

Handlingsplan for korrigerende handlinger (CAP)

Software Fabric ApS : ISO 27001-projekt

Klassifikation: Intern · august 2026 · CVR 30276981

Dato	25.08.2026
Ejer	ISMS-ansvarlig (adm. direktør)
Klassifikation	Intern
Reference	Audit Rapport Stage 2, Report ID 401, Compliance Group Int. ApS
Auditdato	18.-19. august 2026
Indsendelsesfrist (CAP)	18.09.2026
Omfang	8 minor afvigelser samt 3 frivillige, allerede adresserede punkter

1. Formål og omfang

Denne handlingsplan besvarer de 8 minor afvigelser i Stage 2 audit rapport af 18.-19. august 2026 (Report ID 401). For minor afvigelser fremlægges planen for at opnå certifikatet, mens gennemførelsen verificeres ved næste overvågningsrevision. Planen fastlægger for hver afvigelse rodårsag, korrektion, korrigerende og forebyggende handling, ansvarlig og deadline.

Flere af afviklerne er dokumentationsopgaver, hvor kontrollen findes i den daglige drift, men endnu ikke er fuldt afspejlet i dokumentationen efter migrationen til MicroK8s. Handlingerne prioriterer varige, dokumenterede kontroller og klart ansvar frem for enkeltstående tiltag, i tråd med organisationens værdi om mennesker først.

Tekniske specifikationer, der hører under CTO, er markeret i teksten med [CTO: ...] og udfyldes af CTO. Angivne datoer er forslag, der bekræftes internt inden indsendelse. Ud over afviklerne behandles tre punkter frivilligt (opbevaring af kundedata, opsigelsesvilkår og disciplinær proces). De er ikke klassificeret som afvigelser i rapporten, men adresseres på forkant, så de ikke rejses igen ved næste surveillance.

2. Oversigt over afvigelser

ID	Krav/kontrol	Område	Type	Ansvarlig	Deadline	Status
403	Clause 8.2	Statement of Applicability	Minor	ISMS-ansvarlig / konsulent	18.09.2026	Planlagt
404	Clause 7.5.3	Dokument-/revisionsstyring	Minor	Konsulent / ISMS-ansvarlig	18.09.2026	Planlagt
406	Clause 9.1	Måling og KPI'er	Minor	ISMS-ansvarlig / CTO	18.09.2026	Planlagt
408	A.5.12	Informationsklassifikation	Minor	ISMS-ansvarlig / DPO	18.09.2026	Planlagt
412	A.5.9	Asset register	Minor	ISMS-ansvarlig / CTO	18.09.2026	Planlagt
413	A.7.5	Fysisk og miljømæssig sikring	Minor	CTO / direktør	27.08.2026 +	Delvist gennemført
414	A.8.13	Backup og restore-test	Minor	CTO	18.09.2026 +	Planlagt

ID	Krav/kontrol	Område	Type	Ansvarlig	Deadline	Status
415	A.8.21	SLA for kundevedt systemer	Minor	Direktør / CTO	Fastlægges	Planlagt

3. Handlingsplan pr. afvigelse

Afvigelse 403 : Statement of Applicability (clause 8.2)

Afvigelse (auditor)	SOA mangler de ansvarlige og er ikke helt gennemskuelig grundet implementeringen i MasterQMS.
Krav / kontrol	Clause 8.2, Statement of Applicability, jf. audit rapport.
Rodårsag	Ved overførsel af Statement of Applicability til MasterQMS blev feltet for ansvarlig pr. kontrol ikke udfyldt konsekvent, og det samlede udtræk er ikke opsat til et læsbart overblik. Kontrollerne har ejerskab i den daglige drift, men det fremgår ikke entydigt af SoA.
Korrektion	Statement of Applicability gennemgås, og ansvarlig påføres pr. kontrol.
Korrigerende handling	Der oprettes et obligatorisk felt for ansvarlig og ejer pr. kontrol i SoA i MasterQMS, og der genereres et samlet, læsbart SoA-udtræk med kontrolstatus og ansvarlig.
Forebyggende handling	Ansvarlig-feltet gøres obligatorisk i dokumentskabelonen, og gennemgang af SoA-ejerskab indgår som fast punkt i årshjulets dokumentgennemgang.
Ansvarlig	ISMS-ansvarlig i samarbejde med ekstern ISMS-konsulent.
Deadline	18.09.2026.
Status	Planlagt.

