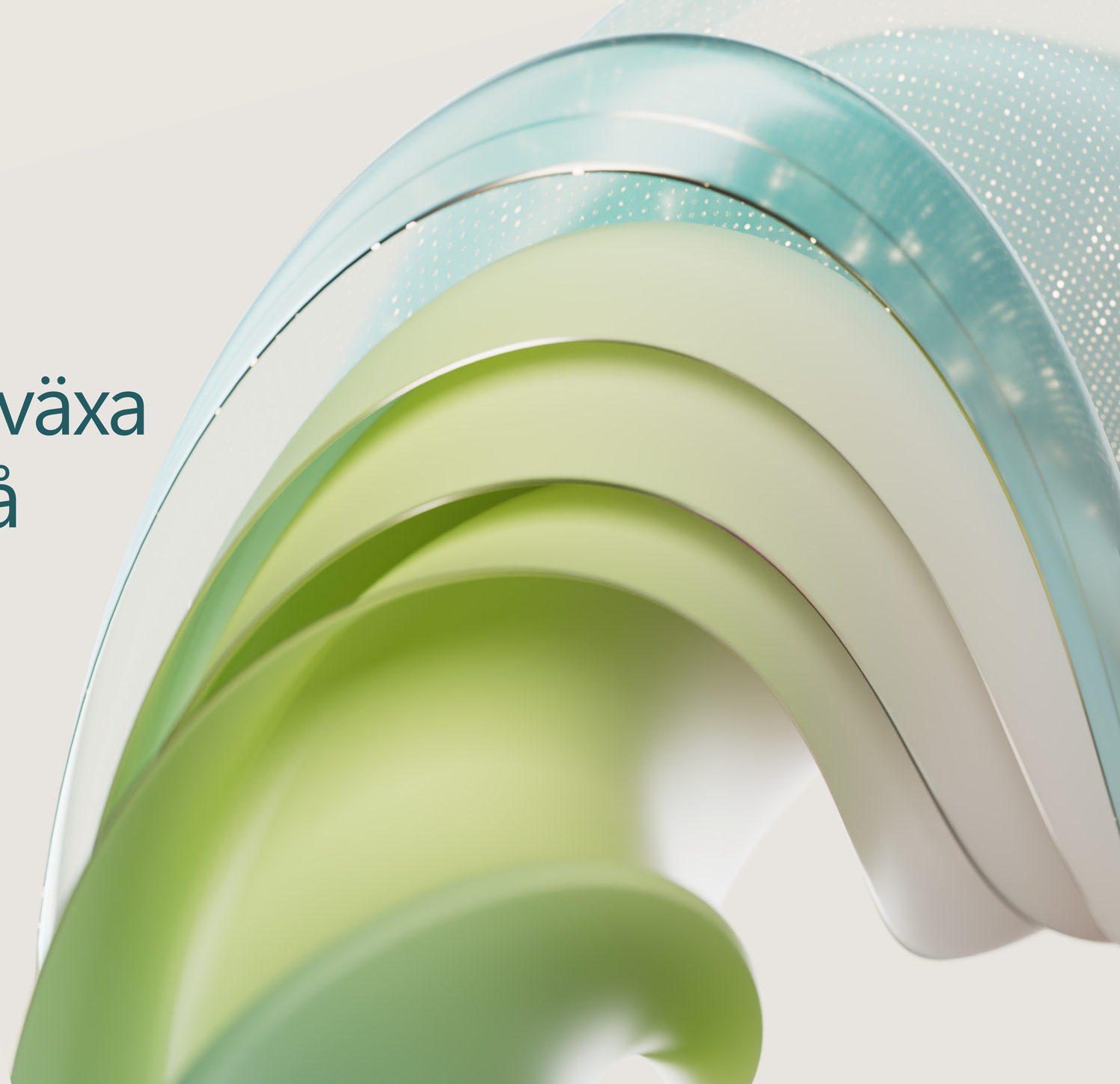
Microsoft

# Få verksamheten att växa med AI du kan lita på

Att tänka på för verksamhetsledare som vill planera en trygg AI-omställning



# Innehåll

# Inledning

AI-lösningar innebär en otrolig möjlighet för både små och stora organisationer inom alla branscher att öka intäkterna, minska kostnaderna, förbättra medarbetarnas välbefinnande och arbeta mer effektivt. Det kommer alltså inte som någon överraskning att verksamhetsledare känner en press på sig att införa AI-lösningar så snabbt som möjligt, så att de inte hamnar på efterkälken.

