Et billede, der indeholder Font/skrifttype, Grafik, logo, skærmbillede

Automatisk genereret beskrivelse

OS2compliance

Løsningsbeskrivelse

|  |  |  |
| --- | --- | --- |
| Version: | Dato: | Ansvarlig |
| 1.0 | 23.05.2023 | NIBIS & KBP |

Indholdsfortegnelse

[2 Indledning 3](#_Toc136090787)

[3 Overordnet beskrivelse af OS2compliance 3](#_Toc136090788)

[3.1 Leverancemodel 3](#_Toc136090789)

[3.2 Drift af OS2compliance løsningen 4](#_Toc136090790)

[4 Løsningsbeskrivelse 4](#_Toc136090791)

[4.1 Brugerflade 4](#_Toc136090792)

[4.1.1 Gennemgående elementer 4](#_Toc136090793)

[4.1.2 Løsningsmoduler 4](#_Toc136090794)

[4.2 Master service 6](#_Toc136090795)

[4.3 Integrationer 6](#_Toc136090796)

[4.3.1 CVR 6](#_Toc136090797)

[4.3.2 AD FS integration 6](#_Toc136090798)

[4.3.3 KITOS integration 6](#_Toc136090799)

[5 Udruldning og implementering 7](#_Toc136090800)

[5.1 Teknisk opsætning 7](#_Toc136090801)

[5.2 Etablering af indhold & onboarding 7](#_Toc136090802)

[5.3 Organisatorisk implementering 8](#_Toc136090803)

[6 Tidsplan 8](#_Toc136090804)

# Indledning

Dette dokument er en løsningsbeskrivelse for version 1.0 af OS2compliance – et ISMS system (Information Security Management System).

Formålet med dokumentet er at sætte scope for en fuld funktionel version af OS2compliance, med understøttelse af de nødvendige ISMS-moduler.

Samtidig er dokumentet et beslutningsgrundlag for tilslutningen til OS2compliance projektet i OS2- regi, og har til mål at indeholde alle de relevante oplysninger som må indgå i denne beslutning.

Afsnit 3 indeholder en samlet, men overordnet, beskrivelse af OS2compliance, og suppleres af uddybende detaljer i de efterfølgende afsnit.

Afsnit 6 indeholder en tidsplan for projektets udviklingsplan.

# Overordnet beskrivelse af OS2compliance

OS2compliance er en komplet ISMS-løsning der udvikles med det formål at skabe et simpelt kommunespecifikt værktøj, der understøtter kommunernes komplekse setup med mange IT-systemer og mange behandlingsaktiviteter.

Udgangspunktet for designet er en naturlig sammenhæng mellem modulerne, så der skabes et godt overblik og det sikres, at viden er, hvor man har behov for den. Sammenhæng vil være i fokus, så der sikres så få klik som muligt.

Løsningen skal kunne rumme at være fagsystem for Informationssikkerhedsteamet, kontrolværktøj for de decentrale enheder og rapporteringsværktøj for ledelsen. Et samlet sted for arbejdet med compliance vedr. informationssikkerhed, som er udviklet til og af kommunerne.

Løsningen vil være bygget med mulighed for tilpasning, så man arbejder med compliance på kommunens aktuelle modenhedsniveau.

Videre vil løsningen have relevante integrationer, herunder AD-integration, KITOS-integration og CVR-integration, så tiden bruges på compliance og ikke vedligeholdelse af organisationsopsætning eller indtastning af aktiver.

OS2compliance tilgås via en browser.

## Leverancemodel

I forbindelse med udviklingen af OS2compliance er der nedsat en styregruppe, som sætter retningen, varetager projektets økonomi og driver udviklingsprojektet til version 1.0.

Det er forventningen, at der i løbet af udviklingsperioden vil blive nedsat en koordinationsgruppe der fremadrettet vil koordinere de deltagende kommuners ønsker og behov for videreudvikling og vedligeholdelse af produktet.

Dette dokument beskriver funktionaliteten i version 1.0 af OS2compliance.

Kommunerne der tilslutter sig OS2compliance styrer løbende, gennem styregruppen, videreudviklingen af OS2compliance, herunder nye moduler, nye integrationer m.m. som måtte ønskes. Leverandøren af OS2compliance har ansvaret for distribution af nye releases, fejlrettelser m.m. Information om kommende releases informeres løbende til de tilsluttede kommuner, med fuld transparens i økonomi, prioritering af opgaver og beslutninger via OS2s governance model.

## Drift af OS2compliance løsningen

Der etableres fælles drift af løsningen i OS2-regi, og det vil være muligt for den enkelte kommune at tilslutte sig den fælles driftsmodel, eller etablere egen drift af løsningen, hvis dette ønskes. Hvis man ønsker at drifte løsningen lokalt, skal man etablere de nødvendige servere, overvågning m.m. i egen it-infrastruktur.

# Løsningsbeskrivelse

OS2compliance består af en række moduler med en række integrationer. I dette afsnit beskrives modulernes indhold, og de integrationer der vil være mulige i version 1.0.

