

Når angriperen ser legitim ut.

Hva skal fortsatt stoppe en farlig handling når meldingen er troverdig, kontoen er ekte og innloggingen er godkjent?

IANS · Henrik Bergfjord · 17. oktober 2026

Selvstendig analyse med KI-assistanse · Kilder kontrollert samme dag · Versjon 1.0

01 · VÅR VURDERING

Vi må beskytte beslutningen, ikke bare innloggingen.

Den viktigste endringen vi leser ut av IOCTA 2026, er kombinasjonen av ferdige kriminelle tjenester, gjenbrukte data, troverdig kommunikasjon og raskere arbeidsflyter. KI kan forsterke dette. Men virksomheten kan tape penger eller data uten at angriperen har en spesielt avansert KI-modell.

Vår hovedvurdering: Sikkerhet bør bygges slik at én vellykket imitasjon eller én kompromittert konto ikke er nok til å endre en bankkonto, overta identiteten eller hente ut de mest verdifulle dataene. Det er et krav til arbeidsprosessen og systemene, ikke bare til den ansattes årvåkenhet.

En korrekt innlogging er et bevis på en autentiseringshendelse. Den er ikke et løfte om at alle etterfølgende handlinger er riktige.

Vi ville derfor prioritert sterke innlogginger, kontrollert gjenoppretting og tydelige handlingsgrenser før en stor innkjøpsrunde med nye sikkerhetsprodukter. Samtidig må patching, enhetssikring, logging og gjenoppretting fortsette. En identitetsstrategi beskytter ikke en upatchet, internettekspontert tjeneste.

DOKUMENTERT

Kriminaliteten er en verdikjede

Europol beskriver spesialiserte markeder, tilgangsmeglere, infostealere og ransomware-tjenester. Aktørene kan kjøpe deler av operasjonen. [\[1. s. 12–15, 23–28\]](#)

IANIS-VURDERING

Det billige steget kan avgjøre

Når sikker innlogging gjør ett steg vanskeligere, bør vi forvente press mot support, gjenoppretting, appgodkjenning og normale arbeidsrutiner. Forsvaret må dekke disse overgangene.

BETINGET UTVIKLINGSBANE

Flere oppgaver kan automatiseres

Det gjør det fornuftig å redusere tiden fra avvik til stopp. Det gir ikke grunnlag for et bestemt årstall for fullt autonome angrep mot alle virksomheter.

02 · HVA MATERIALET TÅLER

En sterk trusselbeskrivelse er ikke en sannsynlighetsmodell.

IOCTA er et politifaglig situasjonsbilde. Metodedelen beskriver et hovedsakelig kvalitativt grunnlag fra større etterforskninger støttet av Europol i 2025, supplert med ekspertkunnskap og andre rapporter. Dette er verdifullt for å forstå metoder og sammenhenger, men ikke et representativt utvalg av alle norske virksomheter. [\[1, s. 38\]](#)

Den vedlagte norske syvsidersrapporten er et nyttig arbeidsnotat. Vi bruker den som et utgangspunkt som skal prøves mot primærkildene, ikke som en uavhengig bekreftelse av Europol. Rangeringer som «svært høy» i notatet videreføres derfor ikke som tallfestet eller kalibrert risiko.

Hva tallene sier – og ikke sier		
Kildeobservasjon	Rimelig slutning	Det kan vi ikke slutte
Over 120 aktive ransomware-brands observert i 2025	Et fragmentert økosystem med overlapp og omprofilering. [1, s. 23–24]	At det finnes 120 uavhengige grupper, eller at en norsk virksomhets risiko har økt med en bestemt prosent.
Minst 1 200 SIM-box-enheter, 40 000 SIM-kort og over 49 millioner opprettede nettkontoer i én sak	Kriminell identitets- og kommunikasjonsinfrastruktur kan drives industrielt. [1, s. 19]	At 49 millioner personer ble hacket, eller at alle de opprettede kontoene er bekreftede ofre.
Generativ KI i blant annet kodehjelp og samtaleskript; agentisk KI omtales også	En blanding av eksisterende hjelpemidler og utvikling mot mer automatisering. [1, s. 15, 21, 36–37]	At alle kriminelle arbeidsflyter allerede er autonome, eller at rapporten dokumenterer selvreplicherende KI i vanlige hjem.