Det snackas mycket om möjligheterna AI, men det finns en hel del oro över teknikens negativa effekter. I de följande avsnitten beskriver vi olika överväganden som verksamhetsledare bör planera efter, så att de bättre kan ta vara på den här nya tekniken och undvika oavsiktliga konsekvenser.

Genom att upprätta rutiner för ansvarsfull och säker AI kan ditt företag implementera AI-verktyg på ett säkert sätt. I takt med att den globala AI-regleringen ökar blir det lättare att uppfylla nya lagstadgade krav allt eftersom de kommer om du redan nu investerar i ansvarsfull AI. Genom att använda en genomtänkt strategi för implementering av ansvarsfull och säker AI i företaget blir det enklare för ledare att ta till sig AI-tekniken och stärka innovationskraften.


av verksamhetsledarna uppgav att de var ”**lika bekymrade som entusiastiska**” när det gällde generativ AI.[1]

**Vi strävar efter att uppnå tillförlitlig AI och skapa branschledande kompletterande teknik. Med funktioner som förbättrar skyddet, säkerheten och integriteten fortsätter vi att göra det möjligt för kunderna att använda och skapa tillförlitliga AI-lösningar.**

**Läs mer**

# Arbeta ansvarsfullt med AI

# Principerna för ansvarsfull AI

Politiken och näringslivet ligger fortfarande steget efter den senaste utvecklingen inom AI-tekniken, vilket gör att företagsledare söker efter tillförlitlig vägledning i hur de kan implementera AI-system som har en positiv inverkan på företag, individer och samhället.

Om du tar dig tid att tänka igenom hur en ansvarsfull AI-strategi skulle se ut för din organisation kan ni tryggt arbeta vidare och skydda verksamheten mot oavsiktliga risker. Vi har tagit fram sex principer för ansvarsfull AI som du bör ha i åtanke när du planerar och tar fram en egen strategi. Dessa principer omfattar följande:

- **Integritet och säkerhet**
- **Ansvarstagande**
- **Öppenhet**
- **Tillförlitlighet och säkerhet**
- **Inkludering**
- **Rättvisa**

# Integritet och säkerhet

AI-system bör följa samma standarder för integritet och säkerhet som företaget tillämpar på sina känsligaste data.

**Prioritera säkerheten för infrastrukturen och integriteten för data.**

Ta reda på var data finns, hur de används och kontrollera att de är säkra i vila och under överföring. Kontrollera att AI-verktygen uppfyller företagets värderingar gällande integritet och säkerhet.

Om du implementerar rigorösa databehörigheter och tilldelar användarbehörigheter baserat på roller och gruppmedlemskap, kan bara behöriga personer få tillgång till känslig information, vilket minskar risken för interna överträdelser.

Dessutom kan du upprätthålla säkerheten och uppfylla efterlevnadskraven med en styrningslösning. Det innebär att bevara och logga interaktioner med AI-appar, identifiera eventuella överträdelser av organisationens regler och policyer när dessa appar används och undersöka incidenter när de uppstår.

AI-implementeringen måste också följa alla lokala lagar och förordningar avseende dataanvändning och integritet. När det gäller datasäkerhet är det bäst att vara överdrivet försiktig och bara arbeta med leverantörer av säkerhetsverktyg med bevisad tillförlitlighet.

**Exempel på integritet och säkerhet i praktiken:**

Att använda ett AI-verktyg för att analysera kundkommunikation vid hanteringen av ett supportärende kan innebära åtkomst till känsliga eller identifierbara kunddata. Genom att förstå lokala lagar och förordningar, följa organisationens egna höga standarder för säkerhet och tillämpa lämpliga kontroller kan du se till att känsliga data förblir privata.

**Efterleva AI-regelverk**

**Microsoft har åtagit sig att konstruera produkter och lösningar som följer lagar som EU:s AI-lag för att hjälpa våra kunder att använda AI enligt reglerna.**

**Läs mer**

# Tillförlitlighet och säkerhet

Tillförlitlighet och säkerhet innebär att AI-systemen fungerar som förväntat, utan fel eller avbrott. Utvecklare av AI-verktyg ansvarar för att deras produkter ger korrekta resultat genom testning och dokumentation, men med ett tillsynssystem kan du kontrollera om verktyget verkligen ger det avsedda resultatet. Systemen bör också genomgå regelbundna processer för övervakning, underhåll, feedback och utvärdering som kan identifiera nya användningsområden, snabbt felsöka och lösa problem och förbättra AI-systemet allt eftersom.

