ITAGIL
WE MAKE IT EASY

UDVIKLING ODDER · OPLÆG VED ITAGIL

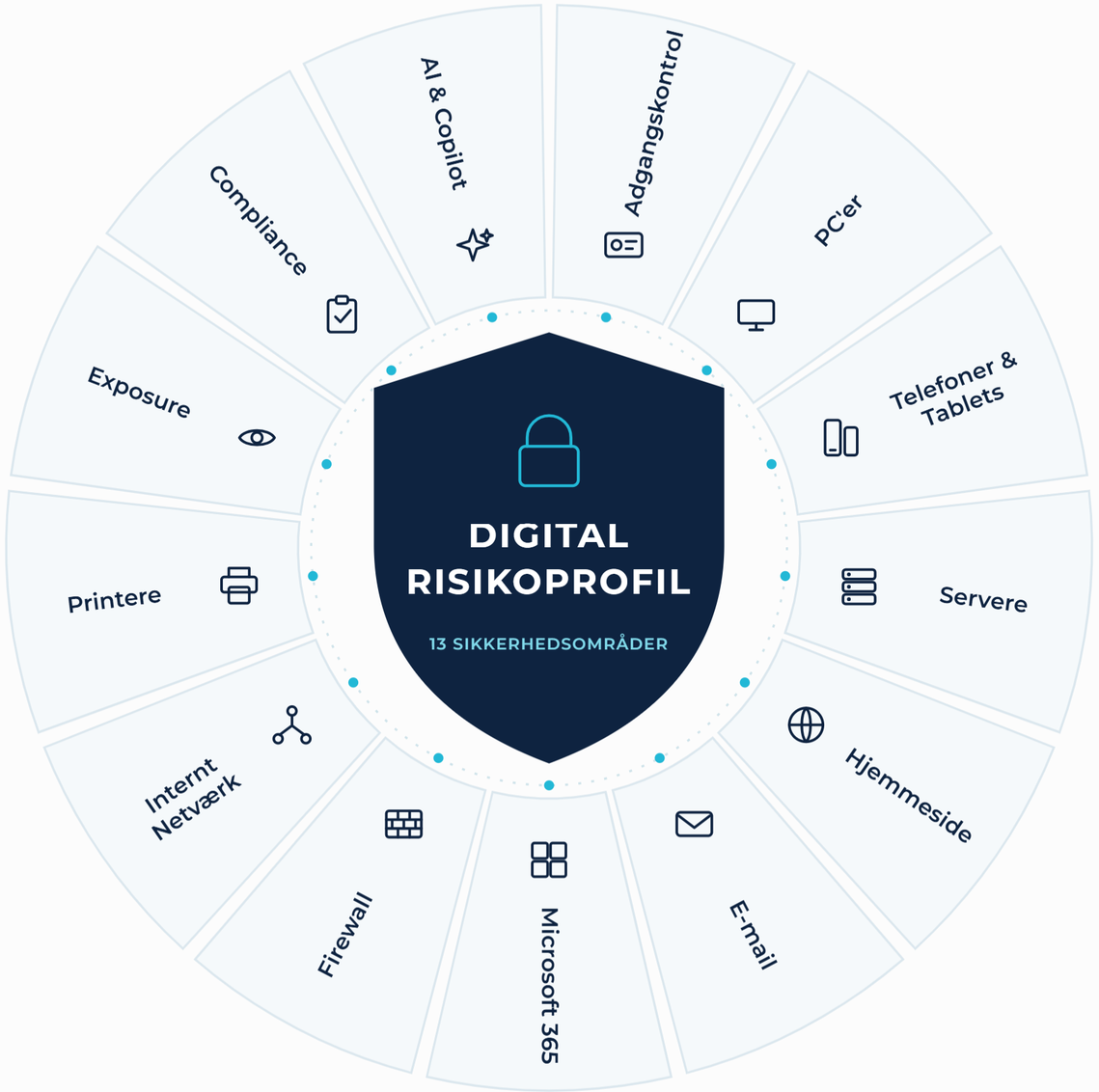
Microsoft Copilot, compliance og sikkerhed

Er jeres virksomhed – og jeres data – klar til AI?

