Hvordan bruke Normens krav i anskaffelser.
Veiledning i bruk av arbeidsboken

Dette dokumentet gir en beskrivelse av arbeidsboken oppbygging og kort veiledning i hvordan det kan brukes.

SUSANNE HELLAND FLATØY

Innhold

Veiledning i bruk av dokumentet «Hvordan bruke Normens krav i anskaffelser».

Det er utviklet et nytt vedlegg med navnet «Hvordan bruke Normens krav i anskaffelser[1]». Vedlegget er utarbeidet i Excel og kan sees som en plukkliste med krav som gir støtte i arbeidet med konkurransegrunnlag, utarbeidelse av kvalifikasjonskrav og kravspesifikasjoner. Dokumentet inneholder også mapping av alle normens krav mot krav i NS-EN ISO/IEC 27001:2017og NS-EN ISO/IEC 27002:2017.

Dette dokumentet gir en beskrivelse av arbeidsboken oppbygging og kort veiledning i hvordan det kan brukes.

Bakgrunn

Arbeidet med utvikling av nytt vedlegg om hvordan bruke Normens krav i anskaffelser har tatt utgangspunkt i "Vedlegg Oversikt over Normens krav". Målet er å gjøre det lettere å bruke normens krav i it-anskaffelser.

Om oppbygging

Vedlegget er utformet i Excel og inneholder 5 følgene Ark

- ARK 01 OM ARBEIDSBOKEN
- **02 NORM FOR INF.SIKKERHET-KRAV**
- ARK 03 KRAV I ANSKAFFELSER
- ARK 04 KOBLING ISO 27001
- ARK 05 KOBLING ISO 27002

Se vedlegg med beskrivelse av de ulike arkene

Om anskaffelsesprosessen

Påvirkningsmuligheten størst tidlig i prosessen. Det er her alle premisser og føringer blir lagt. Feil i planleggingsfasen kan medføre uønskede konsekvenser senere i prosessen. Det er også viktig å gjennomføre selve konkurransen i markedet profesjonelt og ikke minst følge opp kontrakten slik at behov og resultater blir oppfylt i henhold til inngått kontrakt.

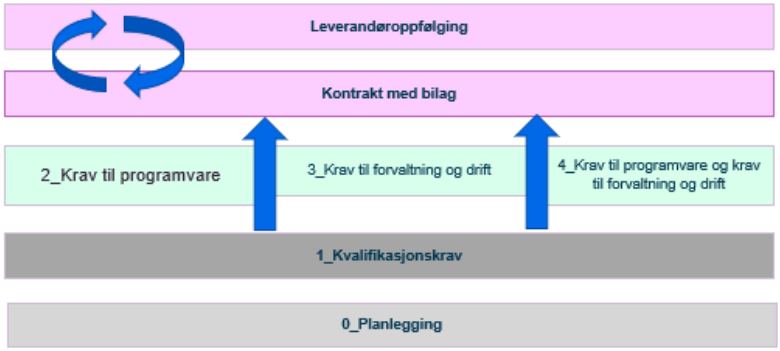
Inndeling av ulike type krav

Krav som kan være nyttig å vurdere i forbindelse med anskaffelser har blitt merket med følgende type kategori under kolonnen «**Krav i anskaffelser»**

- Krav til planlegging
- Kvalifikasjonskrav
- Krav til programvare
- Krav til forvaltning og drift
- Krav til programvare og krav til forvaltning og drift

Alle krav i normen er utledet fra lovkrav og vil derfor være obligatorisk krav.

[1] Bruk gjerne vedlegget sammen med DFØs veiledning i anskaffelsesprosessen https://anskaffelser.no/anskaffelsesprosessen/anskaffelses-prosessen-steg-steg