**Utför regelbundet stresstester.**

Stresstester förbereder ett AI-system för att hantera de typer av användning och mängden användning som det är avsett att hantera, utan att generera fel eller bli sårbart för risker.

Red Teaming är en typ av stresstester som innebär att simulera verkliga angrepp och använda de tekniker som hackare ofta använder för att få tillgång till säkra system. År 2018 införde Microsoft vårt eget AI Red Team och sedan dess har vi utökat teamets uppdrag till att kartlägga risker utanför traditionella säkerhetsrisker, bland annat risker från icke-konfrontativa användare som bryter mot regler för ansvarsfull AI. Till exempel kan Red Teaming av ett generativt AI-verktyg innebära att testa om en användare kan generera innehåll som skapar stereotyper av en marginaliserad grupp med hjälp av verktyget. Red Teaming kan också innebära att undersöka en AI-modell för att identifiera potentiellt missbruk, funktionernas omfattning och förstå dess begränsningar. Dessa insikter kan sedan tillämpas på framtida versioner av modellen så att den fungerar mer tillförlitligt och säkert.[2]

**Undersök tillförlitlighet och säkerhetsåtgärderna noggrant i ett AI-system vid inköpstillfället, och utför sedan regelbundna stresstester för att identifiera risker.**

Genom att noggrant gå igenom dokumentationen kan organisationer förstå vilka åtgärder AI-systemleverantören har vidtagit för att underlätta tillförlitlig och säker användning av systemet, och det blir enklare för organisationen att uppfylla alla krav som ställs för att använda systemet på ett säkert sätt.

**Exempel på tillförlitlighet och säkerhet i praktiken:**

Ett AI-verktyg används för att modellera finansiella resultat och rapportera resultaten. Tester utförs regelbundet för att säkerställa att AI-verktyget på ett tillförlitligt sätt ger korrekta resultat, så att företaget undviker negativa effekter på det finansiella tillståndet.

# Ansvarstagande

I många fall utgår ansvarsfull AI från människan. Genom att upprätta ett tydligt tillsynssystem kan dina medarbetare styra de AI-verktyg du inför och ta ansvar för de resultat som dessa verktyg producerar.

**Upprätta ett tillsynssystem som tydligt definierar roller och ansvar under varje skede av AI-resan.**

Genom att införa ett tillsynssystem som utför konsekvensbedömningar och reagerar på resultaten sätts människan i centrum. På så sätt kan man skydda organisationen mot eventuellt negativa effekter och se till att lämpliga kontroller genomförs under varje fas.

**Se till att AI-verktygen passar för ändamålet.**

Utvärdera regelbundet att AI-verktygen ger de rätta lösningarna på problemen som de var avsedda att lösa – och ta reda på hur organisationen ska reagera om ett verktyg inte uppfyller det avsedda syftet.

**Exempel på ansvarstagande i praktiken:**

Om ett AI-verktyg används för att granska juridiska avtal måste tillsynen utföras av en person som har rätt sammanhang och expertkunskaper för att kontrollera att tillämpliga lagar och förordningar efterföljs, och den personen måste godkänna det slutliga resultatet av den AI-assisterade granskningen.

# Inkludering

I grund och botten innebär inkludering att AI-verktygen måste vara tillgängliga för människor med olika förmågor. Det innebär i sin tur att de verktyg som verksamhetsledare skapar eller upphandlar bör följa principer för tillgängliga design och följa de europeiska tillgänglighetskraven (EN 301 549), avsnitt 508 i den amerikanska lagen om rehabilitering (Rehabilitation Act) samt riktlinjerna för tillgänglighet för innehåll(WCAG).

**Identifiera möjligheter till bättre inkludering i din organisation med AI.**

Till exempel skapar mottagare av Microsoft-stipendier en rekryteringsplattform för funktionsvarierade sökande, skapar bättre och mer prisvärda punktskriftsläsare för studenter med nedsatt syn och skapar en webbapp som hjälper människor med nedsatt talförmåga att kommunicera effektivare.

