WHITEPAPER · v1.0 · 19. maj 2026

NIS2 Artikel 21 → Microsoft 365, komplet implementerings-mapping

Whitepaper der mapper de 10 NIS2 Artikel 21-krav til konkret Microsoft 365-feature, licens og audit-bevis. Gratis med email. Opdateret maj 2026.

> **ANSVARSFRASKRIVELSE**
> Dette dokument er en teknisk vejledning, ikke juridisk rådgivning. Mapningerne mellem NIS2-krav og Microsoft 365-features er Licenslys vurdering baseret på offentligt tilgængelig dokumentation. Konsulter altid jeres egen jurist og en certificeret Microsoft-partner inden I træffer compliance-beslutninger.

10	80%	EUR 10M
ARTIKEL 21-KONTROLLER	DÆKKET AF BUSINESS PREMIUM	MAKS. BØDE, VÆSENTLIG ENHED

INDHOLD

1. Politikker for risikoanalyse og informationssikkerhed
2. Hændelseshåndtering
3. Business continuity og backup
4. Leverandørkæde-sikkerhed
5. Sikker anskaffelse, udvikling og vedligehold
6. Effektivitetsvurdering
7. Cyberhygiejne og awareness-træning
8. Kryptering
9. HR-sikkerhed, adgangskontrol og enhedsstyring
10. MFA og sikker kommunikation

Om Licensly

Licensly er udviklet af Michal Lampe Sørensen — cand.it fra Aarhus Universitet og dansk IT-konsulent med 6× Microsoft-certificeringer. Sitet bruges af danske SMV'er til at navigere Microsoft 365-licensering uden konsulent-fee.

licensly.dk · Spørgsmål: mso@ihanstholm.dk

01 KONTROL 1

Politikker for risikoanalyse og informationssikkerhed

A. JURIDISK KRAV

"Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems... including (a) policies on risk analysis and information system security."

Dansk oversættelse: Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at håndtere risici for sikkerheden af netværks- og informationssystemer... herunder (a) politikker for risikoanalyse og informationssystemsikkerhed.

B. HVAD DET BETYDER I PRAKSIS

I skal have skriftlige politikker der dokumenterer hvordan I identificerer, vurderer og håndterer cyberrisici. Det er ikke nok at "vi tager sikkerhed alvorligt", der skal være konkrete dokumenter, der bliver opdateret regelmæssigt, og som ledelsen har godkendt.

C. MICROSOFT 365-FEATURES

Microsoft Purview Compliance Manager (primær)

Microsoft Secure Score (primær)

Purview Risk Management (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem

E. KONFIGURATION

- Gå til **Microsoft 365 Defender → Secure Score** og baseline jeres nuværende score
- Åbn **Purview Compliance Manager** og start en NIS2-assessment (eller IT-grundbeskyttelse som proxy)
- Eksportér Compliance Manager-rapport månedligt som dokumentation
- Dokumentér jeres egne politikker (kan skrives i SharePoint eller eksternt værktøj)

F. AUDIT-BEVIS

- Eksporteret Secure Score-historik (mindst 12 mdr)
- Compliance Manager assessment-rapport, dateret seneste 3 mdr
- Skriftlig informationssikkerhedspolitik godkendt af ledelsen, version-stemplet
- Mødeprotokoller fra ledelsesreviews af politikken (kvartalsvis anbefalet)

02 KONTROL 2

Hændelseshåndtering

A. JURIDISK KRAV

"(b) incident handling"

Dansk oversættelse: (b) hændelseshåndtering

B. HVAD DET BETYDER I PRAKSIS

I skal kunne detektere, registrere, undersøge og rapportere cyberhændelser. NIS2 kræver tidlig advarsel inden 24 timer og formel rapport inden 72 timer. Det forudsætter at I overhovedet kan se hvad der sker i jeres miljø, og at I har et team eller en partner der reagerer.

