

dunamis technology

Du leder ikke bare en virksomhet.
Du forvalter tilliten til den.

Selskapspresentasjon · Dunamis Technology

SLIK HENGER DET SAMMEN

Fire spørsmål, én fortelling

01 Hvorfor vi finnes

Ansvaret har flyttet seg oppover, og det er tilliten som står på spill. Compliance alene er en felle. Vi ser på spørsmålene som avdekker om det holder.

02 Hvem vi er og for hvem

Et norsk fagmiljø i Halden som gir SMB samme beskyttelse som de store, uten egen sikkerhetsavdeling.

03 Hva vi gjør

En samlet portefølje: digital sikkerhet, styring og etterlevelse, rådgivning og forretningssystemer.

04 Hvordan vi jobber

Én metode og fire verdier som gir forutsigbar kvalitet i alt vi leverer. Vi kaller det Dunamis Excellence.



01

Hvorfor vi finnes

Ansvaret for digital sikkerhet har flyttet seg oppover. Det som står på spill, er tilliten virksomheten er bygget på.

EN NY VERDEN, MED NYE REGLER

Trusselbildet endrer seg raskere enn de fleste rekker å ruste seg

Geopolitiske spenninger

Påvirker cyberstrategien i nær 6 av 10 virksomheter. Spionasje og tap av sensitiv informasjon bekymrer toppledere.

Mer sofistikert kriminalitet

72 % melder om økt cyberrisiko det siste året. Svindel, phishing og identitetstyveri øker mest.

Leverandørkjeden

54 % av store virksomheter peker på tredjepartsrisiko som en av de største utfordringene for robusthet.

Regulatoriske krav

NIS2, DORA og AI Act stiller nye krav. To av tre opplever regelverket som komplekst å etterleve.

AI og ny teknologi

66 % venter at AI endrer sikkerhetsbildet, men bare 37 % har prosesser for trygg bruk av AI.

Kompetansegapet

To av tre virksomheter mangler sikkerhetskompetanse. Bare 14 % er trygge på at de har folkene de trenger.

Ingen av de seks løses av IT alene. Alle krever beslutninger som må tas i ledelsen: om prioritering, om penger og om hva virksomheten skal tåle.

Kilde: World Economic Forum, Global Cybersecurity Outlook

HVEM RAMMES HARDEST

Små og mellomstore virksomheter står mest utsatt

43 %

av alle cyberangrep rammer små og mellomstore virksomheter

14 %

er rustet til å forsvare seg mot angrepene som kommer

71 %

av sikkerhetsledere mener små virksomheter ikke lenger kan sikre seg alene

Ansvaret for å tette gapet ligger i ledelsen. Kravene kom gradvis gjennom kunder, kontrakter og nye regelverk. Det er ikke sikkert noen har sagt tydelig fra om at det har skjedd.

Kilder: Accenture / WEF Annual Meeting on Cybersecurity

DET SOM STÅR PÅ SPILL

Du leder ikke bare en virksomhet. Du forvalter tilliten til den.

01

Kundene

De har lagt noe hos dere de ikke kan hente tilbake. Tilliten deres er avtalt i kontrakt, men bygget på antakelser om hvordan dere håndterer den.

02

Leverandører og partnere

Driften deres henger sammen med deres. Når noe stopper hos én, merkes det raskt hos de andre.

03

Ansatte og styret

Arbeidsplasser på den ene siden, tilsynsansvar på den andre. Begge deler hviler på et grunnlag noen må skaffe.

Det er dette som forsvinner først når noe skjer. Og det er det ingen andre enn ledelsen kan forvalte.

VÅRT UTGANGSPUNKT

«Tror du teknologi kan løse sikkerhetsproblemene dine, så har du verken forstått problemene eller teknologien.»

Bruce Schneier, sikkerhetsekspert og kryptograf

Derfor kombinerer vi teknologi med metode og menneskelig vurdering. Verktøy alene løser ingenting. Det er styringen rundt verktøyene som skaper varig trygghet. Det er der de fleste snubler.

FELLEN

Papiret føles som trygghet

Det er ikke rart at det blir sånn. Revisor ber om dokumenter. Styret ber om status. Kunden ber om et sertifikat. Alle spør om det som kan vises fram, og ingen har som jobb å spørre om det virker. Så bygger man det som etterspørres, og risikoen står igjen der den var.