# Öppenhet

Öppenhet är en grundläggande faktor för den som vill bygga upp förtroende. Om du vill uppnå och upprätthålla bättre öppenhet ska du alltid vara tydlig med hur och när AI används, samt teknikens funktionalitet och begränsningar.

**Var öppen med om hur AI implementeras och används i organisationen.**

Intressenter och medarbetare kan känna sig mer trygga när de använder AI-verktyg om de förstår hur verktyget kommer fram till slutsatserna, men också är på det klara med verktygens begränsningar. Tack vare den här öppenheten kan medarbetare och intressenter utveckla sin förmåga att använda AI-assisterade verktyg, och de vet med sig när de behöver komplettera utdata med ytterligare information.

Kunderna vill veta när de interagerar med ett AI-verktyg, huruvida AI används för att fatta beslut eller när en ljud- eller bildtillgång har genererats eller manipulerats med hjälp av AI. Verksamhetsledare bör fundera över hur den här informationen ska förmedlas till kunderna.

**Exempel på öppenhet i praktiken:**

Generativ AI används för att skapa innehåll för en marknadsföringskampanj, och organisationen identifierar vilka element som skapas med hjälp av AI. En specialist granskar det AI-genererade innehållet för att verifiera att det är korrekt, så att det inte vilseleder kunderna om funktionerna i den annonserade produkten.

# Rättvisa

Vid en rättvis AI-implementering fördelas möjligheter, resurser och information rättvist mellan de människor som använder och påverkas av AI-tekniken.

**Se till att AI-systemen ger alla – inom olika demografiska grupper – som använder eller påverkas av tekniken likartad kvalitet och leverans av resurser och möjligheter.**

När du använder AI-verktyg som beskriver, skildrar eller på annat sätt representerar människor ska du minimera risken för stereotyper eller att människor förminskas – särskilt när det gäller marginaliserade grupper.

Inkludera medlemmar med olika bakgrunder, erfarenheter, utbildningsnivåer och perspektiv i teamet som hanterar AI-implementeringen, och identifiera statistiska systematiska avvikelser i datauppsättningarna så att AI-systemet blir mer rättvist. Det blir också lättare att undvika partiska beslut genom mänsklig granskning av ämnesexperter i beslut som bygger på AI.

**Exempel på rättvisa i praktiken:**

Ett AI-verktyg används för att granska sökanden och identifiera prioriterade kandidater i en rekryteringsprocess med hjälp av tillsyn från en personalrepresentant. Den här personen bekräftar att verktyget bedömer informationen korrekt, utan statistiska avvikelser, och står för den slutliga granskningen inför beslutet.

# Fatta välgrundade beslut om AI och säkerhet

Genom att införa AI på ett ansvarsfullt sätt kan du minimera riskerna samtidigt som företaget kan dra nytta av tekniken inom olika användningsområden. Använd följande frågor som diskussionsunderlag med ditt team när ni börjar tänka igenom hur AI ska införas.

### Integritet och säkerhet

- [ ] Skyddas data som används av AI-systemen i enlighet med organisationens policyer för hantering av känsliga data?
- [ ] Har du kontroll över organisationens data, inklusive var de lagras och hur de används?
- [ ] Är data skyddade hela tiden, även när de överförs från ett system till ett annat?
- [ ] Har ni säkerhetsverktyg av hög kvalitet för att försvara organisationen mot åtkomst från tredje part eller cyberangrepp?
- [ ] Har ni verktyg för att kunna identifiera och reagera på hot vid cyberangrepp?

### Inkludering

- [ ] Har ni kontrollerat att verktygen ni tänker använda uppfyller principerna om tillgänglig design?
- [ ] Uppfyller verktygen de europeiska tillgänglighetskraven, EN 301 549?
- [ ] Uppfyller verktygen avsnitt 508 i den amerikanska lagen om rehabilitering (Rehabilitation Act)?
- [ ] Uppfyller verktygen riktlinjerna för tillgänglighet för innehåll (WCAG)?

### Tillförlitlighet och säkerhet

- [ ] Har de verktyg ni tänker använda testats tillräckligt för att minimera antalet fel?
- [ ] Har ni en plan för hur ni kan åtgärda eventuella fel som uppstår?
- [ ] Kommer verktygen att övervakas regelbundet när det gäller tillförlitligheten?
- [ ] Är ni förberedda på att uppfylla alla krav på hur verktygen kan användas på ett säkert sätt?