Europol bruker sterkere fremtidsformuleringer på side 36 enn den mer nyanserte omtalen av dagens bruk på side 21. Vi behandler dette som en grunn til å være tydelige om usikkerhet, ikke til å velge den mest dramatiske formuleringen. NSMs Risiko 2026 gir et norsk korrektiv: sosial manipulering og mer avansert phishing er også observert her. Det er ikke det samme som at alle MFA-metoder har mistet verdi. [\[2, PDF s. 24\]](#)

Passnøkler er et viktig løft. Gjenoppretting er også en inngang.

Vi støtter en planlagt overgang fra SMS-koder til phishing-resistent autentisering for kritiske kontoer. NSM anbefaler robuste MFA-løsninger, strukturert utrulling og jevnlig revisjon. Ikke fjern eksisterende MFA før en fungerende erstatning og gjenoppretting er på plass. [\[3\]](#)

En SIM-farm som oppretter mange kontoer, SIM-bytte som overtar et telefonnummer og falsk avsender-ID er forskjellige mekanismer. Samlet viser de hvorfor telefonnummeret er et svakt, universelt tillitsanker. Men ingen av dem alene beviser at enhver SMS kan avlyttes. SMS kan fortsatt brukes til praktiske beskjeder; den bør ikke alene avgjøre en kritisk godkjenning.

Det oversette spørsmålet er hvem som får registrere neste passnøkkel. Hvis support kan fjerne den gamle faktoren etter en overbevisende telefonsamtale, kan en sterk innlogging få en svak bakdør gjennom rutinen. Vår anbefaling er at ny faktor, ny enhet og gjenoppretting behandles som egne sikkerhetshendelser: med kjent identitet, dokumentert kontroll, varsling og sporbarhet. Høyrisikoendringer bør ha separat godkjenning.

Synkroniserte passnøkler, enhetsbundne nøkler og fysiske sikkerhetsnøkler har ulike avhengigheter. En synkronisert løsning må også vurderes ut fra skykontoen og dens gjenoppretting. For administratorer kan enhetsbundet nøkkel, separat adminidentitet og en reservenøkkel i kontrollert oppbevaring være et godt valg. Dette er et rollebasert designvalg, ikke et argument mot passnøkler generelt.

Phishing-resistent innlogging fjerner heller ikke behovet for å beskytte enheten og sesjonen. Skadevare på en legitim PC eller misbruk av en allerede etablert sesjon må møtes med flere lag. Microsoft beskriver både forebygging, deteksjon og vern mot gjenbruk av stjålne tokens. Token Protection har konkrete plattform-, app- og klientbegrensninger som må kontrolleres før utrulling; det er ikke et universelt vern for alle nettleserøkter. [\[4\]](#)

1

Opprette / gjenopprette

Hvem bekrefter personen og den nye faktoren?

2

Logge inn / bruke sesjon

Er faktor, enhet og sesjon tilstrekkelig beskyttet?

3

Gjøre noe kritisk

Er akkurat denne handlingen godkjent og avgrenset?

4

Stoppe / etterprøve

Kan vi stanse tilgang og finne berørte data?

Kontroller som bruker samme kompromitterte konto, enhet eller administrator kan svikte sammen. To meldinger i to apper er derfor ikke automatisk to uavhengige kontroller.

Behold Teams. Gjør grensene forståelige og testbare.

Å erstatte Teams med en annen chat løser ikke tilliten til en kompromittert kollega eller en falsk supporthenvendelse. Vi ville heller skilt mellom ekstern chat, gjestemedlemskap og delte kanaler. De gir forskjellige typer tilgang og må ikke behandles som én bryter. Et godkjent eksternt domene reduserer eksponering, men gjør ikke alle kontoer på domenet trygge.

Her trenger arbeidsnotatet en teknisk presisering: Teams' grunnleggende beskyttelse mot skadelige URL-er viser varsler. Microsoft skiller dette fra Safe Links, som kan kontrollere og blokkere ved klikk med riktig lisens og oppsett. Et advarselsbanner er ikke en teknisk sperre. [5]

Det er også forskjell på datatapssikring, DLP, for chatmeldinger og for filer. Filer delt gjennom Teams ligger i SharePoint eller OneDrive og må omfattes der. En etikett eller policy på ett sted gir ikke automatisk full dekning overalt. Test faktisk blokkering, varsling og eventuelle overstyringer med ufarlige testdata. [6]