COMPLIANCE SVARER PÅ

«Kan vi vise at vi gjorde noe?»

Nødvendig. Kreves i anbud, av revisor og av regelverket. Produserer et dokument, en logo og et styrereferat.

ROBUSTHET SVARER PÅ

«Hva skjer faktisk når det smeller?»

Like nødvendig, men mye sjeldnere etterspurt. Produserer ingenting å vise fram før dagen det gjelder.

Vi lever av å få kunder gjennom sertifisering, og vi tar ansvar for at de kommer i mål. Men et sertifikat er ikke beviset på at dere er trygge. Det er beviset på at dere har begynt.

FUNDAMENTET

Secure, compliant og resilient som fundament

En virksomhet er alltid i én av fire tilstander. Sertifisering dokumenterer tilstand 4, men er sertifikatet det eneste målet, kan det skjule de reelle problemene.



NØKKELSETNINGEN

«Compliance bør være en naturlig bivirkning av sikker og robust drift, ikke målet i seg selv.»

Secure Controls Framework Council, SCRMS v2026.3

I praksis betyr det: dokumenter det dere faktisk gjør riktig. Ikke gjør ting bare for å tilfredsstille revisor.

HVA SOM SKAL TIL

Robusthet krever hele bildet, ikke bare beskyttelse

Cyber Defense Matrix kobler fem typer eiendeler mot funksjonene i NIST CSF 2.0. Styring ligger over alt, og respons og gjenoppretting avgjør hvor godt dere tåler et slag.

FØR HENDELSEN · UNDER · ETTER · OPERATIV UTHOLDENHET

STYRE — Strategi, roller, risikoappetitt, policy og leverandørstyring. Broen mellom teknisk sikkerhet og ledelsens ansvar. Dunamis Guardian i Nexus

	Identifisere	Beskytte	Oppdage	Respondere	Gjenopprette
Enheter					
Applikasjoner					
Nettverk					
Data					
Brukere					

Teknologi ⟶ AVHENGIGHET ⟶ Mennesker →

Hvor er dere svakest? Det er der samtalen bør starte.

VEIEN UT

Ni spørsmål som ikke kan besvares med et dokument

Du trenger ikke bli teknisk for å lede dette. Du trenger spørsmål som avdekker om det faktisk holder. Disse fungerer i et ledermøte, i et styremøte og over bordet hos en kunde.

BESLUTNING OG ROLLER

- Hvem har fullmakt til å stanse driften, og tør de å bruke den?
- Hvis noe skjer klokka 23 på fredag, hvem svarer telefonen?
- Når må vi varsle kunder, eiere og Datatilsynet, og hvem gjør det?

AVHENGIGHET

- Hvilke leverandører kan stanse driften vår, og hva står det faktisk i avtalen?
- Hva gjør vi hvis e-post og Teams er nede i tre dager?
- Hva klarer vi ikke å gjenopprette?

BEVIS

- Når øvde vi sist, og hva lukket vi etterpå?
- Hva har endret seg siden forrige risikovurdering?
- Hvem hos oss vet at de eier dette?

Får du ikke svar i rommet, er det svaret.

Spørsmålene er dine å bruke, med eller uten oss. Vil du ha et bilde av hvor dere står, tar modenhetstesten vår ti minutter.



02

Hvem vi er og for hvem

Et lite, sertifisert fagmiljø med stor leveransekraft. Selskapet ledes etter verdier, ikke bare etter tall.

OM DUNAMIS TECHNOLOGY

Et lite, sertifisert miljø med stor leveransekraft

2019

etablert, med hovedkontor i Halden

Gaselle

kåret til gasellebedrift i 2024 og 2025

100 %

suksessrate på ISO 27001-sertifisering hos kunder

9+

ulike bransjer blant kundene våre

VISJON

En digital verden alle kan stole på

Vår del av jobben. Deres del er tilliten til egen virksomhet. Vi bygger grunnlaget den skal hvile på.

MISJON

Å styrke virksomheter i den digitale tidsalderen

Vi håndterer den digitale risikoen og bygger den digitale tilliten, slik at dere kan bruke tiden på å drive virksomheten.