### Öppenhet

- [ ] Har ni utbildat intressenterna i hur den här implementeringen kommer att fungera, till exempel lösningens funktionalitet och begränsningar, eller planerar ni att göra det innan de börjar använda AI-verktygen?
- [ ] Har ni en plan för hur ni ska kommunicera med medarbetarna om hur organisation ska använda AI och hur resultaten ska tolkas?
- [ ] Har ni bestämt hur och när ni ska meddela kunderna att de interagerar med AI eller tittar på AI-genererat innehåll?

### Ansvarstagande

- [ ] Har ni bedömt vilken effekt den här implementeringen får på medarbetare, på organisationen och på kunderna?
- [ ] Har ni upprättat ett system för tillsyn och åtgärder vid potentiella negativa effekter?
- [ ] Har ni implementerat bästa praxis för datastyrning och -hantering?
- [ ] Har ni bestämt vilka som ska ha tillsyn över AI-verktygen, och har de rätt utbildning och kontrollsystem?
- [ ] Har ni kontrollerat att den här lösningen passar för det avsedda ändamålet?

### Rättvisa

- [ ] Har ni sett till att implementeringen erbjuder samma tjänstkvalitet för alla som påverkas av den?
- [ ] Har ni testat systemets resultat för att se till att resurser och möjligheter fördelas rättvist mellan olika demografiska grupper?
- [ ] Är resultaten av systemet fria från stereotyper och negativa skildringar av marginaliserade grupper?

# Skydda dina data och AI-system

# Skydda dina AI-verktyg nu och i framtiden

Felaktigt implementerad kan all teknik som har tillgång till känsliga data utgöra en säkerhetsrisk för företagen. Eftersom AI-systemen kräver mycket egna data är det viktigt att prioritera säkerheten från början när man funderar på att införa AI eller skaffa AI-lösningar.

På Microsoft har vi lanserat initiativet Secure Future Initiative, där vi samlar våra lärdomar så att vi lättare kan itu med och förbereda oss på den ökande omfattningen och de ökande riskerna med cyberangrepp i AI-eran. Secure Future Initiative identifierar tre principer som Microsoft upprätthåller för att skydda det digitala ekosystemet:

1. **Inbyggd säkerhet**
   När du designar en produkt eller tjänst måste säkerheten ha högsta prioritet.

2. **Inbyggd säkerhet**
   Säkerhetsskyddet ska aktiveras och verkställs som standard, får inte kräva extra arbetsinsatser och ska inte vara valfritt.

3. **Säkerhet i driften**
   Säkerhetskontroller och övervakning förbättras kontinuerligt för att uppfylla dagens och framtida hot.

Säkerhet är grundläggande för alla AI-implementeringar. Genom att säkerställa rutiner för grundläggande säkerhetshygien skyddar du data, medarbetare och enheter från mer än 98 procent av cyberangreppen.[3]

Effektiva rutiner för säkerhetshygien är bland andra följande:

- Aktivera multifaktorautentisering för att skydda organisationen mot knäckta användarlösenord och göra identiteter mer motståndskraftiga.
- Tillämpa Zero Trust-principer, vilket innebär explicit verifiering, användning av lägsta privilegierade åtkomst och antagande av intrång för att begränsa effekten av ett angrepp.
- Använd utökad identifiering och åtgärder samt program mot skadlig kod för att identifiera och automatiskt blockera angrepp och få insikter i säkerhetsprogramvaran, så att det går att reagera snabbare.
- Se till att alla system hålls uppdaterade med de senaste versionerna av inbyggd programvara, operativsystem och appar.
- Implementera rätt skydd för viktiga data, vilket kräver kunskap om vilka data som är viktigast och var de finns.

# Hantera dina AI-system genom styrning

Med en stark styrningsmodell går det att lägga en stabil grund för införandet av ansvarsfull AI. Det är tillsynsmyndigheternas uppgift att upprätthålla grundläggande krav för att minimera AI-användningens negativa effekter på samhället. Men kommersiella organisationer har också ett etiskt ansvar för att skapa en styrningsstruktur, så att de kan hantera sin egen utveckling eller användning av AI-system i enlighet med organisationens värderingar, lokala lagar och föreskrifter, och för allmänhetens bästa.

