouwen ook bij zo'n terugkerend werkprobleem (Ong e.a., 2026; Li e.a., 2026); dat is een voorbeeld en geen toets.
2. **Oorzaak.** Het bouwteam en de werkvloer zoeken samen waarom het terugkomt. Een gesprek met medewerkers over het werk is wat de Wegwijzer (ICTU, n.b.) en JenV (Bennink & Drukarch, 2023, p. 49) beschrijven, zonder effectbewijs.
3. **Klein bouwen binnen kaders.** Het bouwteam bouwt; alleen niveau 0 en 1 van de risicoladder (zie 4.4) in een eerste ronde; AI als hulp met een tweede lezer; de werkvloer geeft feedback.
4. **Overdracht.** De werkvloer neemt over na uitleg en oefenen (adoptie, wat wel en niet mag). Een benoemde eigenaar en een plan voor beheer vóór ingebruikname (OWASP, n.b.; Ong e.a., 2026, p. 9). Over deze stap is in de gelezen bronnen weinig onderzoek gevonden; zij wordt in meerdere bronnen als risico genoemd (OWASP, Ong, Viljoen).
5. **Zien wat het oplevert.** Een nulmeting en een tweede meting; zelfgerapporteerde winst telt niet als bewijs (zie hoofdstuk 5).
6. **Delen.** Leerpunten gaan naar andere teams en terug naar de behoefte. Bronnen over delen zijn niet gelezen, behalve dat psychologische veiligheid samenhangt met het delen van fouten (Edmondson & Bransby, 2023).

4.3 Rol van het bestuur

Het bestuur kiest de organisatievorm en geeft mandaat aan de stuurder. Het heeft in het voorstel vier taken. Het geeft ruimte (tijd en mensen, want overbelasting remt; Kunnen e.a., 2023; Clarke e.a., 2017). Het stelt kaders vast (de risicoladder en wie op welk niveau beslist). Het geeft aandacht: draagvlak van directie wordt door Q-Consult Zorg (n.b.), een factsheet op basis van interviews zonder aantallen, als succesfactor bij digicoaches genoemd. En het laat los: Weerheim e.a. (2018, p. 10) beschrijven dat dit in hun casus moeilijk was.

Daarbij hoort een klimaat zonder straf voor meldingen (NCSC, 2025, principe 2 en 5). Het bestuur beslist zelf over niveau 3.

De Cyberbeveiligingswet legt voor essentiële en belangrijke entiteiten in de zorgsector (afhankelijk van omvang of aanwijzing; zie 3.8) een bestuursverantwoordelijkheid vast (Staatsblad, 2026, art. 24). Hoe die zich verhoudt tot hulpmiddelen die een bouwteam zelf bouwt is een open vraag (zie 3.8).

4.4 Risicoladder (eigen voorstel, geen bronbevinding)

Niveau	Raakt	Voorbeelden (ter illustratie)	Toets in het voorstel	Verwante ideeën in bronnen (bij benadering)
0	Geen persoonsgegevens	Kennisgidsen, checklists	Inventaris; check dat geen persoonsgegevens erin gaan	Ong e.a. (2026) Tier 1; NCSC (2026)
1	Gegevens van medewerkers	Roosterruil	Verwerkingsregister; DPIA-screening; toegangsbeheer	Ong e.a. (2026) Tier 2 (gegevens van medewerkers komen bij Ong niet voor)
2	Cliënt- of burgergegevens zonder inhoudelijke zorg- of dossiergegevens	Planning, vervoer	DPIA; FG-advies; logging; NEN 7510- maatregelen	Ong e.a. (2026) Tier 3 (identificeerbare gegevens; geen exacte overeenkomst); Alqheedan & Alzughaibi (2026) (niveaus op gevoeligheid van gegevens)
3	Zorginhoudelijke gegevens	Samenvatting van rapportages	Alles daarboven, plus de vragen voor AI Act en MDR; besluit op bestuursniveau	Ong e.a. (2026) Tier 3

Eerste ronde: alleen niveau 0 en 1. Niveau 2 en 3 horen bij het model, maar niet in een eerste proef. De kolom 'Toets in het voorstel' is een eigen voorstel en geen juridische bewering: een DPIA is volgens art. 35 AVG alleen vereist bij waarschijnlijk hoog risico.