Patrick Liebe-Lind · Business Developer & Copilot Lead, ITAGIL

HOLISTISK IT-SIKKERHEDSVURDERING

Holistisk IT-sikkerhed. Ét samlet overblik. Én klar køreplan.



KERNEBUDSKAB

ITAGIL vurderer hele IT-landskabet og tilpasser sikkerhedsanbefalingerne til organisationens specifikke risikoprofil.

RISIKOPROFIL-LAG · TRE MODENHEDSNIVEAUER

GRØN — Minimumsanbefalinger til sikkerhed – dækker de fleste organisationer.

GUL — Anbefales ved øget eksponering, fx:

- Offentligt eksponerede organisationer
- International tilstedeværelse
- Mobil arbejdsstyrke
- Kendte brands
- Åbne kontormiljøer
- 50+ medarbejdere

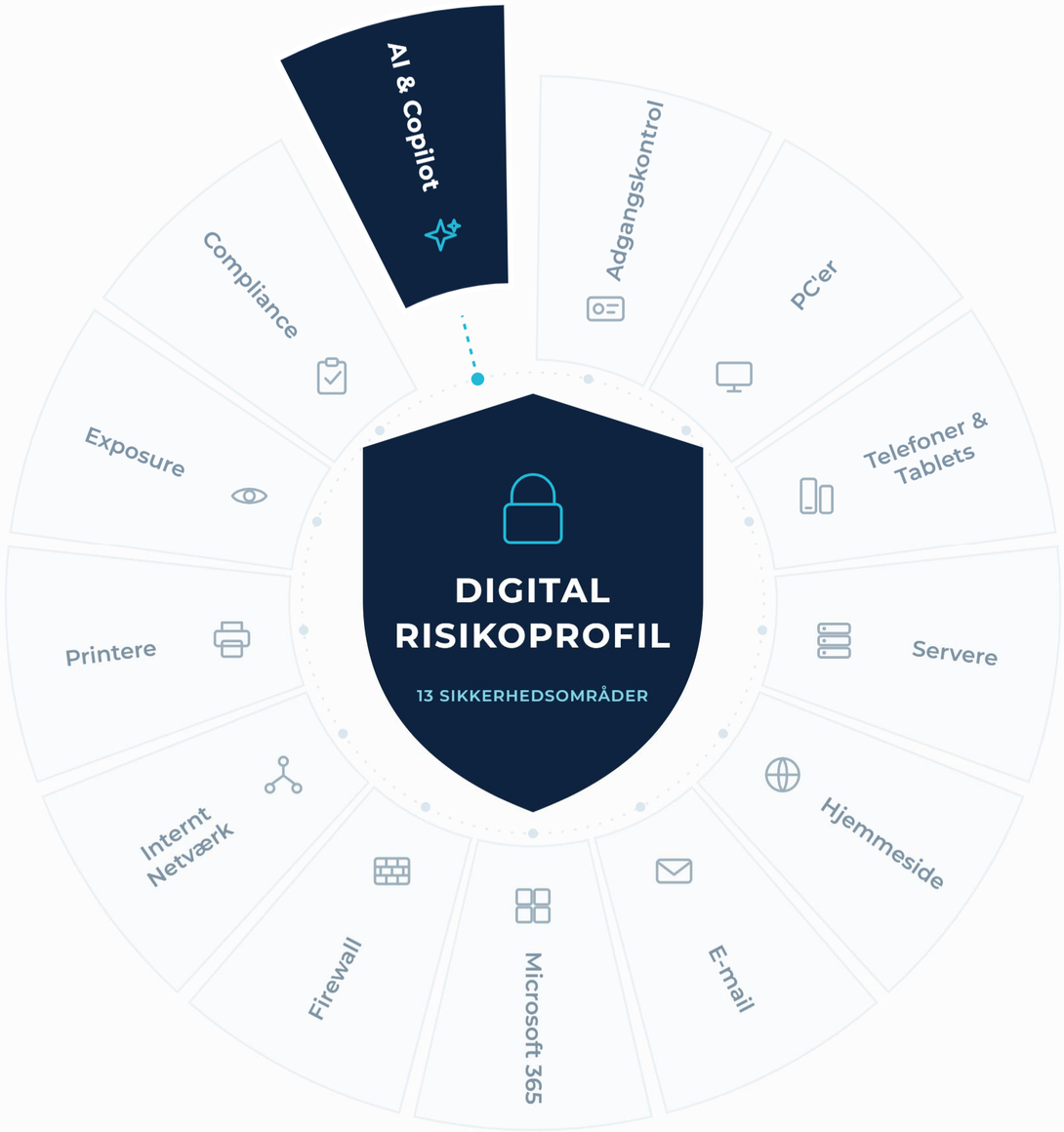
RØD — Anbefales ved forhøjet trusselsniveau, fx:

- Målrettede cyberangreb
- Følsomme persondata
- Høje compliance-krav
- Værdifuld immateriel ejendom
- NIS2-regulerede organisationer

01 **Risikoprofil** → 02 **Vurdering af 13 sikkerhedsområder** → 03 **Prioriterede anbefalinger** → 04 **Øget sikkerhedsmodenhed**

ÉT AF 13 OMRÅDER · I FOKUS I DAG

I dag handler det om AI, Copilot & sikkerhed.



DAGENS EMNE

AI & Copilot er ét af de 13 områder – og det område, hvor mest forandrer sig lige nu.

ZOOM IND PÅ AI & COPILOT

AI & Copilot

Copilot arver de rettigheder og den datastruktur, I har i forvejen. Derfor er de øvrige 12 områder – særligt Microsoft 365, adgangskontrol og compliance – forudsætningen for sikker brug af AI.

01
Rettigheder & oversharing

02
Følsomme data i Microsoft 365

03
Governance for AI-brug

04
Uddannelse af medarbejdere

01 Risikoprofil → 02 Vurdering af 13 sikkerhedsområder → 03 Prioriterede anbefalinger → 04 Øget sikkerhedsmodenhed

MULIGHEDERNE MED COPILOT

Hvad er Copilot – og hvad kan det bruges til?

Microsoft Copilot er en AI-assistent på tværs af Microsoft 365 – fra informationssøgning til automatisering og agenter.

01

FIND & FORSTÅ

Opsummér møder, mails og dokumenter.

Find svar og sammenhænge på tværs af jeres arbejdsdata.

02

SKAB & KOMMUNIKÉR

Skriv og omskriv mails, dokumenter og præsentationer.

Tilpas tone, format og længde.

03

ANALYSÉR & BESLUT

Arbejd med data, sammenlign information og identificér mønstre.

Få forslag til næste skridt.

04

AUTOMATISÉR & BYG AGENTER

Automatisér gentagne opgaver.

Byg specialiserede agenter i Copilot og Copilot Studio.

KORT SAGT

Copilot kan gå fra at svare på spørgsmål til at hjælpe med at få arbejde udført.

Funktioner og agentmuligheder afhænger af licens og opsætning.

ITAGIL WE MAKE IT EASY

MICROSOFTS RETNING

Én Copilot-oplevelse. Flere af de bedste AI-modeller.

Copilot bevæger sig fra at være bundet til én model til at fungere som et orkestreringslag for flere modeller.

> “Your work is not limited by one brand of models. Copilot hosts the best innovation from across the industry and **chooses the right model for the job** regardless of who built it.”
>
> — Microsoft webinar

01

FLERE MODELLER

Claude og ChatGPT findes nu i udvalgte Copilot-oplevelser.

02

MODEL TIL OPGAVEN

I nogle oplevelser kan Copilot automatisk vælge den rigtige model – eller brugeren kan selv vælge.