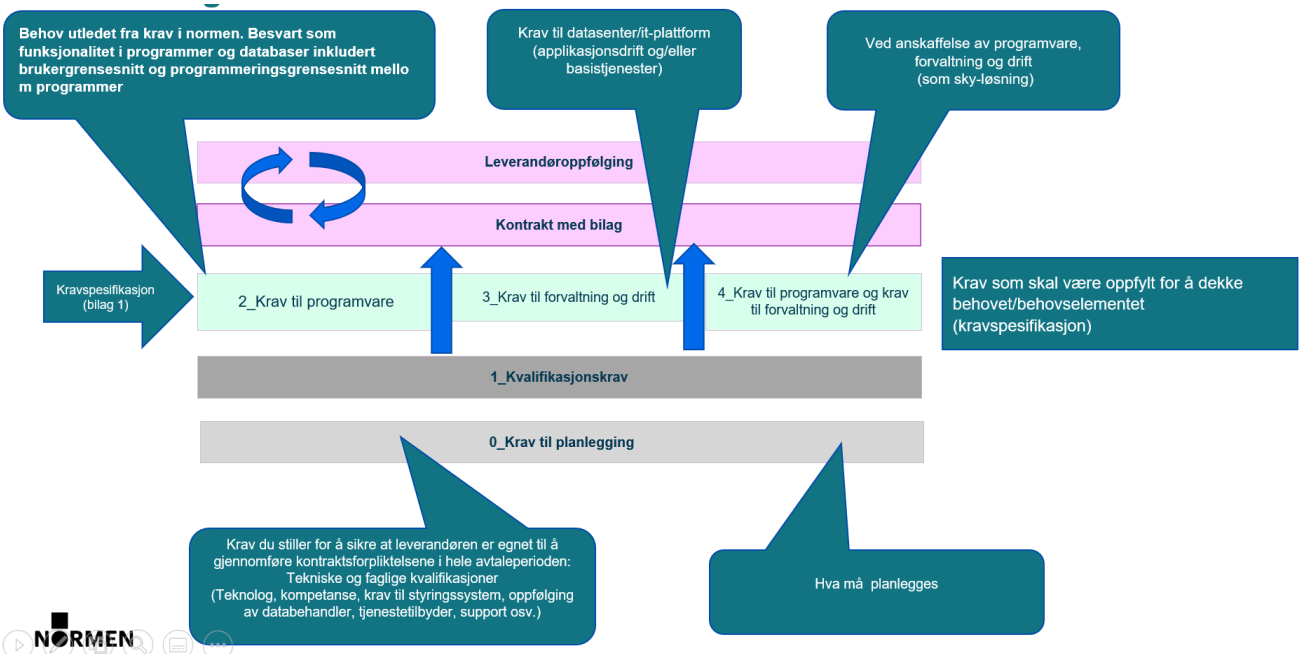


Spesifikasjoner som behovselementer

Vedlegget er ment som en plukkliste for relevante krav, og kraven må formulere slik behovene kommer tydelig frem. Spesifikasjonen er måten behovene beskrives på. Det vil som regel være ulike behovselementer i en og samme anskaffelse:

- Behov for en viss kapasitet
- Behov for en viss tilgjengelighet
- Behov for å tilfredsstille en viss brukervennlighet
- Behov for logging
- Etc, etc

Alle disse behovselementene vil til sammen dekke behovet i anskaffelsen.



Gode spesifikasjoner:

- Øker sannsynligheten for at leveransen dekker behovet
- Åpner for kostnadseffektive løsninger
- Stimulerer til innovasjon
- Gir grunnlag for effektive garantier
- Gir riktig risikofordeling mellom oppdragsgiver og leverandør

Åpne spesifikasjoner

Hovedregelen er at det skal spesifiseres åpent ved å beskrive behovet og krav til ytelsen og ikke ved detaljerte beskrivelser av konkrete løsninger.

Åpne spesifikasjoner legger til rette for å få den beste løsningen fordi åpne spesifikasjoner inviterer til flere løsningsalternativer, løsninger oppdragsgiver ikke kjenner til og også helt nye innovative løsninger som vil dekke behovet på en bedre måte.

Kravspesifikasjonen skal angi kravene som stilles til egenskapene til systemet som skal anskaffe.

Kontrakt og kontraktsvilkår

Kontrakten fordeler risiko og angir partenes ansvar og forpliktelser i avtaleperioden og skal angis i kunngjøringen eller konkurransegrunnlaget.

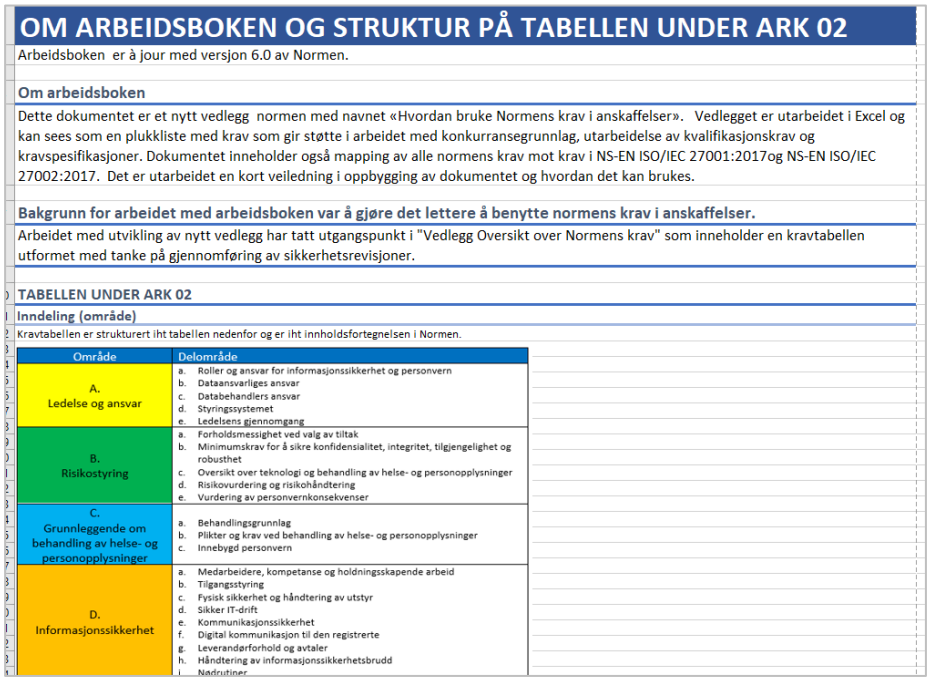
Leverandøroppfølging

Kontrakten legger grunnlag for oppfølging av leverandør.