4.5 Wat het model wel en niet claimt

Het model claimt niet dat samen ontwikkelen awareness aantoonbaar verhoogt, en ook niet dat inbouwen vanaf het begin goedkoper is dan achteraf toevoegen: voor dat kostenargument is geen bron gelezen. De bronnen beschrijven of bepleiten losse bouwstenen (betrokkenheid, meedenkende ondersteuning, kaders in de flow, risicogestuurde controle), grotendeels als beschrijving of voorstel zonder effectbewijs. Het model claimt dat het samenbrengen daarvan een hypothese is die een proef verdient. Een eigen 'stopregel' ontbreekt in dit concept.

5 Casus A en een eerlijke waardelens

5.1 Casus A (geanonimiseerd; voorbeeld, geen bewijs)

Een team had periodiek een overzicht nodig van niet-afgeleverde e-mail. Dat werd steeds handmatig uitgevraagd. Een bouwer keek naar de oorzaak van de terugkerende vraag en bouwde een klein intern overzicht, dat aan het team is overgedragen. Er wordt geen organisatie genoemd.

De casus illustreert verschuiving 1 (oorzaak wegnemen) en 4 (kaderstap; de casus zegt niet of die is gezet). In het verhaal komt alleen 'een bouwer' voor. Dat het bouwen binnen een programma met de werkvloer gebeurde, of dat adviseurs meekeken, is dus een eigen lezing en niet uit de casus af te leiden.

Open vraag aan de FG: zijn e-mailadressen in dit overzicht persoonsgegevens, hoort de kaderstap er dan bij, en wat geldt? In onze eigen risicoladder (4.4) zou dat een DPIA-screening zijn; die invulling is een eigen voorstel en komt niet uit de casus. Dit stuk beantwoordt de juridische vraag niet; de gelezen juridische notities bevatten dit uitgangspunt niet.

Wat de casus niet laat zien: of het team er iets van geleerd heeft over privacy of security (H3), of het hulpmiddel is beheerd na overdracht, en of de bouwer alle risico's kende. Het verhaal is door de bouwer zelf verteld en is één geval. Dat geldt ook voor Ong e.a. (2026; een ervaringsgids van de auteurs) en Li e.a. (2026; een studie waarin de bouwers ook de evaluatoren waren).

5.2 Waardelens

Terugverdienen is één lens en niet de hoofdzaak. Een eerlijke berekening telt kosten en baten op.

Post	Wat erbij hoort	Wat de bronnen zeggen
Kosten: bouw	Tijd van bouwteam en werkvloer, AI-abonnement	Nakijken en opschonen van AI-uitvoer kostte 9% van de tijd bij ervaren ontwikkelaars (J. Becker e.a., 2025, p. 11)
Kosten: overdracht	Eigenaar, documentatie, uitleg aan het team	Weinig onderzocht in de gelezen bronnen: geen van de 11 studies bij Clarke e.a. (2017) evalueerde duurzaamheid; Viljoen e.a. (2024; abstract) noemt technical debt als risico
Kosten: kaderstappen	DPIA-screening (eigen voorstel), FG-advies, tweede lezer	Dat een kundige tweede lezer nodig is, is een afleiding: Zhao e.a. (2026) meten agents zonder mens en Perry e.a. (2023) meten geen review (wel kopieerden deelnemers met beveiligingservaring AI-uitvoer minder vaak); in de gelezen bronnen geen kostencijfers gevonden
Kosten: beheer	Updates, afhankelijkheden, toegang, opruimen	Verweesde apps worden als risico genoemd (OWASP, n.b., een expertlijst zonder prevalentiecijfers; Microsoft, 2026b)
Baten: tijd	Minder handmatige uitvragen	Zie hieronder
Baten buiten uren	Grip, minder afhankelijkheid, kleiner aanvalsvlak, leren	Hypothesen; niet gemeten in de gelezen bronnen

Zelfgerapporteerd versus gemeten. In de METR-studie schatten ontwikkelaars 20% tijdswinst terwijl de meting 19% vertraging gaf (J. Becker e.a., 2025). De Britse Copilot-proef bij circa 20.000 ambtenaren meldt 26 minuten tijdswinst per dag, volledig zelfgerapporteerd en zonder controlegroep (Government Digital Service, 2025, §4.2).

De evaluatie van het Department for Business and Trade (2025, p. 5, 30-31) had waargenomen taken en een controlegroep die alleen kwalitatief is gebruikt. Zij vond geen bewijs dat tijdswinst tot productiviteit leidde (productiviteit was geen hoofddoel en is beperkt gemeten) en liet Excel-analyse langzamer en slechter zien (6 testpersonen, 5 controlepersonen).