C. MICROSOFT 365-FEATURES

Microsoft Defender XDR-portal (E5 eller Defender Suite-add-on) (primær)

Microsoft Defender for Business (Business Premium) (primær)

Microsoft Sentinel (separat Azure-licens) (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem · **Fuld dækning kræver:** M365 E5

Business Premium dækker basis-detektion via Defender for Business. Defender XDR-portalen og automatiseret undersøgelse kræver E5 eller Defender Suite-add-on (siden september 2025 kan add-on'en købes direkte til Business Premium, max 300 brugere).

E. KONFIGURATION

- Aktivér **Defender for Business** (BP) eller Defender XDR (E5) som primær detektion
- Konfigurér automatiske svar-regler i Defender for kendte trusler
- Opret en incident response-playbook (skriftlig procedure for hvem-gør-hvad)
- Test playbooken med tabletop-øvelser mindst halvårligt
- Konfigurér 24/7-vagt eller MDR-partner hvis I ikke har eget SOC

F. AUDIT-BEVIS

- Defender incident-log med tidsstempler (eksport fra portalen, mindst seneste 12 mdr)
- Skriftlig incident response-playbook med versionshistorik
- Tabletop-øvelses-rapporter (mindst 2/år)
- Indrapporteringer til sektoransvarlig myndighed og CFCS, gem som bevis på at processen virker

03 KONTROL 3

Business continuity og backup

A. JURIDISK KRAV

"(c) business continuity, such as backup management and disaster recovery, and crisis management"

Dansk oversættelse: (c) business continuity, herunder backup-styring og disaster recovery, samt krisestyring

B. HVAD DET BETYDER I PRAKSIS

I skal kunne fortsætte forretningen efter en hændelse. Det betyder testede backups, dokumenterede recovery-tider (RTO/RPO), og en kriseberedskabsplan. Indbygget Microsoft 365-retention er IKKE backup, det er versionshistorik. Egentlig backup kræver Microsoft 365 Backup (add-on) eller tredjepartsløsning.

C. MICROSOFT 365-FEATURES

Exchange/SharePoint retention policies (primær)

Microsoft 365 Backup (separat add-on, ~$3-5/bruger/md) (primær)

OneDrive Files Restore (30 dage) (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem

E. KONFIGURATION

- Konfigurér **retention policies** i Purview for Exchange, SharePoint og OneDrive
- Vurdér om I skal købe **Microsoft 365 Backup** add-on (ransomware-rollback)
- Dokumentér RTO/RPO pr. system
- Skriv en **kriseberedskabsplan** med kontaktliste og eskalations-trin
- Test recovery mindst halvårligt (tabletop eller live)

F. AUDIT-BEVIS

- Skriftlig backup- og disaster recovery-politik med RTO/RPO
- Recovery test-rapporter (mindst 2/år)
- Microsoft 365 Backup-konfigurationsrapport hvis købt
- Retention policy-eksport fra Purview

04 KONTROL 4

Leverandørkæde-sikkerhed

A. JURIDISK KRAV

"(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers"

Dansk oversættelse: (d) leverandørkæde-sikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdet mellem hver enhed og dens direkte leverandører eller tjenesteudbydere

B. HVAD DET BETYDER I PRAKSIS

I skal styre sikkerheden hos jeres leverandører, ikke bare have dem på liste. Det betyder kontrakter med sikkerhedskrav, periodiske vurderinger og B2B-adgangsstyring. I er selv andres leverandør, så denne dokumentation bliver krævet af jer fra større kunder.

C. MICROSOFT 365-FEATURES

Conditional Access til B2B-gæster (Premium+) (primær)

Information Barriers (E5 eller Purview Suite-add-on) (supplerende)

Defender for Cloud Apps, vendor risk-scoring (E5 eller Defender Suite-add-on) (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem · **Fuld dækning kræver:** M365 E5

Business Premium er nok til at opfylde basis-kravene via Conditional Access for B2B-gæster. Information Barriers og Defender for Cloud Apps' vendor risk-scoring kræver E5 eller respektive Suite-add-ons.