Sertifiseringer og kompetanse i teamet: CISSP · ISO 27001 Lead · ISO 9001 Lead · DORA · COBIT 5 · PRINCE2 · ITIL. Hos oss snakker du alltid med en senior.



NAVNET FORPLIKTER

Dunamis betyr kraft og evne.

Vår rolle er å strukturere digital kraft, styre den i tråd med forretningsmål og risikotoleranse, og gjøre den bærekraftig over tid. Det er grunnlaget for identiteten vår, og grunnen til at kontinuerlig styring går igjen i alt vi leverer.

Vi er ikke et rent konsulenthus, ikke en teknologileverandør og ikke en ren sikkerhetsaktør. Vi er en langsiktig partner for kontinuerlig digital tillit og styring.

ET VERDIDREVET SELSKAP

Verdiene avgjør hvordan vi velger når hensyn kolliderer

Målene beskriver hva vi skal oppnå. Verdiene hjelper oss å velge hvordan vi arbeider, og hva som må veie tyngst når målene kommer under press. De fire staver SEIL, og et seil retter vi etter forholdene. Vi senker det aldri.

S

Samarbeid

Vi deler kunnskap i stedet for å samle den hos én person. Kompetansen skal ligge i teamet og i metoden, ikke bare i hodet til den som var der først.

E

Engasjement

Vi tar oppdragene på alvor, også de små. Men engasjement skal aldri brukes som skjult reservekapasitet. Sier vi ja, har vi kapasitet til å levere.

I

Integritet

Vi skjuler ikke vesentlig usikkerhet, pynter ikke på status og lover ikke noe vi mangler grunnlag for. Ubehagelige råd gis likevel.

L

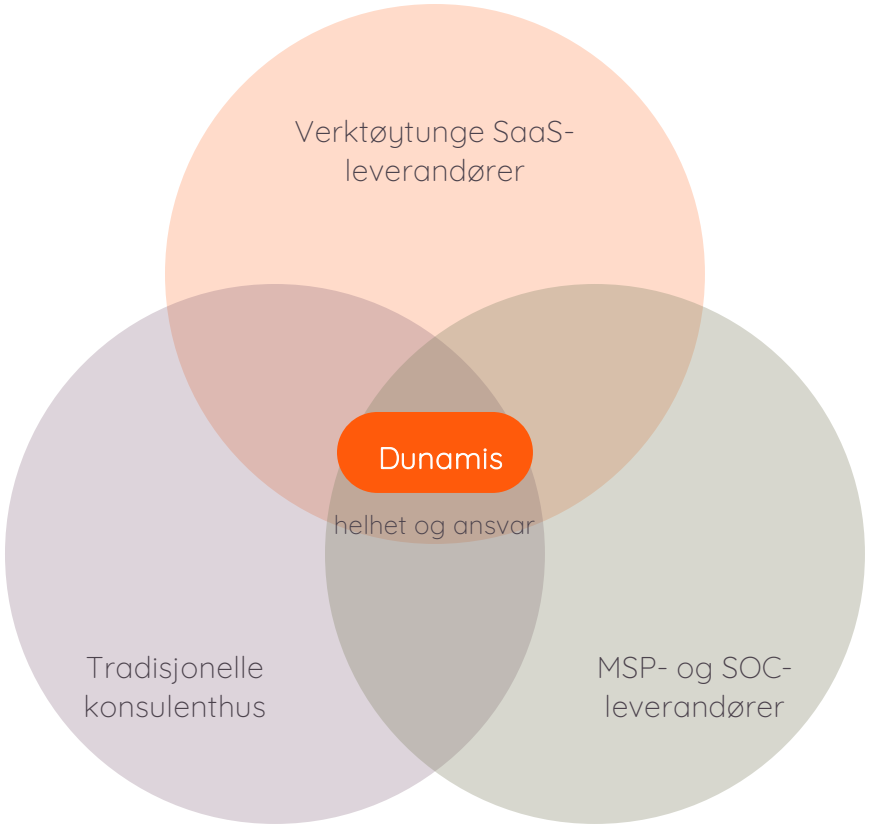
Lederskap

Lederskap handler om ansvar og påvirkning, ikke om tittel. Vi former hvordan norske SMB-er tenker om sikkerhet, men ikke ved å rope høyest.