## Inrätta egna styrningsfunktioner

När du skapar organisationens styrningssystem måste du komma ihåg att syftet med styrningen är att AI-lösningarna ska följa företagspolicyn och principerna om ansvarsfull AI genom en rad policyer och rutiner. Detta omfattar att tillämpa policyer för att bedöma och implementera AI-lösningar från tredje part, samordna intressenternas deltagande och utbildning samt ta fram dokumentation för att informera medarbetare, kunder och andra användare om AI-verktygen.

## Risker

### Kartläggning

Kartläggningen av risker är det första steget i styrningen av AI, och denna bör ligga till grund för beslut om ett verktygs säkerhet, tillförlitlighet och ändamålsenlighet. Att kartlägga risker innebär att man genomför konsekvensbedömningar av AI-tekniken samt integritets- och säkerhetsgenomgångar – bland annat Red Teaming och stresstester.

### Mätning

Att mäta risker innebär att utveckla mätvärden som gör det möjligt att bedöma identifierade risker och testa planerade åtgärder för att avgöra hur effektiva de kommer att vara.

### Hantering

Om en organisation ska kunna hantera riskerna måste resultatet övervakas löpande. I detta skede bör du identifiera möjligheter för användarna och utbilda intressenter om ansvarsfull användning. Mänsklig granskning och tillsyn bör ingå i hanteringsprocessen, men även bästa praxis för öppenhet enligt principerna om ansvarsfull AI.

# Ta vara på potentialen med AI

# Hur företag ställt om på ett säkert sätt

Genom att använda AI på ett ansvarsfullt och säkert sätt kan en organisation förbättra verksamheten, hantera de mest akuta utmaningarna och skapa förtroende och tillit hos kunderna. Här följer några exempel från verkligheten på hur detta kan uppnås.

## Inrättade ett råd för ansvarsfull AI

Wipro, ett företag med 240 000 anställda i 65 länder, har en unik möjlighet att undersöka hur man kan förändra hur människor arbetar med hjälp av AI. Wipros anställda har utbildats i principerna för generativ AI och organisationen har bestämt sig för att använda tekniken för att snabbare skapa värde för kunderna och förbättra verksamhetens resultat.

För att medarbetarna ska kunna ta vara på kraften i AI inrättade Wipro-ledningen först ett AI-råd för att ta reda hur man bäst kunde införa ett AI-program internt. I sessioner som genomfördes varannan vecka utarbetade Wipro-ledningen en profilbaserad modell för hur man kunde implementera Microsoft 365 Copilot i hela den globala verksamheten. Genom att skapa särskilda profiler, som säljare, utvecklare och medarbetare i CTO-organisationen, såg Wipro att olika Microsoft 365 Copilot-moduler kunde komplettera dessa olika roller.

**Läs mer**

## Skyddar viktig forskning och känsliga data

Oregon State University (OSU), ett respekterat forskningsfokuserat universitet i USA, prioriterar skyddet av forskningen så att de kan upprätthålla sitt goda anseende. Universitet måste ha en öppen miljö som främjar samarbete med andra institutioner och forskare, och samtidigt säkerställa att all forskning förblir säker och följer relevanta standarder.

Efter att en incident inträffat inrättade OSU ett eget säkerhetscenter. OSU integrerade Microsoft 365 A5-licensiering och började tillämpa Zero Trust-metoden för cybersäkerhet genom att brett distribuera Microsoft Sentinel och Microsoft Defender. OSU uppskattar att man uppnått fem års mognad på ungefär två år, tack vare införandet av säkerhetstekniken och Microsofts stöd och rådgivning som hjälpte dem att få ut mesta möjliga av dessa verktyg.

**Läs mer**

IFAD
Investing in rural people

## Extraherar rätt data i rätt tid

IFAD (International Fund for Agricultural Development) har ett globalt uppdrag att utrota fattigdom och svält i några av världens mest sårbara jordbrukssamhällen i utvecklingsländer. Organisationen samarbetar med regeringar för att finansiera projekt och innovativa metoder som gör det möjligt för småskaliga producenter att utveckla hållbara jordbruksmetoder, förnya livsmedelssystemen och bygga upp motståndskraft inför några av de största globala utmaningarna. IFAD behövde ett bättre sätt för sina globala team och partner att komma åt och dela viktig information från och till de avlägsna platser som organisationen arbetar på.