In de apothekersstudie waren de bouwers de evaluatoren (Li e.a., 2026) en bij Ong e.a. (2026) is de tijdswinst een schatting van de auteurs. Geen van deze studies meet gedragsverandering rond

privacy of security.

Voor casus A: leg vooraf een nulmeting vast (hoe vaak komt de vraag terug, hoeveel tijd kost beantwoorden), meet later opnieuw, noem het een schatting zolang het niet gemeten is en reken beheerkosten mee.

6 Discussie en beperkingen

Wat opvalt.

1. De bronnen steunen sneller de kritiek op de les dan de oplossing. Ho e.a. (2025) en Lain e.a. (2022) laten zien dat gangbare phishingtraining weinig of niets opleverde. Dat geldt ook voor embedded training, die als leren door doen gelezen kan worden (onze lezing): bij Ho beperkt, bij Lain zonder effect en met meer herhaald falen.

Ontwerpmaatregelen komen het sterkst uit, maar smal: waarschuwingen en een meldknop in één veldexperiment (Lain); technische maatregelen zijn een vermoeden van de auteurs van Ho. Silic en Lowry (2020; alleen abstract) melden dat gegamificeerde training tot gedragsverandering kan leiden en zijn een voorbehoud bij het beeld dat training weinig oplevert. H3 is daarmee niet weerlegd, maar het is niet aannemelijk gemaakt dat 'doen' op zichzelf de winst is.

1. De AI-studies nuanceren het beeld dat AI alles omhoog tilt (J. Becker e.a., 2025; Perry e.a., 2023; Shen & Tamkin, 2026; Zhao e.a., 2026). Dat maakt een kundige tweede lezer en een goede manier van werken met AI, zoals uitleg vragen, plausibel als aandachtspunt. Het blijft een afleiding: geen studie toetst een tweede lezer, en de gebruikspatronen bij Shen en Tamkin zijn achteraf ingedeeld in kleine groepen (2 tot 7 per patroon).
2. De bronnen wijzen twee kanten op. IBM (2025) meldt schaduw-AI-datalekken (20%) en het ontbreken van AI-governancebeleid (63%) als losse cijfers; een verband daartussen is niet getoetst. Volgens de NCSC (2025, principe 1; richtlijn zonder effectonderzoek) worden kaders die als barrière worden ervaren omzeild. Het model zoekt het midden, maar de bronnen tonen niet waar dat ligt.

Zwakke plekken. Veel bronnen zijn preprint, vendor-gelieerd of alleen via een abstract of samenvatting gelezen (zie het kader). De co-creatieliteratuur lijdt onder publicatiebias en ontbrekende uitkomstmaten (Clarke e.a., 2017; Voorberg e.a., 2013; Vandekerckhove e.a., 2020). De zelfsturingsstudie is een casus met mogelijk positieve selectie (Weerheim e.a., 2018).

De bronnen komen uit uiteenlopende velden: software-ontwikkeling (METR, Perry, Zhao, Shen en Tamkin, DORA), onderwijs (Freeman), bedrijven (Lain, Becker e.a. 2017, Verizon, IBM, Microsoft en LinkedIn), zorg en ziekenhuizen (Ho, Clarke, Li, Hegedüs, O'Donovan en McAuliffe), een Nederlandse ggz-organisatie (Weerheim), Britse overheidsdiensten (GDS, DBT, NCSC) en een Britse universiteit (Demjaha). Rechtstreeks bewijs uit VVT-instellingen of gemeenten ontbreekt.

Niet gevonden in de gevoerde zoekrondes (afwezigheid is geen bewijs): bewijs dat privacy en security vanaf het begin inbouwen goedkoper is dan achteraf toevoegen, onderzoek naar samenwerking tussen een bouwteam en de business in zorg of gemeenten, Nederlandse voorbeelden van zorgmedewerkers of ambtenaren die zelf bouwen, evaluaties van overdracht en beheer, bronnen over teamgestuurde verandering bij gemeenten en een onafhankelijke Buurtzorg-evaluatie. Nieuws is anekdotisch.

Te veel of te weinig toezicht. Alqheedan en Alzughaihi (2026) noemen het risico van te zware governance voor laag-risico hulpmiddelen. Zhao e.a. (2026) laten zien dat AI-agents zonder mens in de lus vaak onveilige code opleveren (menselijke review is niet gemeten). De ladder is het voorgestelde antwoord, maar niet getoetst.