Afvigelse 404 : Dokument- og revisionsstyring (clause 7.5.3)

Afvigelse (auditor)	Revisionsstyring er ikke konsekvent.
Krav / kontrol	Clause 7.5.3, Styring af dokumenteret information.
Rodårsag	Dokumenter er migreret ind i MasterQMS over en længere periode, og revisionsnummer, dato og godkender fremstår ikke ensartet på tværs af dokumentindsamlingen. Indskrevet nogen steder som en del af dokumentet.
Korrektion	Dokumentoversigten gennemgås, og revisionsfelterne ensrettes.
Korrigerende handling	Der fastlægges en ensartet revisionsstandard (versionsnummer, dato, godkender og ændringslog), som anvendes i MasterQMS, og styringsproceduren for dokumenteret information (PRO016) opdateres tilsvarende.

Forebyggende handling	Fremover fjerner vi felterne fra skabelonerne, og lader MasterQMS automatisk styre revisionsnummer, ansvarlig og godkender.
Ansvarlig	Ekstern ISMS-konsulent i samarbejde med ISMS-ansvarlig.
Deadline	Procedure og standard inden 18.09.2026, ensretning af eksisterende dokumenter løbende og senest ved næste surveillance.
Status	Planlagt.

Afvigelse 406 : Måling og KPI'er (clause 9.1)

Afvigelse (auditor)	Der er ikke udvalgt målepunkter til KPI'er. Dette er tilsyneladende på grund af skiftet til ny platform og derfor ikke kørt helt på plads.
Krav / kontrol	Clause 9.1, Overvågning, måling, analyse og evaluering.
Rodårsag	Migrationen til MicroK8s ændrede grundlaget for de tekniske målepunkter, og et opdateret sæt informationssikkerheds-KPI'er er endnu ikke fastlagt og dokumenteret.
Korrektion	Der udvælges et første sæt KPI'er for informationssikkerhed.
Korrigerende handling	Der defineres et sæt KPI'er med kilde, målemetode, frekvens, målsætning og ansvarlig. Ledelsen fastlægger de organisatoriske KPI'er, fx gennemførelse af awareness, antal hændelser og lukning af afvigelser. <i>[CTO: fastlægger de tekniske målepunkter og datakilder, fx oppetid, backup-restore-succes og lukning af sårbarheder.]</i>
Forebyggende handling	KPI-opfølgning indarbejdes i ledelsesevalueringen og i årshjulet som kvartalsvis aktivitet.
Ansvarlig	ISMS-ansvarlig (organisatoriske mål) og CTO (tekniske målepunkter).
Deadline	KPI-sæt fastlagt inden 18.09.2026, første måling ved førstkomende kvartalsreview. Teknisk KPI-sæt (CTO): 09.10.2026
Status	Planlagt.

Afvigelse 408 : Informationsklassifikation (A.5.12)

Afvigelse (auditor)	Der er ikke formuleret en klassifikation for information, selvom den er initieret i SOA.
Krav / kontrol	Kontrol A.5.12, Klassifikation af information.
Rodårsag	Klassifikation håndteres i praksis for persondata (GDPR), men et samlet klassifikationsskema for information er ikke nedskrevet, og klassifikation af dokumenter er implicit.

Korrektion	Der udarbejdes et bevidst enkelt klassifikationsskema for information med tre niveauer.
Korrigerende handling	Der udarbejdes et klassifikationsskema med tre niveauer, kriterier, mærkning og håndteringsregler med udgangspunkt i DOC013. Skemaet holdes bevidst enkelt for at minimere vedligehold: Offentlig: information, der bevidst kan være frit tilgængelig, herunder strategi og markedsmateriale. Åbenheden er en bevidst ledelsesbeslutning, og risikoen ved videregivelse vurderes lav. Intern: information til brug i organisationen, som ikke er bestemt til offentliggørelse, men hvor utilsigtet spredning ikke medfører væsentlig skade. Fortroligt: de mest beskyttelseskrævende af virksomhedens egne data, herunder medarbejderes fortrolige data og personalesamtaler samt tekniske hemmeligheder som nøgler og adgangskoder. Kunde- og borgerdata i Planner4You er kundens data (kommunen er dataansvarlig, Software Fabric er databehandler) og indgår ikke i virksomhedens egen klassifikation, men håndteres efter databehandleraftale og GDPR. Kundeoplysninger fra CVR-registret er offentligt tilgængelige og klassificeres som Offentlig.
Forebyggende handling	Klassifikation gøres til obligatorisk felt i dokumentskabelonen og medtages i awareness-materialet.
Ansvarlig	ISMS-ansvarlig i samarbejde med DPO (for kategorier af persondata).
Deadline	18.09.2026.
Status	Planlagt.