Genom att använda Microsoft Azure OpenAI Service, Azure AI Search och Power BI skapade organisationen Omnidata, en centraliserad analysplattform som kopplar samman data, instrumentpaneler, visualiseringar och analyser genom maskininlärning och AI. Med den här lösningen får all personal snabb och direkt tillgång till viktiga data i alla regioner som IFAD arbetar i, samt utbildning i analys och maskininlärning så att de kan skapa nya verktyg som hanterar specifika dagliga utmaningar.

Läs mer

avanade

## Minskar krånglet och stärker säkerheten

Avanade, ett samarbete mellan Accenture och Microsoft, är ett konsultföretag som bistår organisationer över hela världen i sin digitalisering. Avanade har en stor och komplex dataegendom. Företaget använder data och analyser för en mängd olika aktiviteter inom organisationen, från att fatta beslut till att säkerställa att kunderna uppnår bästa möjliga resultat.

Tidigare använde företaget flera olika resurser, däribland Microsoft Azure Synapse Analytics, Azure SQL Database och Power BI för att hantera data och analyser. Det innebar att IT-teamet måste duplicera data varje gång som en användare behövde överföra information från ett verktyg till ett annat. Nu går Avanade över till Microsoft Fabric, som omfattar alla de verktyg som behövs. Detta innebär att man kan undvika att duplicera data, minska krånglet, spara tid och ge medarbetarna en bättre upplevelse.

Läs mer

# Bättre hållbarhet med AI

Precis som säkerhet är en viktig grund för ansvarsfull AI, är hållbarhet avgörande för hur tekniken kan användas på ett ansvarsfull sätt. AI kan fungera som ett kraftfullt verktyg för den som vill få en bättre förståelse för och minska sin miljöpåverkan, så att man kan uppnå hållbarhetsmålen snabbare. Med AI kan både företag och offentliga institutioner bättre förstå och skydda miljön, hantera resurser och begränsa klimatförändringarna.

Med AI-baserade verktyg för datahantering och rapportering kan organisationer få insyn i sitt hållbarhetsarbete så att de kan registrera, rapportera och minska sin miljöpåverkan. AI kan skapa insikter som kan ligga till grund för mer välgrundade beslut, vilket underlättar för organisationer att arbeta vidare mot sina hållbarhetsmål.

Men vi vet också att dessa tillämpningar är mycket resurskrävande och att vi måste analysera miljöpåverkan från alla synvinklar.

Verksamhetsledare kan göra sina egna datacenter mer hållbara, eller arbeta med leverantörer som redan vidtar åtgärder som minskar miljöpåverkan från de datacenter som driver deras AI-lösningar.

På Microsoft har vi investerat mycket i detta och ökar vårt fokus på tre huvudområden avseende hållbarhet: optimera energi- och vatteneffektivitet i våra datacenter, prioritera koldioxidsnåla material och förbättra energieffektiviteten hos AI- och molntjänster – allt med målet att ge våra kunder och partner verktyg för kollektiva framsteg.

# Inled omställningen till AI

Genom att noga överväga metoder för ansvarsfull AI och prioritera organisationens säkerhet kan du utforska hur AI kan användas för att få verksamheten att växa.

Våra åtaganden och funktioner gör det möjligt för dig att tryggt och snabbt ställa om till AI, och du kan lita på att Microsoft sätter din säkerhet, integritet och säkerhet gällande AI i första rummet.

**Läs mer om Microsoft AI om du vill börja använda AI.**

**Upptäck hur Microsoft arbetar för att utveckla AI på ett ansvarsfullt sätt.**

**Utforska hur Microsoft kan hjälpa din organisation att skydda AI med omfattande lösningar för säkerhet och styrning.**

# Källor

[1] ”What Business Leaders Really Think About Generative AI”, INSEAD, 11 april 2024, https://knowledge.insead.edu/leadership-organisations/what-business-leaders-really-think-about-generative-ai.

[2] ”Microsofts öppenhetsrapport om ansvarsfull AI 2024”, Microsoft, läst den 10 juli 2024, https://www.microsoft.com/corporate-responsibility/responsible-ai-transparency-report.

[3] Quy Nguyen, ”Basic cyber hygiene prevents 98% of attacks”, Microsoft Tech Community, 18 september 2023, https://techcommunity.microsoft.com/t5/security-compliance-and-identity/basic-cyber-hygiene-prevents-98-of-attacks/ba-p/3926856.