Open keuzes en dit stuk zelf. De organisatievorm, de rollen in grote lijnen en dat het stuk voor bestuurders is, zijn lezingen die nog bevestigd moeten worden; de precieze rollen zijn per organisatie. Het stuk is gebaseerd op bronnotities en geschreven met AI-hulp. Zinnen die zo niet in de bron staan, kunnen zijn ingeslopen; dat is in eerdere versies gebeurd, steeds bij een vervangende formulering. Versie 0.3 verwerkte de bevindingen van vier claimcontroles, die zelf ook op de notities steunen; de nieuwe en gewijzigde zinnen van versie 0.4 zijn pas na dit stuk gecontroleerd. Het is niet beoordeeld door een bestuurder, FG of jurist.

7 Aanbevelingen en vervolg

7.1 Voor bestuurders (voorstellen)

1. **Maak AI-gebruik zichtbaar en bespreekbaar** in plaats van het alleen te verbieden of te negeren. Dat gebruik lijkt al voor te komen (Verizon Business, 2025; Microsoft & LinkedIn, 2024; beide leveranciersrapporten). Een totaalverbod is volgens een ethisch hacker in Nieuwsuur geen goede oplossing (NOS Nieuwsuur, 2026; anekdotisch en een expertmening).
2. **Begin klein, als programma digitalisering:** een stuurder, een klein bouwteam en drie tot vijf behoeften die de werkvloer inbrengt (eigen voorstel; de H3-proef in 7.3 vraagt om vier tot zes teams), niveau 0 en 1 van de ladder, met een tweede lezer en een benoemde eigenaar vóór ingebruikname. Evalueer na een afgesproken periode of het een vaste afdeling moet worden.
3. **Geef ruimte, geen extra werk erbij:** tijd in het rooster voor de werkvloer, want werk in eigen tijd hinderde projecten (Clarke e.a., 2017) en overbelasting remt (Kunnen e.a., 2023). Clarke noemt betaalde facilitators die projecten op koers hielden, in co-design in acute zorg en niet bij softwarebouw; geen gelezen bron vergelijkt samenwerking met een bouwteam met een loket (zie 3.3).
4. **Meet zelf:** nulmeting en tweede meting; scheid zelfrapportage en gemeten gedrag; noem winst een schatting zolang zij niet gemeten is.
5. **Leg juridische vragen voor aan de FG en een jurist** voordat niveau 2 of 3 begint: DPIA, AI Act, MDR, Cyberbeveiligingswet en de bestuursverantwoordelijkheid (de open vragen staan in 3.8 en

5.1).

6. **Beloof geen awareness-winst.** Zeg dat het een hypothese is die in de proef wordt getoetst.

7.2 Vervolgonderzoek in de bibliotheek

- De volledige tekst lezen van de bronnen met code B die alleen als abstract of recordpagina zijn gelezen (Deng e.a., 2026; Viljoen e.a., 2024; Binzer & Winkler, 2022; Ajimati e.a., 2025; Salvatore, 2024; Bennion e.a., 2024; Silic & Lowry, 2020) en de cijfers van Li e.a. (2026) in het origineel nalezen.
- Zoeken naar Nederlandse voorbeelden van zorgmedewerkers of ambtenaren die zelf bouwen, naar teamgestuurde verandering bij gemeenten, en naar onderzoek over overdracht en beheer.
- Een extra bronnenronde over de drie open gaten: kosten van inbouwen vooraf tegenover achteraf toevoegen, samenwerking tussen een bouwteam en de business in zorg of gemeenten, en borgen en beheer na oplevering.
- Voor de Cyberbeveiligingswet: de positie van overheid en gemeenten en de uitzondering voor uitsluitend jeugdhulp of maatschappelijke ondersteuning uitzoeken.

7.3 Een kleine, eerlijke proef om H3 te toetsen

Geen enkele gelezen bron toetst H3. De proef hieronder is een voorstel voor een kleine, voorlopige toets; zij mist statistische kracht en moet als zodanig worden benoemd.