E. KONFIGURATION

- Lav **CA-politikker for eksterne gæster** (kræv MFA, kun managed devices)
- Implementér leverandør-onboarding-proces med sikkerhedsspørgeskema
- Anvend Information Barriers for at adskille datagrupper hvis I har konkurrerende kunder
- Vedligehold leverandørregister med risk-rating
- Få kontraktklausuler der kræver NIS2-lignende sikkerhed

F. AUDIT-BEVIS

- Leverandørregister med risk-vurderinger
- Underskrevne sikkerhedsklausuler i kontrakter
- Eksport af CA-politikker for ekstern adgang
- Periodiske leverandør-reviews (årligt minimum)

05 KONTROL 5

Sikker anskaffelse, udvikling og vedligehold

A. JURIDISK KRAV

"(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure"

Dansk oversættelse: (e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af netværks- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

B. HVAD DET BETYDER I PRAKSIS

Den mest "ude i kanten" kontrol for typiske SMV'er. Hvis I IKKE udvikler software, er kravet primært patch management og en simpel procurement-checkliste. Hvis I gør, bliver det enterprise-territorium med SAST/DAST, signed code og secret scanning.

C. MICROSOFT 365-FEATURES

Intune patch management for endpoints (primær)

Defender for Cloud (Azure, kun hvis I bygger på Azure) (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem

E. KONFIGURATION

- Patch management: Konfigurér Intune Update Rings for Windows og Office
- Procurement-checkliste: simpel skabelon, kræver leverandøren MFA? CMMC? ISO 27001?
- Hvis I udvikler: Defender for Cloud DevOps integration + signed commits + Dependabot/Snyk
- Vulnerability disclosure: publicér en security.txt-fil på domænet med kontakt-email

F. AUDIT-BEVIS

- Patch compliance-rapport fra Intune
- Skriftlig procurement-politik
- Hvis udvikling: SAST/DAST-rapporter, signed commit-logs
- security.txt-fil tilgængelig på domænet

06 KONTROL 6

Effektivitetsvurdering

A. JURIDISK KRAV

"(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures"

Dansk oversættelse: (f) politikker og procedurer til vurdering af effektiviteten af cybersikkerhedsrisikostyringsforanstaltningerne

B. HVAD DET BETYDER I PRAKSIS

I skal regelmæssigt vurdere om jeres sikkerhedsforanstaltninger faktisk virker. Det er ikke nok at have politikker. I skal **måle**. Compliance Manager-assessments eller en årlig sikkerhedsrevision dækker kravet. Plus mødeprotokoller med action items og opfølgning.

C. MICROSOFT 365-FEATURES

Microsoft Purview Compliance Manager assessments (primær)

Audit Premium (E5 eller Purview Suite-add-on), 1 års retention (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem · **Fuld dækning kræver:** M365 E5

Business Premium giver basis Compliance Manager, nok til at få NIS2-assessment kørt og dokumenteret. Audit Premium med 1 års retention af high-value events kræver E5 eller Purview Suite-add-on (typisk relevant for finans og sundhed).

E. KONFIGURATION

- Lav årlig **Compliance Manager-assessment** mod NIS2 (eller IT-grundbeskyttelse)
- Konfigurér **Audit Premium** (E5 eller Purview Suite) hvis I har juridiske retention-krav
- Hold **kvartalsvise sikkerhedsreviews** med ledelsen
- Få **ekstern revision** mindst hvert andet år

F. AUDIT-BEVIS

- Compliance Manager assessment-rapporter (mindst årligt)
- Mødeprotokoller fra sikkerhedsreviews
- Ekstern revisor-rapport (hvis udført)
- Action item-tracker med status

07 KONTROL 7

Cyberhygiejne og awareness-træning

A. JURIDISK KRAV

"(g) basic cyber hygiene practices and cybersecurity training"

Dansk oversættelse: (g) grundlæggende cyberhygiejne-praksis og cybersikkerhedstræning

B. HVAD DET BETYDER I PRAKSIS

Medarbejdere skal trænes regelmæssigt, phishing, password-hygiejne, hvordan man rapporterer en mistænkelig email. Best practice er kvartalsvise simulationer og årlig formel træning. Completion tracking pr. medarbejder skal kunne fremvises.