Afvigelse 412 : Asset register (A.5.9)

Afvigelse (auditor)	Der skal udarbejdes et asset register, som fyldestgørende viser alle informationsaktiver, altså både hardware, hvor information er lagret, men også andre typer af informationer, som for eksempel regnskabsdata, kundedata, salgsdata og HR-data.
Krav / kontrol	Kontrol A.5.9, Fortegnelse over information og øvrige tilhørende aktiver.
Rodårsag	IT-udstysregisteret dækker hardware, men informationsaktiver (regnskabs-, kunde-, salgs- og HR-data mv.) er ikke registreret som selvstændige aktiver med ejer, placering og klassifikation.
Korrektion	Registeret udvides til at omfatte informationsaktiver ud over hardware.
Korrigerende handling	Asset register udvides med informationsaktiver med angivelse af ejer, system eller placering og klassifikation, koblet til klassifikationsskemaet under afvigelse 408. Kunde- og borgerdata i Planner4You medtages som et kundeejet aktiv, hvor Software Fabric er databehandler, og styres efter

	databehandleraftale og GDPR frem for virksomhedens egen klassifikation. <i>[CTO: kortlægger, hvilke systemer de enkelte informationsaktiver er lagret i.]</i>
Forebyggende handling	Asset register gennemgås som fast punkt i årshjulet, og der etableres en procedure for registrering af nye aktiver.
Ansvarlig	ISMS-ansvarlig (register og ejerskab) og CTO (systemplacering).
Deadline	Struktur og hovedaktiver inden 18.09.2026, fuld udfyldelse løbende. Kortlægning af informationsaktiver (CTO): 16.10.2026
Status	Planlagt.

Afvigelse 413 : Beskyttelse mod fysiske og miljømæssige trusler (A.7.5)

Afvigelse (auditor)	Der er ikke tilstrækkeligt designet procedure for beskyttelse mod fysiske og miljømæssige trusler. Som minimum skal der tilføjes til risikoregisteret: (1) at der forefindes aktive vandør i server- og kommunikationsrum, (2) at der mangler brandslukningsudstyr i server- og kommunikationsrum, (3) at der er manglende temperaturstyring i serverrum.
Krav / kontrol	Kontrol A.7.5, Beskyttelse mod fysiske og miljømæssige trusler.
Rodårsag	Proceduren for fysisk og miljømæssig beskyttelse dækkede ikke server- og kommunikationsrum tilstrækkeligt, og de tre konkrete forhold var ikke afspejlet i risikoregisteret. Temperaturudbedring var bestilt hos leverandør primo maj 2026 med lovet levering på 14 dage, men blev forsinket af leverandøren.
Korrektion	Temperaturstyring i serverrum udbedres den 27.08.2026 (leverandør bestilt primo maj 2026). De tre forhold tilføjes risikoregisteret med vurdering og behandling.
Korrigerende handling	Proceduren for beskyttelse mod fysiske og miljømæssige trusler opdateres, så server- og kommunikationsrum er omfattet. <i>[CTO og direktør: fastlægger de konkrete facilitetsmæssige tiltag vedrørende aktive vandør og brandslukningsudstyr.]</i>
Forebyggende handling	Temperaturlogging med alarm i serverrum, eskalering ved leverandørforsinkelse, og periodisk fysisk inspektion som fast punkt i årshjulet.
Ansvarlig	CTO i samarbejde med ISMS-ansvarlig (direktør).
Deadline	Temperatur 27.08.2026. Risikoregister og procedure inden 18.09.2026. Vandør og brandslukningsudstyr: dato fastlægges af CTO og direktør.
Status	Delvist gennemført (temperatur planlagt 27.08.2026).

Afvigelse 414 : Backup og restore-test (A.8.13)

Afvigelse (auditor)	Der skal anføres i proceduren scope og interval for udførelse af restore-test.
Krav / kontrol	Kontrol A.8.13, Sikkerhedskopiering af information.
Rodårsag	Sikkerhedskopiering udføres, men backup- og DR-proceduren angiver ikke eksplicit scope og interval for restore-test. DR-test er tidligere gennemført på den tidligere platform og er ikke gentaget efter migrationen til MicroK8s.
Korrektion	Scope og interval for restore-test anføres i proceduren.
Korrigerende handling	Backup- og DR-proceduren (jf. PRO009) opdateres med scope og interval for restore-test. <i>[CTO: fastlægger konkret testomfang, hyppighed og metode for restore-test.]</i>
Forebyggende handling	Restore-test indarbejdes som fast aktivitet i årshjulet med logføring af resultatet.
Ansvarlig	CTO.
Deadline	Proceduretekst inden 25.09.2026 Første restore-test på ny platform: 02.10.2026
Status	Planlagt.