Onderdeel	Voorstel
Vraag	Gaan medewerkers van vrijwillig meedoende teams die samen met het bouwteam een klein hulpmiddel ontwikkelen (co-creatie, testen, overnemen) binnen kaders na drie maanden beter om met gevoelige gegevens en AI-tools dan medewerkers die een korte les kregen?
Opzet	Vier tot zes vrijwillige teams uit de werkvloer (eigen voorstel: twee armen van elk twee of drie teams, dus klein en verkennend), per loting of gematcht verdeeld over twee armen: (A) samen met het bouwteam een niveau 0- of 1-hulpmiddel ontwikkelen binnen kaders; (B) een korte les over dezelfde onderwerpen, met toegang tot dezelfde kaders. Arm B is tevens de wachtlijst: zij krijgt na de laatste meting alsnog het co-creatietraject
Gedragmaat	Een scenario-opdracht in een testomgeving met nepgegevens (welke gegevens gaan in een AI-tool?). Zelfrapportage apart gelabeld

Onderdeel	Voorstel
Kennismaat (geen gedragsmaat)	Een kennisquiz zonder AI (zoals Shen & Tamkin, 2026). Deze meet kennis en niet gedrag; rapporteer haar apart van de gedragsmaat
Procesgegevens (geen vergelijkende maat)	Meldingen en vragen aan de ondersteuning. Arm A werkt met het bouwteam en zal daardoor meer vragen stellen; als maat voor gedrag bevoordeelt dit arm A. Alleen te gebruiken als beide armen hetzelfde meldkanaal hebben, en dan nog als aanvulling
Meetmomenten	Voor, direct na en na drie maanden
Aandachtspunten	Zelfselectie bij afronden (Ho e.a., 2025), clustering per team, een beoordelaar die niet weet welke arm; weinig teams betekent geen statistische kracht, dus het is een verkennende proef van de meetaanpak. Arm A krijgt meer tijd en contact dan arm B, dus het verschil tussen samen ontwikkelen en les is verward met de hoeveelheid aandacht
Voraf vastleggen	Wat telt als steun, als geen verschil en als tegenbewijs, vóór de eerste meting
Poort	Akkoord van FG en ondernemingsraad voor veldwerk; geen cliënt- of burgergegevens; vrijwillige deelname; geen individuele resultaten naar leidinggevend. Anders dan Lain e.a. (2022), die geen informed consent hadden

Ontbrekende gegevens

Voor een aantal bronnen ontbreken bibliografische gegevens (bijvoorbeeld jaar, auteur, URL of paginabereik). Die zijn niet uit het geheugen aangevuld en staan in de referentielijst hieronder als 'n.b.' (niet bekend).

Referenties

- Ajimati, M. O., Carroll, N., & Maher, M. (2025). Adoption of low-code and no-code development: A systematic literature review and future research agenda. *Journal of Systems and Software*, 222, Artikel 112300. <https://doi.org/10.1016/j.jss.2024.112300>
- Alqheedan, A., & Alzughaibi, S. (2026). The VIBE-HI framework: A conceptual model for evaluating vibe coding appropriateness, quality, and safety in health informatics. *Frontiers in Artificial Intelligence*, 9. <https://doi.org/10.3389/frai.2026.1882814>
- Anthropic. (n.b.). *Claude Code documentation: Security; Data usage* [Webpagina's, opgehaald 19 oktober 2026]. <https://code.claude.com/docs/en/security>; <https://code.claude.com/docs/en/data-usage>
- Autoriteit Persoonsgegevens. (2025). *Aan de slag met AI-geletterdheid: Perspectief op kennisopbouw over AI-systemen bij organisaties* [Handreiking]. URL n.b.
- Becker, I., Parkin, S., & Sasse, M. A. (2017). Finding security champions in blends of organisational culture. *EuroUSEC 2017* (paginabereik n.b.). https://www.ndss-symposium.org/wp-content/uploads/2018/03/eurosec2017_07_Becker_paper.pdf
- Becker, J., Rush, N., Barnes, B., & Rein, D. (2025). *Measuring the impact of early-2025 AI on experienced open-source developer productivity* (arXiv:2507.09089v2) [Preprint]. <https://arxiv.org/abs/2507.09089>
- Bennink, N., & Drukarch, H. (2023). *Handleiding privacy by design, versie 1.0*. Ministerie van Justitie en Veiligheid. <https://open.overheid.nl/documenten/8d338db4-cf0f-420b-8092-c8f711e049c/file>
- Bennion, M. R., Spencer, R., Moore, R. K., & Kenyon, R. (2024). *Digital capability, open-source use, and interoperability standards within the NHS in England: A survey of healthcare trusts* [Preprint]. JMIR Preprints. <https://doi.org/10.2196/preprints.66398>
- Binnenlands Bestuur. (2025, 30 december). AI-gebruik leidt tot meer datalekken. <https://www.binnenlandsbestuur.nl/digitaal/ai-gebruik-leidt-tot-meer-datalekken>
- Binzer, B., & Winkler, T. J. (2022). Democratizing software development: A systematic multivocal literature review and research agenda on citizen development. In *Software Business, ICSOB 2022* (Lecture Notes in Business Information Processing, Vol. 463, pp. 244-259). Springer. https://doi.org/10.1007/978-3-031-20706-8_17
- Clarke, D., Jones, F., Harris, R., & Robert, G. (2017). What outcomes are associated with developing and implementing co-produced interventions in acute healthcare settings? A rapid evidence synthesis. *BMJ Open*, 7, Artikel e014650. <https://doi.org/10.1136/bmjopen-2016-014650>