IANS-forslag: start med handlingen og konsekvensen		
Informasjon / handling	Vår foreslåtte grense	Kontroll som bør prøves
Vanlig prosjektarbeid	Del i et arbeidsrom med tydelig eier og relevant medlemskap.	Kan tidligere deltakere fortsatt lese eller dele?
Kunde-, person- og kommersielle data	Klassifiser etter faktisk innhold og skade; avgrens mottakere og deling. Ikke alle persondata har samme risiko.	Kan en uautorisert gjest eller uadministrert enhet åpne testfilen?
Betaling eller endring av bankkonto	Dialog i chat er tillatt; godkjenning skjer i kontrollert økonomiflyt.	Kan én person endre mottaker og godkjenne betaling alene?
Passord, API-nøkler og recovery-koder	Ikke i ordinær chat. Bruk en godkjent løsning for hemmeligheter og avgrenset utlevering.	Er nøkler fortsatt gyldige etter at noen har delt dem feil?

For omfattende blokkering kan skyve arbeidet over i private apper, skjermbilder og uregistrerte unntak. Vår vurdering er derfor at hver begrensning må følges av en fungerende, enkel vei for legitimt arbeid. Det er en del av sikkerhetsdesignet, ikke bare et spørsmål om brukervennlighet.

Den nye faren er også hva vår egen automatisering får gjøre.

IOCTA beskriver KI som en forsterker av kriminelle prosesser. Vår videre vurdering er at virksomhetens egen KI-utrulling kan forstørre konsekvensen av gamle tilgangsproblemer: enklere søk, sammenstilling og handling gjør brede rettigheter mer verdifulle å misbruke. Det betyr ikke at KI skaper rettighetene eller automatisk omgår dem.

Microsoft opplyser at Microsoft 365 Copilot bare henter organisasjonsinnhold brukeren har rett til å se. Agentutvidelser har egne tillatelser og vilkår som også må vurderes. Vår anbefaling er å rydde brede tilganger og gjøre dataeierskap tydelig før stor utrulling. Ikke forveksle et fravær av tilgangsbrudd med riktig tilgangsdesign. [7]

En assistent som bare oppsummerer et godkjent dokument har et annet skadepotensial enn en agent som kan sende e-post, dele filer eller godkjenne endringer. Vi ville startet med leseadgang til avgrensede data, eget formål og eier, små handlingsrammer og menneskelig godkjenning utenfor agentens egen kontroll for kritiske steg. Ubetrodd dokumentinnhold må ikke få bestemme verktøytilgang eller overstyre godkjenningsregler.

Kontrollen må også omfatte ikke-menneskelige identiteter: integrasjoner, tjenestekontoer og apper. En brukers passnøkkel hjelper lite mot en fortsatt gyldig integrasjon med for vide rettigheter. Kartlegg eier, formål, datatilgang og hvordan tilgangen trekkes tilbake. Dette er en IANS-anbefaling om styring, ikke et funn om at et bestemt Copilot-opplett er sårbart.

06 · PRØV TANKEGANGEN

Tre forløp som avslører forskjellige hull.

Dette er konstruerte øvingsscenarioer, ikke rapporterte hendelser hos IANS eller en navngitt virksomhet. Åpne hvert forløp og se hvor en uavhengig kontroll bør ligge.

▼ 1. Ekte konto, feil betalingsbeslutning

Forløp: En melding fra en kompromittert samarbeidspartner ber om nytt kontonummer. Den passer inn i en eksisterende dialog. En kjent stemme i telefonen bekrefter at det haster. Medarbeideren logger inn helt korrekt og endrer betalingsmottaker.

Det som ikke er nok: Språkkontroll, avsendernummer og sterk innlogging hos medarbeideren. Alle kan være i orden samtidig som forespørselen er feil.

Bruddpunkt: Endringen må verifiseres mot en tidligere etablert kontakt og godkjennes av en annen person i økonomisystemet. Samtalen er støtteinformasjon, ikke sluttgodkjenning. Tilbakeoppringing til kjent nummer er bedre enn svar til avsenderen, men er heller ikke tilstrekkelig alene dersom kontakten eller telefonen er overtatt.

Bevis i øvelsen: Loggen viser hvem som endret opplysningene og hvem som godkjente. Den samme personen kan ikke fullføre begge steg.