03

ENTERPRISE DATA PROTECTION

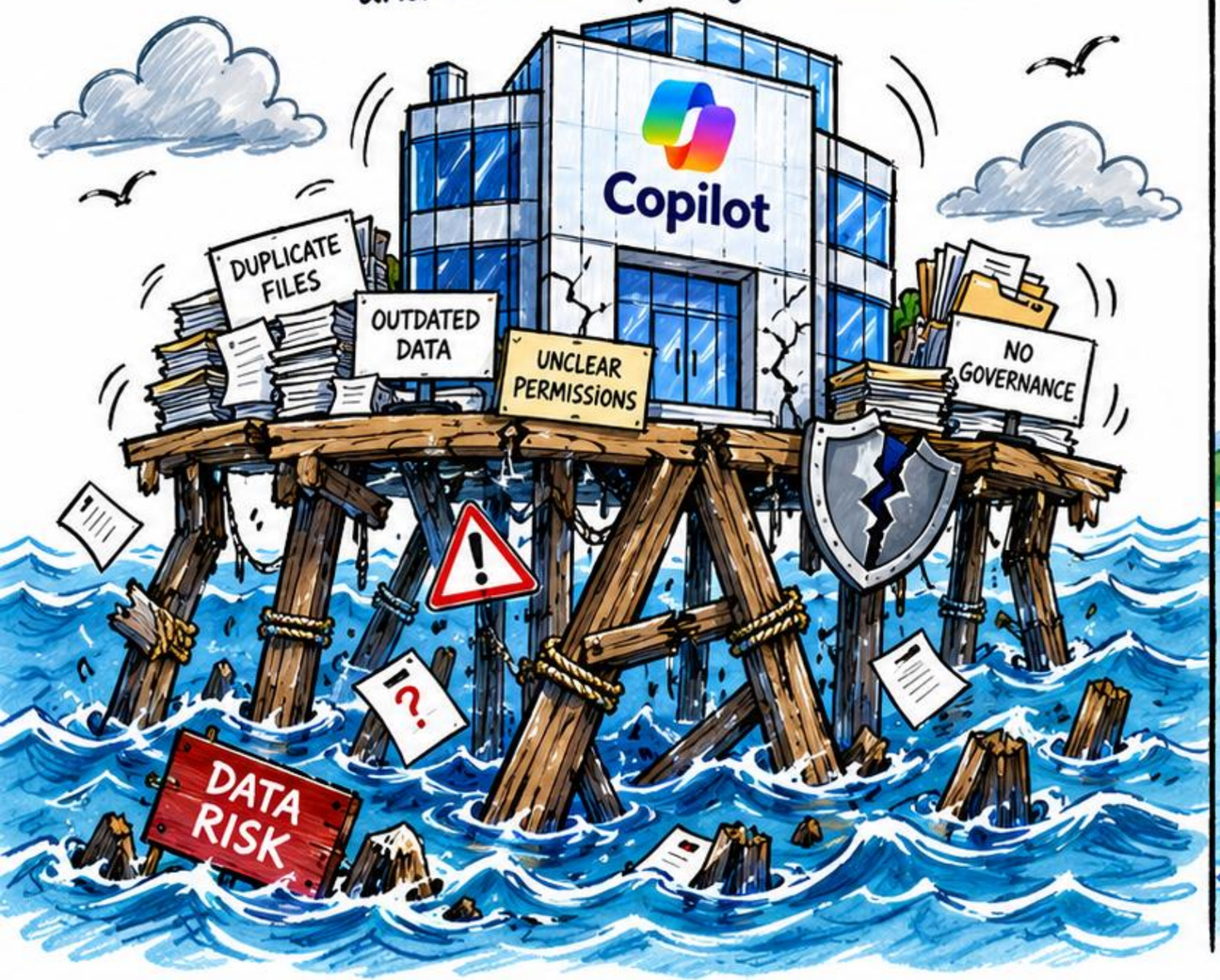
Prompts, svar og Graph-data bruges ikke til at træne foundation-modeller.

Kilder: Microsoft Learn / Microsoft Support, september 2026 · Tilgængelighed varierer efter Copilot-oplevelse, licens og tenant-indstillinger.

Copilot Needs a Strong Foundation

Weak foundation

Poor governance, unclear permissions, and low data quality create risk.



Foundation first

Secure, compliant, and well-governed data unlocks real value.

HVORDAN DET HÆNGER SAMMEN

Sådan bruger Copilot virksomhedens data

Copilot ser præcis det, brugeren selv kan se .

Copilot henter kun det frem, medarbejderen selv kan åbne i dag

Jeres data forlader ikke jeres eget miljø

ITAGIL
WE MAKE IT EASY

LAD OS RYDDE BORDET

Myter og virkelighed

MYTE

“Microsoft træner sin AI på vores data.”