- Demjaha, n.b. (2024). "The trivial tickets build the trust" [volledige titel n.b.]. *Journal of Cybersecurity*, 10(1), Artikel tyae007.
<https://academic.oup.com/cybersecurity/article/10/1/tyae007/7696551>
- Deng, J., Fan, Z., & Meng, R. (2026). *Understanding the (in)security of vibe-coded applications* (arXiv:2606.23130v4) [Preprint]. <https://arxiv.org/abs/2606.23130>
- Department for Business and Trade. (2025). *The evaluation of the M365 Copilot pilot in the Department for Business and Trade*. GOV.UK.
<https://assets.publishing.service.gov.uk/media/68adbe409e1cebdd2c96a19d/dbt-microsoft-365-copilot-evaluation.pdf>
- DORA. (2025). *2025 DORA state of AI-assisted software development report* (v. 2025.2). Google Cloud. <https://cloud.google.com/devops/state-of-devops>
- DORA. (2026, 12 januari). *Platform engineering* [Webpagina]. Google Cloud.
<https://dora.dev/capabilities/platform-engineering/>
- Edmondson, A. C., & Bransby, D. P. (2023). Psychological safety comes of age: Observed themes in an established literature. *Annual Review of Organizational Psychology and Organizational Behavior*, 10, 55-78. <https://doi.org/10.1146/annurev-orgpsych-120920-055217>
- Europees Parlement & Raad van de Europese Unie. (2016). Verordening (EU) 2016/679 (algemene verordening gegevensbescherming). *Publicatieblad van de Europese Unie*, L 119, 4.5.2016.
<https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679>
- Europees Parlement & Raad van de Europese Unie. (2017). Verordening (EU) 2017/745 (medische hulpmiddelen), geconsolideerde tekst van 10 januari 2025 [Publicatiegegevens n.b.].
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02017R0745-20250110>
- Europees Parlement & Raad van de Europese Unie. (2024). Verordening (EU) 2024/1689 (AI-verordening). *Publicatieblad van de Europese Unie*, 12.7.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
- Europees Parlement & Raad van de Europese Unie. (2026). Verordening (EU) 2026/1744 (Digital Omnibus on AI). *Publicatieblad van de Europese Unie*, L, 24.7.2026. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202601744
- Fowler, M. (2023, 25 juli). *Team Topologies* [Blogbericht]. martinoflower.com.
<https://martinoflower.com/bliki/TeamTopologies.html>
- Freeman, S., n.b. (2014). Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences*, 111(23), 8410-8415.
<https://www.bu.edu/eng/files/2025/01/Active-learning-increases-student-performance-in-science-engineering-and-mathematics.pdf>