Grensen som ligger fast: integritet kan ikke kompenseres med høy leveranse, inntjening eller effektivitet. Verdiene brukes til å vurdere handlinger, ikke personlighet.

VÅR POSISJON

Vi står der de tre aktørtypene overlapper



Verktøytunge SaaS-leverandører

+ Skalerbare og teknologisk moderne
– Forutsetter høy modenhet, så SMB får sjelden ut verdien

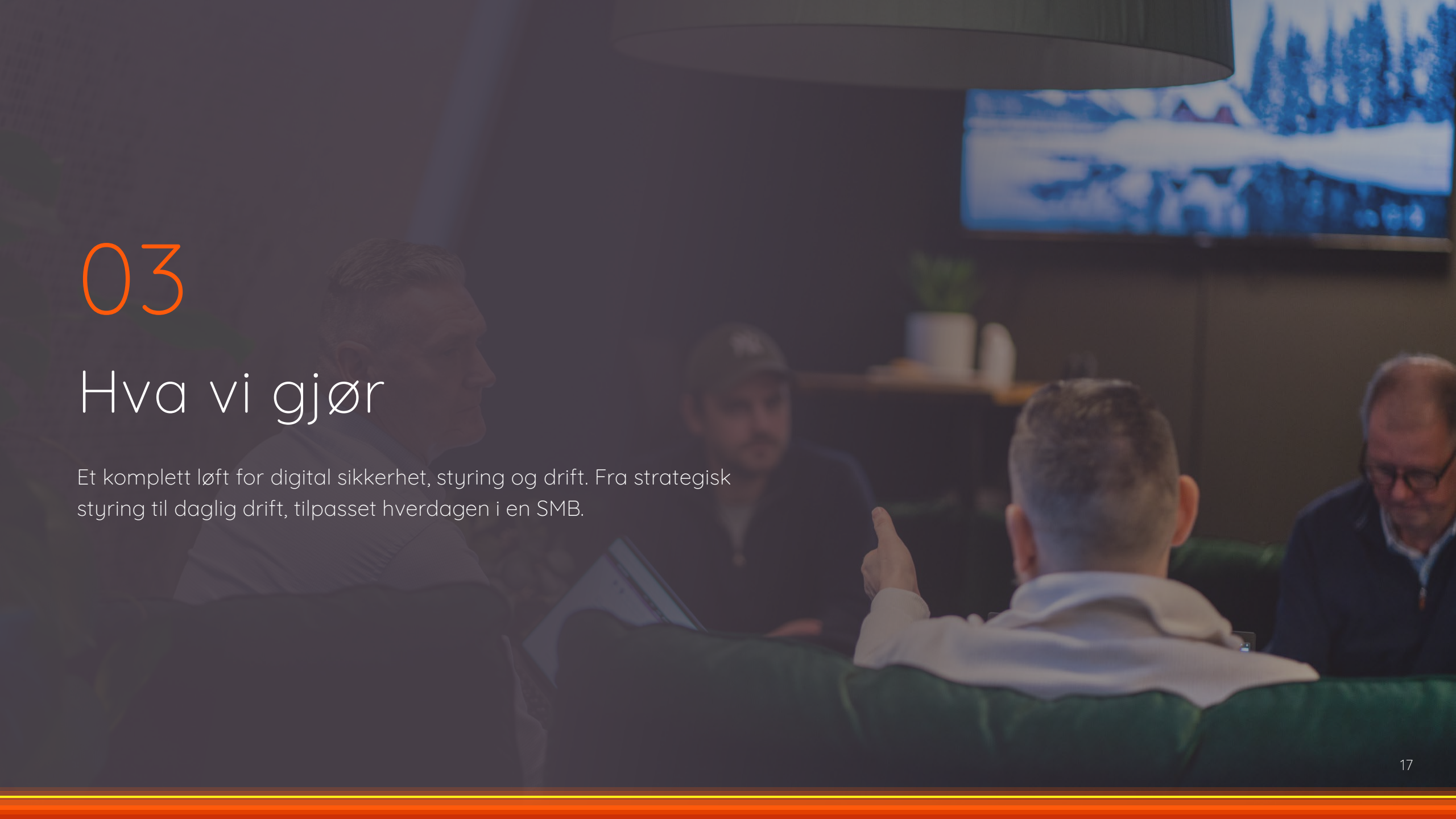
Tradisjonelle konsulenthus

+ Dyp fagkompetanse og rådgivning
– Lav skalerbarhet fordi de er avhengige av enkeltpersoner og prosjekter