C. MICROSOFT 365-FEATURES

Defender for Office 365 Attack Simulator (Premium+) (primær)

Defender Training campaigns med completion tracking (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem

E. KONFIGURATION

- Konfigurér **Attack Simulator** med kvartalsvise phishing-kampagner
- Opsæt **træningskampagner** for medarbejdere der falder for simulationer
- Krev **årlig formel awareness-træning** (intern eller ekstern udbyder)
- Track **completion pr. medarbejder** og dokumentér

F. AUDIT-BEVIS

- Phishing simulation-rapporter (mindst 4/år)
- Træningskampagne-completion-rapporter pr. medarbejder
- Årlig awareness-træning-bevis (signeret deltagerliste eller LMS-eksport)
- Skriftlig awareness-politik

08 KONTROL 8

Kryptering

A. JURIDISK KRAV

"(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption"

Dansk oversættelse: (h) politikker og procedurer vedrørende brugen af kryptografi og, hvor det er hensigtsmæssigt, kryptering

B. HVAD DET BETYDER I PRAKSIS

Data skal være krypteret både under overførsel og i hvile (in transit og at rest). Microsoft 365 har dette som standard for cloud-tjenester, men endpoints kræver BitLocker (Windows Enterprise via E3+). Plus styring af krypteringsnøgler, for de fleste SMV'er er Microsoft-managed nøgler tilstrækkeligt.

C. MICROSOFT 365-FEATURES

BitLocker via Intune (Windows Enterprise. E3+) (primær)

Sensitivity Labels med kryptering (Premium+) (primær)

Microsoft Purview Message Encryption (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem · **Fuld dækning kræver:** M365 E5

Manuel sensitivitetsmærkning og BitLocker dækkes af Business Premium. Auto-labeling (politik-baseret automatisk klassificering) og Customer Key til egen nøgle-styring kræver E5 eller Purview Suite-add-on plus Azure Key Vault.

E. KONFIGURATION

- Aktivér **BitLocker** via Intune device configuration profile
- Opret Sensitivity Labels for klassificering (Fortroligt, Internt, Offentligt)
- Konfigurér auto-labeling for følsomme data (kræver E5 eller Purview Suite)
- Slå Message Encryption til for ekstern email-trafik
- Skriv krypteringspolitik med nøglestyring

F. AUDIT-BEVIS

- Intune device compliance-rapport (BitLocker-status pr. enhed)
- Sensitivity Labels-politik-eksport fra Purview
- Skriftlig krypteringspolitik
- Message Encryption usage-rapport

09 KONTROL 9

HR-sikkerhed, adgangskontrol og enhedsstyring

A. JURIDISK KRAV

"(i) human resources security, access control policies and asset management"

Dansk oversættelse: (i) sikkerhed i forbindelse med menneskelige ressourcer, politikker for adgangskontrol og enhedsstyring (asset management)

B. HVAD DET BETYDER I PRAKSIS

Hele medarbejder-livscyklussen: ansættelse → adgang → ændringer → afslutning. Plus styring af enheder og data. Mindste-privilegium (least privilege), joiner-mover-leaver-processer og regelmæssige access reviews. Intune giver jer overblik over hvilke enheder der eksisterer og hvem der har dem.

C. MICROSOFT 365-FEATURES

Microsoft Entra ID Governance (E5 eller Entra ID Governance SKU) (primær)

Entra Access Reviews (Entra ID P2, del af E5) (primær)

Intune device inventory (supplerende)

D. LICENS-KRAV

Minimum-licens: M365 E5

Denne kontrol er den eneste hvor Business Premium *ikke* er tilstrækkelig på baseline. Entra ID Governance og Access Reviews kræver Entra ID P2, enten via E5 eller via Entra ID Governance som standalone-SKU ($7/bruger/md oven i en P1- eller P2-licens i listepris, aktuel DKK ses i sammenligningsværktøjet). For SMV'er er en kombination almindelig: Business Premium til hovedparten plus Entra ID Governance-SKU til 3-5 IT- og compliance-personer.