- Government Digital Service. (2025, 2 juni). *Microsoft 365 Copilot experiment: Cross-government findings report*. Cabinet Office, GOV.UK.
<https://www.gov.uk/government/publications/microsoft-365-copilot-experiment-cross-government-findings-report/microsoft-365-copilot-experiment-cross-government-findings-report-html>
- Hartholt, S. (2025, 19 december). Eindhoven blokkeert ChatGPT na datalek. *Binnenlands Bestuur*.
<https://www.binnenlandsbestuur.nl/digitaal/gemeente-eindhoven-blokkeert-chatgpt-na-datalek>
- Hegedüs, A., Schürch, A., & Bischofberger, I. (2022). Implementing Buurtzorg-derived models in the home care setting: A scoping review. *International Journal of Nursing Studies Advances*, 4, Artikel 100061. <https://doi.org/10.1016/j.ijnsa.2022.100061>
- Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C. A., Dameff, C., Savage, S., & Voelker, G. M. (2025). Understanding the efficacy of phishing training in practice. In *2025 IEEE Symposium on Security and Privacy (S&P)* (paginabereik n.b.).
<https://doi.org/10.1109/SP61157.2025.00076>
- IBM. (2025). *Cost of a data breach report 2025: The AI oversight gap* [Onderzoek uitgevoerd door Ponemon Institute]. <https://www.ibm.com/reports/data-breach>
- ICTU. (n.b.). *Effectief door focus op gedrag: Unieke aanpak voor meer informatieveiligheid in de zorg* [Brochure bij het handboek *Aan de slag met informatieveilig gedrag*]. Project Informatieveilig gedrag in de Zorg, in opdracht van ActiZ, de Nederlandse ggz, NFU, NVZ, VGN en VWS. URL n.b.
- KPMG Plexus. (2015). *De toegevoegde waarde van Buurtzorg t.o.v. andere aanbieders van thuiszorg: Een kwantitatieve analyse van thuiszorg in Nederland anno 2013*.
<https://zoek.officielebekendmakingen.nl/blg-453119.pdf>
- Kunnen, Y. S., Roemeling, O. P., & Smailhodzic, E. (2023). What are barriers and facilitators in sustaining lean management in healthcare? A qualitative literature review. *BMC Health Services Research*, 23 (artikelnummer n.b.). <https://doi.org/10.1186/s12913-023-09978-4>
- Lain, D., Kostianen, K., & Čapkun, S. (2022). *Phishing in organizations: Findings from a large-scale and long-term study* (arXiv:2112.07498v1, versie van 14 december 2021) [Preprint].
<https://arxiv.org/abs/2112.07498>
- Lazzaro, S. (2025, 15 december). AI coding tools exploded in 2025. The first security exploits show what could go wrong. *Fortune*. <https://fortune.com/2025/12/15/ai-coding-tools-security-exploit-software>
- Li, B., Chen, X., & Xiong, L. (2026). Improving medication safety and efficiency in hospital pharmacy through a pharmacist-led, low-code mobile application: A prospective study. *Frontiers in Public Health*, 14, Artikel 1844863. <https://doi.org/10.3389/fpubh.2026.1844863>

- Microsoft & LinkedIn. (2024). *2024 Work Trend Index annual report: AI at work is here. Now comes the hard part*. <https://news.microsoft.com/2024/05/08/microsoft-and-linkedin-release-the-2024-work-trend-index-on-the-state-of-ai-at-work/>
- Microsoft. (2026a, 22 augustus). *Establish a Microsoft Power Platform Center of Excellence* [Webpagina]. Microsoft Learn. <https://learn.microsoft.com/en-us/power-platform/guidance/adoption/coe>
- Microsoft. (2026b, 21 april; bijgewerkt 29 augustus). *Power Platform Center of Excellence (CoE) Starter Kit overview* [Webpagina]. Microsoft Learn. <https://learn.microsoft.com/en-us/power-platform/guidance/coe/overview>
- National Cyber Security Centre. (2025, 4 juni). *Cyber security culture principles* (versie 1.0). <https://www.ncsc.gov.uk/collection/cyber-security-culture-principles>
- National Cyber Security Centre. (2026, 18 juni). *The 'vibe coding spectrum' approach to AI-assisted software development* [Blogbericht]. <https://www.ncsc.gov.uk/blogs/the-vibe-coding-spectrum-approach-to-ai-assisted-software-development>
- NOS Nieuws. (2024, 7 augustus). Privacywaakhond: pas op met gebruik AI-chatbots, ging mis bij huisarts. <https://nos.nl/artikel/2532234-privacywaakhond-pas-op-met-gebruik-ai-chatbots-ging-mis-bij-huisarts>
- NOS Nieuwsuur. (2026, 8 juni [jaar afgeleid]). Waarschuwing voor personeel dat met AI aan de slag gaat: 'Kans op datalek groot'. <https://nos.nl/nieuwsuur/artikel/2617591-waarschuwing-voor-personeel-dat-met-ai-aan-de-slag-gaat-kans-op-datalek-groot>
- O'Donovan, R., & McAuliffe, E. (2020). A systematic review exploring the content and outcomes of interventions to improve psychological safety, speaking up and voice behaviour. *BMC Health Services Research*, 20, Artikel 101. <https://doi.org/10.1186/s12913-020-4931-2>
- Ong, A. Y., Livingstone, I., Kilduff, C., Sevgi, M., Merle, D. A., Ruffell, E., Keane, P. A., & Antaki, F. (2026). *Vibe coding for clinicians: Democratising bespoke software development for digital health innovation* (arXiv:2604.22604) [Preprint]. <https://arxiv.org/pdf/2604.22604>
- OWASP. (n.b.). *OWASP Citizen Development Top 10* [Webpagina's]. OWASP. <https://owasp.org/www-project-citizen-development-top10-security-risks/>
- Perry, N., Srivastava, M., Kumar, D., & Boneh, D. (2023). Do users write more insecure code with AI assistants? In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*. <https://doi.org/10.1145/3576915.3623157>
- Q-Consult Zorg. (n.b.). *Succesvolle inzet van digicoaches binnen jouw zorgorganisatie* [Factsheet]. Q-Academie. URL n.b.