MSP- og SOC-leverandører

+ Sterke på drift og overvåkning
– Svake på styring, forankring og endringsledelse

Vårt fortrinn: vi kombinerer metode, teknologi og mennesker, tar ansvar for helheten og leverer kontinuerlig, ikke prosjekt for prosjekt.



03

Hva vi gjør

Et komplett løft for digital sikkerhet, styring og drift. Fra strategisk styring til daglig drift, tilpasset hverdagen i en SMB.

PORTEFØLJEN

Fire områder. Ett samlet ansvar.

01 Digital sikkerhet

Beskytt driften fra strategi til 24/7-respons. Guardian, Shield, Aware, Patch Guard, SOC og sikkerhetstesting.

02 Styring og etterlevelse

Gjør krav og regelverk til kontroll, ikke kaos. Comply, GAP-analyser, implementering, Assure, SOC 2, øvelser, leverandør- og konsentrasjonsrisiko, DPO og AI-styring.

03 Rådgivning og prosjekt

Spisskompetanse når og der dere trenger den. ISO og regelverk, beredskap, kvantemigrasjon og AI-risiko.

04 Forretningssystemer og drift

Systemene som driver virksomheten, satt opp riktig. ERP og Odoo, prosjektledelse og prosessarbeid.

Du kan bruke én tjeneste eller kombinere flere. Poenget er at de henger sammen: styringen vi etablerer i ett område, gjør de andre enklere og billigere.

01 · DIGITAL SIKKERHET

Beskytt driften fra strategi til 24/7-respons

STRATEGI

Dunamis Guardian

Ledelsens sikkerhetsfunksjon på abonnement. Sikkerhetsledelse, risikostyring og styrerapportering.

SITUASJONSFORSTÅELSE

Dunamis Shield

Situasjonsforståelse døgnet rundt. Endepunkt, e-post, sky og brukeradferd.

MENNESKER

Dunamis Aware

Sikkerhetskultur, mikrolæring og phishing-simulering med målbar risikoscore.

SÅRBARHET

Dunamis Patch Guard

Sårbarhetshåndtering og tredjeparts-patching som tjeneste. Automatisert og AI-drevet.

DRIFT

SOC for SMB

Et sikkerhetssenter skalert for små og mellomstore. Ekspertene bak Shield, uten å bygge eget team.

TESTING

AI-basert sikkerhetstesting

Kontinuerlig, AI-drevet testing, ikke bare en årlig penetrasjonstest. Svakheter avdekkes løpende.

Alle tjenestene leveres som abonnement: forutsigbar pris, kontinuerlig leveranse.

02 · STYRING OG ETTERLEVELSE

Gjør krav og regelverk til kontroll, ikke kaos

STYRINGSSYSTEM

Dunamis Comply

Din operative GRC-leder, fra GAP-analyse til sertifisering og løpende drift.

BESLUTNINGSGRUNNLAG

GAP- og readiness-analyser

Modenhet per krav, prioriterte funn og veikart. ISO, NIS2, DORA og AI Act.

IMPLEMENTERING

Implementeringsstøtte

Krav omsatt til tiltak i ett styringssystem, uten dobbeltarbeid.

INTERNREVISJON

Dunamis Assure

Uavhengig revisjon av styring, risiko og internkontroll, uten eget revisjonsteam.

ATTESTASJON

SOC 2 Type 1 og 2

Fra readiness til gjennomført revisjon, kartlagt mot Trust Services Criteria.

BEREDSKAP

Øvelser

Krise, beredskap og incident response, med evalueringsrapport revisor kan lese.

LEVERANDØRKJEDEN

Tredjepart- og leverandørrisiko

Kritiske leverandører kartlagt, klassifisert og fulgt opp gjennom året.