▼ 2. Passnøkkel på plass, gjenoppretting som omvei

Forløp: «Jeg har mistet telefonen og skal inn i et viktig møte.» En falsk henvendelse får support til å nullstille en faktor. En ny faktor registreres og brukes til helt normal pålogging.

Det som ikke er nok: At nesten alle innlogginger bruker en sterk metode. Statistikken kan være god mens etableringen av nye metoder er svak.

Bruddpunkt: Support skal ha en dokumentert identitetskontroll som ikke kan tilfredsstilles bare med opplysninger fra e-post eller chat. Kritiske roller krever en separat godkjenner og en kontrollert reservevei. Unntak må ha eier og utløp.

Bevis i øvelsen: Et ufarlig reset-forsøk uten riktig dokumentasjon blir avvist. Uventet faktorregistrering utløser varsel med en ansvarlig mottaker. En legitim bruker kan likevel få hjelp gjennom den godkjente rutinen.

▼ 3. Data tatt ut, men ingen filer er kryptert

Forløp: En kompromittert enhet, sesjon eller integrasjon leser mer informasjon enn den trenger. Data samles og hentes ut. Virksomheten oppdager utpressingskravet før driftsstans.

Det som ikke er nok: At alle tjenester fortsatt virker og at backup kan gjenopprettes. En kopi hos angriperen forsvinner ikke ved restore.

Bruddpunkt: Små tilgangsområder, kontrollert eksport, overvåking av relevante avvik og en øvd vei for å stanse bruker-, sesjons- og apptilgang. Ikke anta at passordbytte alene avslutter alle former for tilgang.

Bevis i øvelsen: Kan vi med testdokumenter finne hva som ble lest og delt, få stoppet tilgangen og avklare ansvar for hendelsen? Loggdekning og oppbevaring må være bestemt før hendelsen.

07 · TO FORSKJELLIGE TAP

Backup løser tilgjengelighet. Ikke hele utpressingen.

Europol beskriver et økende press rundt offentliggjøring av stjalne data, i tillegg til kryptering og andre pressmidler. Det betyr ikke at kryptering har sluttet å være farlig. Vi må planlegge for både tappt drift og tappt kontroll over informasjon. [\[1. s. 23–25\]](#)

Vår anbefaling er å teste to spor separat: Kan vi gjenopprette tjenesten innen akseptabel tid, og kan vi håndtere at dokumenter allerede er kopiert? Det andre sporet krever kunnskap om hvilke data som finnes, hvem de gjelder og hvem som skal ta beslutninger og kommunisere. En slettepåstand fra en utpresser er ikke et teknisk bevis på at kopiene er borte.

En backup som styres av samme høyt privilegerte identitet som resten av miljøet kan gi en felles feilårsak. Uforanderlig eller offline backup, separate administrative grenser og prøvd restore er derfor en bedre test enn bare en grønn «backup OK»-status. Leverandørens tilgang og gjenopprettingsmulighet må inngå i øvelsen.

For leverandøravhengige virksomheter ville vi dessuten avklart hva som skjer hvis identitetsleverandøren, driftspartneren eller samhandlingsplattformen er utilgjengelig. En beredskapskontaktlister som bare ligger i den rammede e-posten, er et svakt utgangspunkt. Dette er et argument for øvd reservekommunikasjon og avgrensede avhengigheter, ikke for å avskaffe skytjenester.

Hva kan endre prioriteringene frem mot 2030?

Vi har ikke grunnlag for presise prosenter eller et årstall der én teknologi «vinner». Følgende er betingede hypoteser for planlegging. Alle bygger på at økonomi, teknisk kvalitet, tilgang til ofre og mottiltak kan endre utviklingen.

IANS-hypoteser for 2026–2030		
Hvis dette skjer	Vår forventede konsekvens	Hva bør vi følge med på?
Mer av svindelarbeidet blir billig å automatisere	Flere troverdige forsøk per ansatt og kortere tid mellom henvendelse og skade. Prosesskontroller får større verdi.	Egne hendelsesforløp og responstider. Hvis automatiseringen gir lav suksess og stoppes tidlig, svekkes antakelsen om større skade.
Sterke innlogginger blir utbredt	Relativt større press mot recovery, sesjoner, apprettigheter og legitime godkjenninger.	Faktorendringer, supportunntak og nye apptillatelser. Redusert omgåelse uten flytting til andre innganger vil utfordre hypotesen.
KI-agenter får mer handlingsrom	En feil i mandat eller datatilgang kan forplante seg raskere til deling eller handling.	Hvilke apper kan skrive, sende og godkjenne? Hvis robuste grenser holder og effekten uteblir, skal vurderingen justeres.