VIRKELIGHED

Nej. Jeres prompts, svar og data bruges ikke til at træne modellerne – og de forlader ikke jeres eget miljø.

MYTE

“Copilot kan læse alt i virksomheden.”

VIRKELIGHED

Copilot ser præcis det, brugeren selv kan se. Udfordringen er, hvor meget det ofte viser sig at være.

MYTE

“Microsoft beskytter Copilot, så vi behøver ikke gøre noget.”

VIRKELIGHED

Microsoft passer på platformen. Hvem der har adgang til hvad hos jer, er stadig jeres beslutning.

MYTE

“Copilot skaber vores adgangsproblemer.”

VIRKELIGHED

Problemerne var der i forvejen. Copilot gør dem lette at støde ind i.

DET RIGTIGE SPØRGSMÅL

Det spørgsmål, alle stiller:

“Er Copilot sikkert?”

Det spørgsmål, der afgør resultatet:

“Er vores data klar til Copilot?”

DET VI TYPISK FINDER

- SharePoint-rettigheder ingen har rørt i årevis
- Links delt med “alle”
- Følsomme dokumenter uden mærkning

HVAD DER ÆNDRER SIG I PRAKSIS

Før skulle man vide, hvor tingene lå. Nu skal man bare spørge.

SÅDAN HAR DET VÆRET

Man leder selv – mappe for mappe.

Åbner mapper og SharePoint-sites

Ruller gennem gamle Teams-tråde og mails

Spørger en kollega, hvor det ligger

Bruger en halv time – og finder måske det halve

SÅDAN ER DET MED COPILOT

Man stiller ét spørgsmål på dansk.

Copilot leder på tværs af filer, mails og chats

Samler det, der hænger sammen

Skriver et kort svar

Det tager sekunder

POINTEN **Der er ikke kommet nye data i huset. Det er bare blevet nemt at finde dem.**

CASE FRA VIRKELIGHEDEN

Mød Bob

En helt almindelig medarbejder. I en helt almindelig virksomhed.

1

Bob arbejdede i en virksomhed, der gennemgik en større fusion.

2

HR- og personalesager blev gemt i mapper uden fuldt overblik over adgangsfordeling.

Bob

3

Bobs virksomhed tilføjede Copilot til alle i virksomheden for at følge med konkurrenterne.

4

Da Bob søgte med AI, dukkede følsomme medarbejderoplysninger op.

5

AI fandt kun data, som allerede var tilgængelige på grund af mangelfuld adgangsstyring.

POINTEN **Copilot skabte ikke adgangsproblemet. Det gjorde det bare synligt.**

ITAGIL
WE MAKE IT EASY

KERNEBEGREBET

Oversharing – flere kan se det, end vi tror

Det sker ikke, fordi nogen er uansvarlige. Det sker, fordi folk har travlt og vælger den nemme løsning.

Et SharePoint-site åbent for hele organisationen
Fordi det var nemmest, da sitet blev lavet

Folk fra afsluttede projekter har stadig adgang
Ingen lukker adgange, når et projekt slutter

Dokumenter delt med brede links
“Alle med linket” er hurtigere end at tænke over det

Eksterne i Teams, som ingen har fjernet
Og som måske selv har delt filerne videre

Lønsedler og kontrakter i fællesmapper
Ligger sammen med alt det almindelige

Sites, hvor ingen ved, hvem der ejer dem
Så er der heller ingen, der rydder op

TAG MED HJEM **Før kunne det ligge skjult i årevis. Nu kan det komme frem i et svar.**

ITAGIL
WE MAKE IT EASY

FUNDAMENTET

Identitet er hoveddøren

Sikker brug af AI starter samme sted som al anden sikkerhed: hos den, der er logget ind.

Multifaktor

På alle brugere – også dem, der plejer at få dispensation.

Conditional Access

Betingelser for hvornår, hvorfra og fra hvilken enhed der logges ind.

Ekstern deling

Eksterne må ikke kunne dele filer og mapper videre, som de ikke selv ejer.

Rigtige brugerkonti

Ikke delte logins, som flere personer bruger i fællesskab.

Mindst mulig adgang

Folk har det, de skal bruge nu – ikke det, de engang skulle.