DIGITAL SUVERENITET

Konsentrasjonsrisiko

Avhengighetskart, exit-vurdering og beredskap for bortfall av skyleverandør.

PERSONVERN

DPO som tjeneste

Eksternt personvernombud for etterlevelse av GDPR og bransjekrav.

AI-STYRING

AI-sikkerhet og styring

Risikovurdering, policy og testing etter ISO 42001 og EUs AI Act.

ISO 27001 · ISO 9001 · ISO 42001 · NIS2 · DORA · CRA · AI Act. Kjøpes hver for seg eller som ett løp.

KRISE, BEREDSKAP OG INCIDENT RESPONSE

Planen dere aldri har øvd på, er en antakelse

Nesten alle har en beredskapsplan. Langt færre har prøvd den. Vi planlegger og gjennomfører øvelsen som avdekker hullene på forhånd, i stedet for natten det gjelder.

FORM 1

Varslingsøvelse

Under én time, uanmeldt. Når varslingslisten faktisk testes.

FORM 2

Skrivebordsøvelse

3 til 4 timer rundt et scenario. Her bør de fleste starte.

FORM 3

Funksjonell øvelse

Én kapabilitet prøvd på ekte, for eksempel gjenoppretting.

FORM 4

Fullskalaøvelse

1 til 2 dager. Hele organisasjonen, reelle systemer og roller.

En øvelse alle består, var bortkastet. Vi legger inn friksjonen: feil informasjon, utilgjengelige nøkkelpersoner, journalisten som ringer for tidlig. Egen variant for styre og ledelse. Kjøpes alene, eller som modul i Dunamis Nexus.

MODENHET OG RISIKO

Riktig modenhet, ikke maksimal modenhet

Risikoen faller bratt når modenheten øker, mens den opplevde merverdien flater ut på de høyeste nivåene. Den beste balansen mellom risiko, kost og verdi ligger i midten: modenhetens beste sone.



Nexus Standard tar dere inn i den beste sonen. Nexus Pluss er for dem der regulering eller store kunder krever de høyeste nivåene.

LEVERANSEMODELLEN

Dunamis Nexus: sikkerhet i sammenheng

Nexus betyr knutepunkt. Det er navnet på modellen som knytter fagområdene sammen til én koordinert leveranse, med én fast rådgiver og én månedspris, i stedet for flere leverandører som hver gjør sin bit.

SIKKERHETSLEDELSE

Dunamis Guardian

Fast rådgiver med avtalt kadens mot ledelsen, veikart med eierskap og rapportering styret kan bruke.

STYRING OG ETTERLEVELSE

Dunamis Comply

Et levende ISMS mot ISO 27001, med policyer og risikovurderinger som holdes oppdatert året gjennom.

TEKNOLOGI OG OPERATIV SIKKERHET

Shield og Patch Guard

Deteksjon og respons døgnet rundt, og sårbarheter prioritert etter faktisk risiko.

MENNESKER OG KULTUR

Dunamis Aware

Trening og phishing-simulering gjennom året, med risikoutvikling målt per avdeling.

KONTINUITET OG BEREDSKAP

Øvelser og leverandørstyring

Planverk som er prøvd, ikke antatt, og kritiske leverandører kartlagt og fulgt opp.

KONTINUERLIG FORBEDRING

Evolve-hjulet

Årshjul, internrevisjon og forbedring mellom hver runde. Her sitter verdien etter sertifiseringen.

Tre nivåer etter behov: Nexus Start (orden på grunnmuren) · Nexus Standard (sertifiseringsklar og overvåket) · Nexus Pluss (regulert og revidert, med beredskapsøvelser og styrerapportering).

Spisskompetanse når og der dere trenger den

Rådgivning og prosjekt

- ISO og regelverk: GAP- og risikovurderinger som peker ut veien videre
- Internrevisjon og RCA: avdekker hva som faktisk svikter, ikke bare symptomene
- Beredskap og kontinuitet: BIA, kontinuitetsplanverk og hendelsesrespons
- Kvantemigrasjon: kryptoinventar og migrering mot post-kvantekryptografi
- Datasuverenitet og eID: rådgivning om hvor data lagres og behandles
- AI-risiko og governance: trygg bruk av AI uten å miste kontroll på data

Forretningssystemer og drift

ERP og Odoo

Rådgivning, implementering og support på Odoo. Ett system for økonomi, salg og drift.