- Salvatore, M. D. (2024). *Guiding chaos into collaboration: Enhancing alignment and support for existing citizen developers and IT professionals in low code development through action research in a company setting* [Proefschrift, Drexel University].
<https://doi.org/10.17918/00010507>
- Sharwood, S. (2025, 21 juli). Vibe coding service Replit deleted user's production database, faked data, told fibs galore. *The Register*.
https://www.theregister.com/2025/07/21/replit_saastr_vibe_coding_incident/
- Shen, J. H., & Tamkin, A. (2026). *How AI impacts skill formation* (arXiv:2601.20245v2) [Preprint].
<https://arxiv.org/abs/2601.20245>
- Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, 37(1), 129-161.
<https://jmis-web.org/articles/1471>
- Slupska, J., Cho, S., Begonia, M., Abu-Salma, R., Prakash, N., & Balakrishnan, M. (2022). "They look at vulnerability and use that to abuse you": Participatory threat modelling with migrant domestic workers. In *31st USENIX Security Symposium* (pp. 323-n.b.).
<https://www.usenix.org/system/files/sec22-slupska-vulnerability.pdf>
- Spracklen, J., Wijewickrama, R., Sakib, A. H. M. N., Jadliwala, M., Maiti, A., & Viswanath, B. (2025). *We have a package for you! A comprehensive analysis of package hallucinations by code generating LLMs* (arXiv:2406.10279v3) [Preprint]. <https://arxiv.org/abs/2406.10279>
- Staatsblad. (2026). *Wet van 8 juli 2026 (Cyberbeveiligingswet)* (Stb. 2026, 187).
<https://zoek.officielebekendmakingen.nl/stb-2026-187.pdf>
- Stalker, J. (2024). Resistance. In M. Bal (Red.), *Encyclopedia of organizational psychology*. Edward Elgar. https://ueaeprints.uea.ac.uk/id/eprint/94381/1/Stalker_2024_Resistance.pdf
- Team Topologies. (n.b.). *Key concepts* [Webpagina]. <https://teamtopologies.com/key-concepts>
- Vandekerckhove, P., de Mul, M., Bramer, W. M., & de Bont, A. A. (2020). Generative participatory design methodology to develop electronic health interventions: Systematic literature review. *Journal of Medical Internet Research*, 22(4), Artikel e13780. <https://doi.org/10.2196/13780>
- Vereniging van Nederlandse Gemeenten. (2025). *AI, algoritmen en gemeenten: Position paper*.
<https://omgevingsweb.nl/wp-content/uploads/2026/03/position-paper-ai-algoritmen-en-gemeenten.pdf>
- Verizon Business. (2025). *2025 data breach investigations report*.
<https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>

Viljoen, A., Radić, M., Hein, A., Nguyen, J., & Krcmar, H. (2024). Governing citizen development to address low-code platform challenges. *MIS Quarterly Executive*, 23(3), Artikel 6.

<https://aisel.aisnet.org/misqe/vol23/iss3/6/>

Voorberg, W., Bekkers, V., & Tummers, L. (2013). *Embarking on the social innovation journey: A systematic review regarding the potential of co-creation with citizens* [Conferentiepaper].

IRSPM Conference, Praag. https://repub.eur.nl/pub/39573/Metis_187234.pdf

Weerheim, W., Van Rossum, L., & Ten Have, W. D. (2018). Successful implementation of self-managing teams. *Leadership in Health Services* (volume en artikelnummer n.b.).

<https://doi.org/10.1108/LHS-11-2017-0066>

Zhao, S., Wang, D., Zhang, K., Luo, J., Li, Z., & Li, L. (2026). Is vibe coding safe? Benchmarking vulnerability of agent-generated code in real-world tasks. In *Proceedings of the 43rd*

International Conference on Machine Learning (PMLR 306). <https://arxiv.org/abs/2512.03262>

Gedachtevoer, geen advies of besluit. [Eerlijk over het bewijs](#)