## Brugerflade

Der tages udgangspunkt i Bilag 1 - OS2compliance.pptx, der illustrerer systemets indhold og struktur.

### Gennemgående elementer

Følgende elementer vil altid være synlig for brugeren:

* Navigationspanelet placeret i venstre side af skærmen.
* En søgebar i toppen af skærmen, der muliggør en global søgning på tværs af hele løsningen. Denne søgefunktion vil tillade brugeren at finde opgaver, leverandører, fortegnelser og aktiver.
* En funktion for oprettelse af nye opgaver vil altid være tilgængelig.

### Løsningsmoduler

OS2compliance består i første version af følgende moduler:

* Dashboard
* SoA
* Fortegnelse
* Aktiver
* Leverandører
* Risikostyring
* Dokumenter
* Opgavecenter
* Rapporter

#### Dashboard

Dashboardet vil have fokus på compliancestatus og opgaver. Det vil være herfra at opgaveansvarlig kan danne sig et overblik over egne fremtidige/forfaldne opgaver og udføre dem.

#### SoA

SoA dækker over arbejdet med de valgte standarder. Modulet er bygget op omkring ISO27001 og ISO27002 og vil også indeholde andre relevante standarder som ISO27701, NSIS, NIS2 og Kommunernes tekniske minimumsstandarder. Modulet giver mulighed for et overblik over efterlevelsen af de tilvalgte standarder og for at arbejde med det enkelte krav. Sammenhængen mellem modulerne vil give et godt overblik over hvilke dokumenter der understøtter de enkelte foranstaltninger.

*Indstillinger for modulet: Man skal kunne til/fravælge hvilke standarder der er relevante*

#### Fortegnelse

Fortegnelsen vil være bygget op omkring KL´s behandlingsaktiviteter og vil leve op til kravene i GDPR-forordningen. Det vil være muligt at tilføje kommunespecifikke behandlingsaktiviteter, ligesom det vil være muligt at undlade import af KL´s behandlingsaktiviteter.

Fortegnelsen vil være en samlet liste hvor et klik på en konkret behandlingsaktivitet vil lede til en fanestruktur med relevante registreringsmuligheder, herunder tilknytning af aktiver (IT-systemer), dokumenter, risikovurderinger, opgaver mv.

*Indstillinger for modulet: tilvalg/fravalg af KL’s behandlingsaktiviteter*

#### Aktiver

Aktiver dækker bredt over de elementer kommunen ønsker at registrere f.eks. IT-systemer, moduler, servere, switche mv. Kategorisering sikrer overblik. En liste over alle registrerede aktiver giver et samlet overblik hvorfra det vil være muligt at klikke sig ind i det enkelte aktiv. Her vil en mappestruktur give mulighed for relevante indtastninger, herunder oplysninger omkring databehandling, tilsyn og risikovurderinger, samt guides til konsekvensanalyse og TIA. Det vil være muligt at få overblik over og registrere sammenhæng til behandlingsaktiviteter, relaterede aktiver, dokumenter og opgaver. Er disse oplysninger allerede registreret f.eks. på en behandlingsaktivitet, vil sammenhæng fremgå af overblikket

*Indstillinger for modulet: Mulighed for opsætning af KITOS integration*

#### Leverandører

Leverandørlisten vil som modulerne for fortegnelse og aktiver være bygget op med en samlet liste med mulighed for klik til den enkelte leverandør, der i en fanestruktur vil give mulighed for at taste relevant data og se sammenhæng til aktiver, dokumenter og opgaver.

#### Risikostyring

Risikostyring bygges op efter ISO27005 hvor det vil være muligt at risikovurdere et aktiv, en behandlingsaktivitet eller et scenarie. Der vil være prædefinerede trusselskataloger og mulighed for at oprette egne. Selve risikovurderingen tager udgangspunkt i en vurdering af sandsynlighed og konsekvens for den enkelte trussel med mulighed for at vurdere ud fra den registrerede og for kommunen. Det vil i en arbejdsgang være muligt at oprette opgaver for trusler der skal mitigeres. Den simple skalerbarhed vil sikre et flydende arbejde med risikovurdering og en oplevelse af, at de giver stor værdi for organisationen.

*Indstillinger for modulet: Mulighed for at tilføje trusselskataloger*

#### Dokumenter

Dokumenter indeholder et overblik over de typer dokumenter kommunen ønsker at registrere, f.eks. politikker, procedurer, arbejdsgange, vejledninger, databehandleraftaler, kontrakter mv. Løsningen vil ikke være dokumentbærende, men give mulighed for at linke til dokumentet.

Dokumenter kan kobles til aktiver, leverandører, behandlingsaktiviteter, opgaver/kontroller mv.

#### Opgavecenter

Opgavecenter skaber overblik over både opgaver/kontroller for hele organisationen, både gennemførte og kommende. Fra alle sider i løsningen, er det muligt at oprette en opgave eller en gentagen kontrol. Oprettelsen er holdt så simpel som muligt så det kun er nødvendige oplysninger der skal registreres for at oprette opgaven. Logsporet for den enkelte opgave/kontrol sikre dokumentation til revisionen.