Prosjektledelse

ERP-implementeringer og digitaliseringsprosjekter, etter PRINCE2.

Prosess og ITSM

Kartlegging og modellering av forretningsprosesser, og IT service management etter ITIL.

Vi jobber på tvers av rammeverkene dere må forholde dere til: ISO 27001 · 9001 · 14001 · 42001 · 31000 · 22301 · DORA · NIS2 · NIST CSF · CRA · AI Act · Sikkerhetsloven · GDPR



04

Hvordan vi jobber

Vi har en metode. Den heter Dunamis Excellence: samspillet mellom leveransemetoden Evolve og verdigrunnlaget SEIL.

DUNAMIS EXCELLENCE

Metode og verdier: to motorer som må gå samtidig

Den vanligste svakheten i konsulentbransjen er at kvaliteten avhenger av hvem som er på jobb. Dunamis Excellence er bygget for å fjerne den avhengigheten, og består av to deler som gjør hver sin jobb.

SEIL

Den indre motoren

Hvordan menneskene hos oss opptrer, vurderer og utvikler seg. Verdiene brukes aktivt når vi setter retning og følger opp. De er også kriteriene vi rekrutterer og utvikler folk etter.

EVOLVE

Den ytre metoden

Hvordan vi forankrer, analyserer, designer, implementerer og videreutvikler leveransen. Samme struktur uansett hvem som leverer, med dokumentert resultat underveis.

Strategiske valg foran kortsiktig inntjening

Kvalitet foran tempo

Mennesker utvikles i takt med teknologi og tjenester

Hva det betyr i praksis: ber du om en omfattende rapport, men egentlig trenger hjelp til å prioritere tre beslutninger, skal vi foreslå det siste. Også når det gir færre timer på oppdraget.

LEVERANSEMETODEN

Evolve: struktur uten å bli stiv

01

Forstå

Vi går grundig gjennom situasjonen før vi anbefaler noe: forretningsmål, risikoappetitt og folkene som skal bruke det vi bygger.

02

Forme

Sammen former vi en konkret plan: hva som skal gjøres, av hvem og når. Referansemodeller tilpasses deres virkelighet.

03

Forankre

Planen forankres i ledelsen og hos de berørte rollene. Uten forankring blir ikke planen gjennomført.

04

Følge opp

Implementering med løpende oppfølging. Vi rapporterer tydelig og skjuler ikke avvik, fordi avvik betyr læring.

05

Forbedre

Etter hver fase går vi tilbake og vurderer hva som virket og hva som ikke gjorde det. Reelle endringer mellom hver runde.

06

Forvalte

Når noe er implementert, forvalter vi det. Der tradisjonelle prosjekter slutter, sitter den varige verdien.

Hva det betyr for deg som kunde: hver kontaktperson hos oss følger samme metode. Er en kollega borte, kan en annen ta over uten kvalitetstap. Spør en revisor om historikk, kan vi vise den.

VÅRT ANSVAR

Hva vi står ansvarlig for

Vi ber ledere ta ansvar for noe som er vanskelig. Da må vi begynne med vårt eget. Dette er de tre løftene vi skriver inn i avtalen.

Vi tar ansvar for sertifiseringen

Følger dere løpet vårt, tar vi ansvar for at dere blir sertifisert, og vi står i det til dere er i mål.

Vi garanterer årshjulet

Hver aktivitet i årsplanen skjer til avtalt tid og dokumenteres. Uteblir en avtalt leveranse, fakturerer vi ikke den måneden.

Vi sier fra når dere ikke er klare

Heller utsette en revisjon enn å sende dere inn i en dere ikke er klare for. Funn som skyldes vårt arbeid, lukker vi uten å fakturere.

Resultatet så langt: 100 % suksessrate på ISO 27001-sertifisering hos kunder · kunder i 9+ bransjer · gasellebedrift i 2024 og 2025


dunamis technology
Digital sikkerhet trenger ikke være komplisert
Start med spørsmålene. Vil du ha et bilde av hvor dere står, tar modenhetstesten ti minutter. Eller vi tar en uforpliktende prat.
www.dunamistechnology.no