E. KONFIGURATION

- Dokumentér **joiner-mover-leaver-processer** skriftligt
- Konfigurér **Access Reviews** (kvartalsvis for privilegerede roller, halvårligt for resten)
- Anvend **Entitlement Management** for adgang til ressource-pakker
- Brug **Intune** til central enhedsregistrering og fjernsletning ved offboarding
- Privileged Identity Management (PIM) for admin-roller, kun just-in-time-adgang

F. AUDIT-BEVIS

- Skriftlig joiner-mover-leaver-politik
- Access Review-rapporter (komplet log over godkendt og nægtet adgang)
- Intune device inventory-eksport
- PIM-aktiverings-log for admin-roller

10 KONTROL 10

MFA og sikker kommunikation

A. JURIDISK KRAV

"(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate"

Dansk oversættelse: (j) brugen af multi-faktor autentificering eller kontinuerlige autentificeringsløsninger, sikrede tale-, video- og tekstkommunikation samt sikrede beredskabskommunikationssystemer i enheden, hvor det er hensigtsmæssigt

B. HVAD DET BETYDER I PRAKSIS

MFA er ikke valgfrit længere, tilsynet spørger først efter dette. Plus krypteret kommunikation (Teams gør det som standard) og en plan for hvordan I kommunikerer hvis primær-systemet er nede. Conditional Access giver granulær MFA-håndhævelse, fx kun fra ukendte lokationer eller nye enheder.

C. MICROSOFT 365-FEATURES

Microsoft Entra MFA (alle planer) (primær)

Conditional Access (Premium+ for granulær) (primær)

Teams Premium for advanced meeting protection (supplerende)

D. LICENS-KRAV

Minimum-licens: Business Prem

E. KONFIGURATION

- Krev MFA på alle konti, inkl. service accounts hvor muligt
- Konfigurér **CA-politikker:** MFA fra ukendte lokationer, blokér login fra højrisiko-lande, kræv compliant device for admin-portaler
- Slå **legacy auth** fra (Basic Auth i Exchange)
- Implementér **passkeys eller FIDO2** for privilegerede konti
- Beredskabskommunikation: dokumentér backup-kanal hvis Teams er nede (fx Signal, opkaldskæde)

F. AUDIT-BEVIS

- MFA registration-rapport (alle konti registreret med MFA)
- Conditional Access policy-eksport
- Sign-in log med MFA-claims (mindst 12 mdr)
- Skriftlig beredskabskommunikationsplan

NÆSTE SKRIDT

Hvordan kommer I i gang?

Mappingen ovenfor er udgangspunktet for jeres NIS2-implementering. Det er ikke en quick-fix — det er typisk et seks-måneders projekt for SMV'er. Tre konkrete skridt:

1. **Gap-analyse**
   Gå systematisk gennem de 10 kontroller og noter hvad I har på plads, hvad der kun er delvist, og hvad der mangler. Brug dette dokument som tjekliste.

2. **Licens-vurdering**
   Hold jeres nuværende Microsoft 365-licens op mod kravene. Særligt kontrol 6, 8 og 9 kræver typisk add-ons (Purview Suite eller Entra ID Governance) eller E5 for fuld dækning.

3. **Ledelses-forankring og projektplan**
   NIS2 kræver dokumenteret styring fra ledelsen. Sæt et kvartalsvis review i kalenderen og fordel ansvar mellem IT, jurist og forretningsejer.

> VÆRKTØJER PÅ LICENSLY.DK
>
> **NIS2-tjekket** — er I omfattet? 6 spørgsmål, 2 minutter → licensly.dk/nis2/tjek
> **Licens-decision matrix** — BP vs E3 vs E5 mod kravene → licensly.dk/nis2/licens-valg
> **Optimizer** — personlig licens-anbefaling → licensly.dk/optimize

---

Spørgsmål eller feedback?

Skriv direkte til **mso@ihanstholm.dk** — typisk svar inden for 24 timer på hverdage. Vi opdaterer dokumentet løbende; næste planlagte version i Q3 2026 når Intune Plan 2-features lander i E3/E5.