Afvigelse 415 : SLA for kundevedte driftssystemer (A.8.21)

Afvigelse (auditor)	Der skal udarbejdes en SLA for kundevedte driftssystemer, alternativt skal kundeaftaler indeholde oplysninger om opetid, kundeservice-kanaler mv.
Krav / kontrol	Kontrol A.8.21, Sikring af netværkstjenester.
Rodårsag	Oppetid og servicevilkår håndteres i praksis, men er ikke formaliseret i en SLA og fremgår ikke entydigt af kundeaftalerne.
Korrektion	Der udarbejdes en SLA for kundevedte driftssystemer.
Korrigerende handling	Der udarbejdes en SLA med opetid, supportkanaler, responstider og vedligeholdelsesvinduer, alternativt indarbejdes disse oplysninger i kundeaftalerne. Den kontraktuelle indarbejdelse varetages af direktør. <i>[CTO: fastlægger de tekniske service- og opetidsmål.]</i>
Forebyggende handling	SLA gennemgås som fast punkt i årshjulet.
Ansvarlig	ISMS-ansvarlig og direktør (kontrakt) samt CTO (tekniske mål).
Deadline	Udkast til SLA inden næste surveillance, endelig dato fastlægges. Tekniske mål (CTO): 16.10.2026
Status	Planlagt.

4. Frivillige, allerede adresserede punkter (ikke afvigelser)

Punkterne nedenfor er ikke afvigelser i audit rapporten, men adresseres frivilligt med lovhenviisning. Argumentation: hvor et vilkår er lovbestemt og ufravigeligt, tilføjer en egen intern beskrivelse ikke styring ud over loven, men indfører en risiko for, at den interne tekst afviger fra loven ved en lovændring. En præcis henvisning til den gældende bestemmelse er derfor både tilstrækkelig og mere robust.

F1 : Opbevaring og sletning af kundedata (relateret til Observation 420, A.8.10)

Baggrund	Auditor har som observation (420) bemærket, at der bør udarbejdes en definition på, hvornår information ikke længere skal opbevares, med henvisning til gældende lovgivning og kundekrav. Punktet er ikke klassificeret som en afvigelse.
Handling	Slette- og opbevaringsreglerne i politik og procedure henviser til bogføringslovens § 10: regnskabsmateriale skal opbevares på betryggende vis i 5 år fra udgangen af det regnskabsår, materialet vedrører. For kundedata i bogholderiet er opbevaringspligten lovbestemt og ufravigelig, og lovhenviisningen er derfor tilstrækkelig som grundlag for perioden.
Ansvarlig	ISMS-ansvarlig i samarbejde med DPO.
Status	Lukket ved lovhenviisning.

F2 : Opsigelsesvilkår (funktionærloven)

Baggrund	Opsigelsesvarsler er beskrevet direkte i standardansættelseskontrakten (pkt. 7) med henvisning til funktionærlovens opsigelsesregler, og kontrakten indgik i auditors gennemgang. Punktet er ikke klassificeret som en afvigelse. Auditors HR-bemærkning om et forhold, der er implicit og ikke nedskrevet, angår den disciplinære proces, ikke opsigelsesvarslerne.
Handling	Ingen egentlig handling er nødvendig. Opsigelsesvarslerne fremgår af kontraktens pkt. 7 (prøvetid samt gradueret varsel efter anciennitet, 1 til 6 måneder) med udtrykkelig henvisning til funktionærlovens § 2, og pkt. 11 fastslår, at funktionær- og ferieloven gælder. Da varslerne er lovbestemte og ufravigelige til ugunst for funktionæren, er henvisningen tilstrækkelig. <i>Evidens: standardansættelseskontrakt, pkt. 7 og pkt. 11.</i>
Ansvarlig	ISMS-ansvarlig i samarbejde med DPO og HR.
Status	Allerede dokumenteret (kontrakt pkt. 7 og 11).

F3 : Disciplinær proces (A.6.4)

Baggrund	Auditors HR-bemærkning om et forhold, der er implicit og ikke nedskrevet, angår den disciplinære proces. Punktet er hverken en
-----------------	--

	afvigelse eller en observation, men nedskrives kort, så kontrol A.6.4 er dækket.
Handling	Den disciplinære proces nedskrives i HR-dokumentationen: hovedreglen ved overtrædelse af informationssikkerhedspolitikken er skriftlig advarsel med rimelig frist til at rette ind. Bortvisning er forbeholdt grov misligholdelse (vold eller trusler, tyveri og lignende). Processen følger funktionærlovens regler. Der lægges bevidst ikke op til væsentlig misligholdelse som selvstændig bortvisningsgrund, da denne er bevismæssigt tung.
Ansvarlig	ISMS-ansvarlig i samarbejde med DPO og HR.
Status	Planlagt (kort notat).