Vi ville brukt 2030 som retning for arkitektur, ikke som frist for grunnsikring. Tiltakene under er nyttige også i en verden der KI utvikler seg saktere enn ventet. Det gjør dem mindre avhengige av at den mest dramatiske prognosen slår til.

Start med grensene som stopper et reelt tap.

Dette er et forslag til rekkefølge for en vanlig norsk virksomhet, ikke en bestilling på en bestemt Microsoft-lisens. Velg tilsvarende funksjoner i det miljøet dere faktisk bruker. Kartlegging, kapasitet og virksomhetskritiske tjenester må styre tempoet.

Foreslått 12-måneders plan – periodene regnes fra oppstart		
Når / ansvar	Leveranse	Slik vet vi at den virker
0–30 dager Ledelse, økonomi og IT	Finn kritiske handlinger, kontoer, MFA-/recovery-veier, eksterne tilganger og dataeiere. Avklar betalingskontroll, patching og beredskap.	Alle kritiske handlinger har navngitt eier og kontroll. Dokumenter hvert unntak; bekreft at to-personersregelen faktisk håndheves.

Når / ansvar	Leveranse	Slik vet vi at den virker
30–90 dager Identitets- og supportansvarlig	Pilotér phishing-resistent innlogging for administratorer, økonomi og andre utsatte roller. Sikre registrering og gjenoppretting. Behold testede nødveier.	Prøv både en legitim og en falsk reset-henvendelse. Avvis svak fallback der erstatning virker; mål gjenværende unntak og brukerstøttebelastning.
3–6 måneder Dataeiere, IT og leverandør	Rydd gruppelemskap og deling. Test enhetskrav, lenkebeskyttelse og DLP. Kartlegg app-/agenttilganger. Rull først ut i test-/rapportmodus der det er mulig.	En ufarlig sensitiv testfil kan ikke åpnes av feil mottaker. Et viktig, legitimt arbeidsforløp fungerer fortsatt. Ingen kontroll regnes som aktiv bare fordi lisensen er kjøpt.
6–12 måneder Beredskap sleder og tjenesteeiere	Øv kompromittert konto, support-reset, dataeksport og separat restore. Reduser de gjenværende kritiske unntakene. Revider leverandørtilgang.	Øvelsen har tidslinje fra første signal til verifisert stopp, dokumentert datagrense og prøvd gjenoppretting. Funn får eier og frist.

For den mindre virksomheten

Begynn med et kort, gjennomførbart minimum: sterk innlogging for sentrale kontoer, en trygg support-/recovery-rutine, uavhengig betalingsgodkjenning, vedlikeholdte enheter, begrenset deling og testet backup. Avtal med driftspartneren hvem som oppdager og stopper en hendelse. Ikke kjøp overvåking uten en avtale om hvem som faktisk følger opp varslet.

Mål effekt fremfor antall produkter

- Andel kritiske kontoer med både phishing-resistent innlogging og kontrollert recovery. Oppgi teller og nevner, ikke bare «MFA aktivert».
- Antall kritiske unntak uten eier eller sluttdato; antall integrasjoner uten ansvarlig.
- Tid fra testhendelse til oppdagelse, beslutning og verifisert stans. Skill øvingsresultater fra reelle hendelser.
- Resultat av restore og av forsøk på uautorisert åpning/deling av testdata. Et avvik skal ikke kunne skjules i et samlet modenhetstall.

Vi setter ikke universelle minuttmaal eller «100 % sikker»-maal her. Den enkelte tjenestens tålegrense og observerte grunnlinje må bestemme akseptkriteriene. Øvelser med personopplysninger og sikkerhetslogger må avgrenses etter formål, tilgang og oppbevaring; mer overvåking er ikke automatisk bedre sikkerhet.

Unngå å gjøre tillitsproblemet til et produktproblem.

Vi ville ikke avviklet telefon eller Teams generelt, slått av all ekstern samhandling, behandlet enhver ansatt som mistenkt eller lovet at en passnøkkel løser hele problemet. Vi ville heller ikke ventet på et perfekt KI-basert forsvar før grunnleggende feil ble rettet.