Administratorkonti

Færre, kendte og bedst beskyttede.

DERFOR **Bliver en konto overtaget, arbejder Copilot med den kontos adgang.**

DATA OG KLASSIFIKATION

Klassifikation gør reglerne konkrete

Sæt en mærkat på, hvor følsomt indholdet er – og lad teknikken håndhæve det.

Offentlig	Må deles frit · ingen beskyttelse nødvendig
Intern	Følsomhedsmærkat “Intern” · ingen anonyme links · deling kun internt
Fortrolig	Mærkat med kryptering · DLP blokerer ekstern deling · adgang på navngivne grupper
Stærkt fortrolig	Kryptering følger filen · rettigheder kan trækkes tilbage · al adgang logges

Værktøjerne ligger i Microsoft Purview. Hvor meget I kan bruge, afhænger af licens og opsætning. Start med to-tre niveauer, I kan holde – ikke fire, der aldrig bliver brugt.

VIGTIGT **Copilot respekterer mærkater og DLP-regler – men kun hvis de er sat op.**

ITAGIL
WE MAKE IT EASY

COMPLIANCE

Fire spørgsmål en ledelse bør kunne svare på

1

Hvilke personoplysninger kan medarbejderne komme til?

Ikke hvad de bruger – hvad de kan åbne.

2

Hvorfor har de den adgang?

Er der en grund i dag – eller er den historisk?

3

Hvor længe gemmer vi informationen?

Har vi taget stilling – eller gemmer vi alt?

4

Kan vi undersøge, hvad der skete, hvis noget går galt?

Kan vi se, hvem der så hvad hvornår?

AT HUSKE **Svarene bliver ikke lettere efter udrulningen. Copilot-aktivitet kan logges med Microsoft 365's compliance-funktioner – afhængigt af licens og opsætning.**

ANSVARSDELING

Microsoft leverer rammerne. I bestemmer indholdet.

MICROSOFT LEVERER

En sikker og krypteret platform

At jeres data er adskilt fra andre kunders

Værktøjerne til at styre adgang, deling og opbevaring

I BESTEMMER

Hvem der har adgang til hvad

Hvad der må deles, og hvor længe det gemmes

Hvordan medarbejderne må bruge AI

KORT SAGT **Sikker platform + svag styring ≠ sikker brug af AI**

EN RAMME

Fem områder, før Copilot rulles ud

01

IDENTITET

MFA på alle. Færre administratorer. Betinget adgang slået til.

02

ADGANGE

Luk gamle rettigheder. Fjern brede links. Sæt en ejer på hvert site.

03

DATA

Find ud af, hvor det følsomme ligger – og sæt en mærkat på det.

04

GOVERNANCE

Skriv reglerne ned for adgang, deling og opbevaring. Slå dem til.

05

MENNESKER

Kort oplæring og klare regler for, hvad man må skrive ind i AI.

BEMÆRK **Ingen af de fem områder handler om Copilot. De handler om Microsoft 365.**

ITAGIL
WE MAKE IT EASY

MINI-SELVTEST

Ville I være rolige ved Copilot i morgen?

Svar for jer selv: **JA** · **IKKE SIKKER** · **NEJ**

	JA	IKKE SIKKER	NEJ
Vi ved, hvem der har adgang til vores vigtigste SharePoint-sites			
Vi har styr på, hvad eksterne kan se og dele videre			
Vi ved, hvor vores følsomme dokumenter ligger			
Vi lukker adgange, når folk skifter job eller stopper			
Vi har taget stilling til, hvad der må deles, og hvor længe vi gemmer det			
Vi har sagt til medarbejderne, hvad de må skrive ind i AI-værktøjer			

HVIS FLERE ER "IKKE SIKKER" **Så er det første, I skal bruge penge på, måske ikke licenser.**

TIL SIDST

“Copilot er kun så klar til jeres virksomhed, som jeres virksomhed er klar til Copilot.”

01

Copilot ser præcis det, brugeren selv kan se.

02

Den reelle risiko er, at rod i adgangene bliver let at finde.

03

Det starter med identitet, adgange, data og mennesker.

“Hvis I gav Copilot til alle medarbejdere i morgen – hvad ville I være mest usikre på?”