Der skal være filtreringsmuligheder så brugeren kan sortere opgaverne baseret på forskellige parametre såsom ansvarlig, opgavetype, eller om opgaven er i fremtiden eller allerede er udført.

#### Rapporter

Rapportmodulet vil udstille et overblik over de rapporter, det er muligt at trække ud af løsningen, herunder SoA, Informationssikkerhedshåndbog, NSIS bilag A, Artikel 30-fortegnelse, ledelsesrapporter fra risikovurderinger, tilsynsrapporter, revisionsrapporter.

Rapporter kan hentes i enten Excel eller Word/PDF format.

Ved generering af en ledelsesrapport er det muligt at vælge den tilknyttede risikovurdering. For at lette processen implementeres der en søgefunktion for nem og hurtig identifikation af den relevante risikovurdering.

#### Indstillinger

Indstillinger vil være tilgængelig på den enkelte modul-side, og vil kun udstille indstillingsmulighederne for netop dette modul. Det vil kun være administrator der har mulighed for at sætte indstillingerne, som vil slå igennem for alle brugere af løsningen.

## Master service

Der udvikles en master service som tilgås på en separat adresse, fx master.os2compliance.dk

Her ligges skabeloner som går på tværs af kommunerne.

I første version vil det være trusselskataloger og standarderne: ISO27001, ISO27002, ISO27701 og NSIS.

## Integrationer

### CVR

CVR Data hentes fra Datafordeleren.

Integrationen benyttes når man opretter en ny leverandør. Når man indtaster CVR nummeret vil integrationen slå virksomheden op og forud udfylde felterne med de værdier som kunne hentes.

### AD FS integration

Login til løsningen, håndteres via SAML 2.0 standarden. Løsningen integrerer til kommunens lokale IdP løsning fx AD FS.

### KITOS integration

Man kan vælge at udtrække it-systemer som aktiver fra Kitos data, eller man kan oprette dem manuelt.

# Udruldning og implementering

OS2compliance indeholder implementering i tre niveauer:

* Teknisk opsætning af løsningen
* Etablering af indhold & onboarding
* Organisatorisk implementering

Når der er indgået en drifts- og implementeringsaftale med OS2 omkring brugen af OS2compliance infrastrukturen, ser et typisk implementeringsforløb med OS2compliance ud som følger:

1. Der udarbejdes kommune-specifikt vejledningsmateriale til teknisk implementering
2. AD FS integrationen opsættes for kommunen (1-2 timers arbejde for en systemadministrator i kommunen)
3. KITOS integration opsættes for kommunen
4. Data indlæses manuelt i OS2compliance parallelt med et oplæringsforløb
5. Organisatoriske implementering påbegyndes

## Teknisk opsætning

Ved etablering opsætter leverandøren et driftsmiljø til kommunen.

Kommunen skal i den forbindelse levere SAML metadata for den Identity Provider (fx AD FS) der skal anvendes til at logge kommunens brugere på løsningen.

## Etablering af indhold & onboarding

Når den tekniske opsætning er gennemført, kan indlæsning af data påbegyndes, hvilket NIBIS Konsulenterne vil gøre manuelt for at sikre den korrekte tilpasning til kommunens arbejde med ISMS.

Udgangspunktet er, at det er kommunens eksisterende data, der indlæses efter følgende plan:

Ovenstående skal ses som NIBIS Konsulenternes forslag til en implementeringsplan, med mulighed for tilpasning til kommunens ønsker for den gode onboarding.

## Organisatorisk implementering

Ofte vil arbejdet med informationssikkerhed i kommunen være bygget op med et centralt informationssikkerhedsteam der har overblik over og drifter kommunens ISMS, med en række kontroller der skal udføres af decentrale ledere.

Ønsker Kommune det, kan implementeringen omfatte 2 indledende og 2 opfølgende workshops med de medarbejdere der skal gennemføre kontrollerne. Workshopsene faciliteres af implementeringskonsulenten fra NIBIS Konsulenterne.

På første workshop introduceres løsningen med en gennemgang af vejledninger og hvordan man konkret gennemfører en kontrol i løsningen. Anden workshop har fokus på at besvare spørgsmål og yderligere gennemgang af arbejdsgange/vejledning mv.

# Tidsplan

Udviklingen af den beskrevne funktionalitet til version 1.0 igangsættes i juni 2023 og vil løbe til september. Løsningen udvikles modulvis efter en metode hvor udviklingen løbende testes af styregruppen. Den løbende test vil sikre, at version 1.0 er gennemprøvet når den er klar til implementering i oktober 2023.

Da løsningen kræver en håndholdt implementering med en grundig onboarding, vil kommunerne efter en individuel aftale løbende blive onboardet. Det betyder at de kommuner der tilslutter sig løsningen først, vil blive onboardet først.