Europol beskriver hvordan kryptering og anonymisering vanskeliggjør etterforskning. Det er et reelt politifaglig perspektiv, men ikke i seg selv et bevis på at svakere kryptering gir bedre samlet sikkerhet. Virksomheter og innbyggere trenger også beskyttelse mot avlytting og datatyveri. Vår vurdering er å bevare sterk kryptering og samtidig sikre relevant, forholdsmessig sporbarhet og lovlig håndtering av hendelser. [\[1, s. 6–9\]](#)

Rapportens kapittel om overgrep og utpressing mot barn viser dessuten at cyberkriminalitet ikke bare er en virksomhetsrisiko. Denne analysen avgrenser seg til organisasjoners identitet, samhandling og data. Den dekker ikke hele Europols mandat eller alle konsekvenser for barn og privatpersoner.

Det avgjørende spørsmålet er ikke bare: «Stoler vi på denne brukeren?»
Det er også: «Hvilken skade kan denne brukeren, sesjonen eller agenten gjøre uten at noen andre griper inn?»

Vårt råd er å teste svaret før det haster. Et godt design gjør det mulig å samarbeide og bruke KI, samtidig som det setter en praktisk grense for hva én feil kan koste.

Hva bygger vi dette på?

Primærgrunnlaget er den vedlagte IOCTA-PDF-en på 43 sider. Sidetallene i analysen viser PDF-/trykksidene. Nettutgaven er kontrollert hos Europol. De tekniske veiledningene under beskriver produkter og kan endres; kontrollerer gjeldende støtte og lisens før gjennomføring.

1. [Europol: The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – IOCTA 2026.](#) 2026; Europols oversikt oppgir publisering 28. april 2026. Særlig s. 12–15, 18–21, 23–28, 36–38. DOI 10.2813/5737847. Politifaglig og hovedsakelig kvalitativt grunnlag fra 2025. [Europols IOCTA-oversikt.](#)
2. [NSM: Risiko 2026.](#) 2026, PDF s. 24. Brukt som norsk kontekst for sosial manipulering, avansert phishing og utpressing; ikke som en frekvensmodell for enkeltvirksomheter.
3. [NSM: Flerfaktoraautentisering.](#) Publisert og oppdatert 12. desember 2024. Produktnøytrale anbefalinger om robuste metoder, utrulling og kontroll. Våre konkrete recovery- og rollevalg er egne anbefalinger.
4. [Microsoft: Protecting tokens in Microsoft Entra og Token Protection i Conditional Access.](#) Første veiledning sist oppdatert 25. april 2025; støtteoversikten kontrollert 17. oktober 2026. Underlag for å skille autentisering, enhet og sesjonsvern. Støtte og lisens må verifiseres i eget miljø.
5. [Microsoft: Malicious URL Protection in Microsoft Teams.](#) Sist oppdatert 28. januar 2026 i den kontrollerte nettutgaven. Underlag for skillet mellom grunnleggende varsling og Safe Links ved klikk.
6. [Microsoft: Data loss prevention and Microsoft Teams.](#) Kontrollert 17. oktober 2026. Underlag for skillet mellom chat, filer i SharePoint/OneDrive, policyomfang og lisensavhengigheter.
7. [Microsoft: Data, privacy and security for Microsoft Copilot.](#) Kontrollert 17. oktober 2026. Brukt for opplysninger om brukerrettigheter og agentutvidelser; ikke som en generell attest for enhver KI-tjeneste.

Arbeidsnotat og egen analyse

«Trusseltrender 2026–2030 – basert på Europol IOCTA 2026 og supplerende sikkerhetsråd», syv sider, mottatt fra brukeren 17. oktober 2026. Dokumentet har ikke en tydelig oppgitt utgiver og behandles som et sekundært arbeidsnotat. Den medfølgende samtaleteksten er bakgrunn, ikke en kildeautoritet. Ingen av de to er publisert som en ny, uavhengig primærkilde her.

Prioriteringer, kontrollmodellen, øvingsscenarioene, utviklingsbanene og tiltaksplanen er IANS' egne vurderinger utarbeidet med KI-assistanse. Vi har ikke målt en konkret virksomhets risiko eller undersøkt en faktisk Microsoft 365-tenant. Dette er et åpent beslutningsgrunnlag som må prøves mot lokale forhold.