Vedlegg – beskrivelse av innhold i ARK 01 – ARK 05

ARK 01 OM ARBEIDSBOKEN

Inneholder informasjon om innhold i de ulike kolonene under ark 2 og de enkelte arkene i arbeidsboken.



OM ARBEIDSBOKEN OG STRUKTUR PÅ TABELLEN UNDER ARK 02

Arbeidsboken er à jour med versjon 6.0 av Normen.

Om arbeidsboken

Dette dokumentet er et nytt vedlegg normen med navnet «Hvordan bruke Normens krav i anskaffelser». Vedlegget er utarbeidet i Excel og kan sees som en plukkliste med krav som gir støtte i arbeidet med konkurransegrunnlag, utarbeidelse av kvalifikasjonskrav og kravspesifikasjoner. Dokumentet inneholder også mapping av alle normens krav mot krav i NS-EN ISO/IEC 27001:2017og NS-EN ISO/IEC 27002:2017. Det er utarbeidet en kort veiledning i oppbygging av dokumentet og hvordan det kan brukes.

Bakgrunn for arbeidet med arbeidsboken var å gjøre det lettere å benytte normens krav i anskaffelser.

Arbeidet med utvikling av nytt vedlegg har tatt utgangspunkt i "Vedlegg Oversikt over Normens krav" som inneholder en kravtabellen utformet med tanke på gjennomføring av sikkerhetsrevisjoner.

TABELLEN UNDER ARK 02

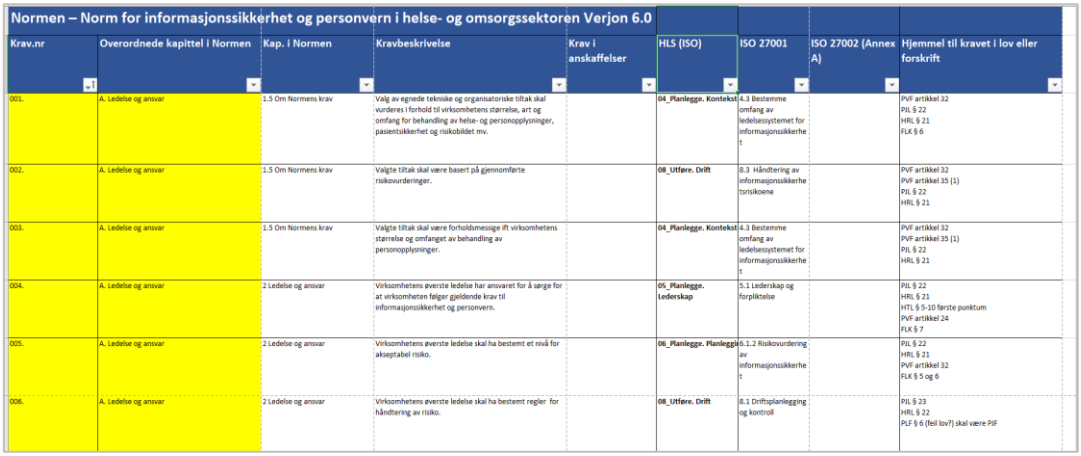
Inndeling (område)

Kravtabellen er strukturert iht tabellen nedenfor og er iht innholdsfortegnelsen i Normen.

Område	Delområde
A. Ledelse og ansvar	a. Roller og ansvar for informasjonssikkerhet og personvern b. Dataansvarliges ansvar c. Databehandlers ansvar d. Styringssystemet e. Ledelsens gjennomgang
B. Risikostyring	a. Forholdsmessighet ved valg av tiltak b. Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet c. Oversikt over teknologi og behandling av helse- og personopplysninger d. Risikovurdering og risikohåndtering e. Vurdering av personvernkonsekvenser
C. Grunnleggende om behandling av helse- og personopplysninger	a. Behandlingsgrunnlag b. Plikter og krav ved behandling av helse- og personopplysninger c. Innebygd personvern
D. Informasjonssikkerhet	a. Medarbeidere, kompetanse og holdningsskapende arbeid b. Tilgangsstyring c. Fysisk sikkerhet og håndtering av utstyr d. Sikker IT-drift e. Kommunikasjonssikkerhet f. Digital kommunikasjon til den registrerte g. Leverandørforhold og avtaler h. Håndtering av informasjonssikkerhetsbrudd i. Nødrutiner

02 NORM FOR INF.SIKKERHET-KRAV

Inneholder alle kravene i normen fra nummer 1 til 294. For hver krav er gitt referanser i de ulike kolonne.

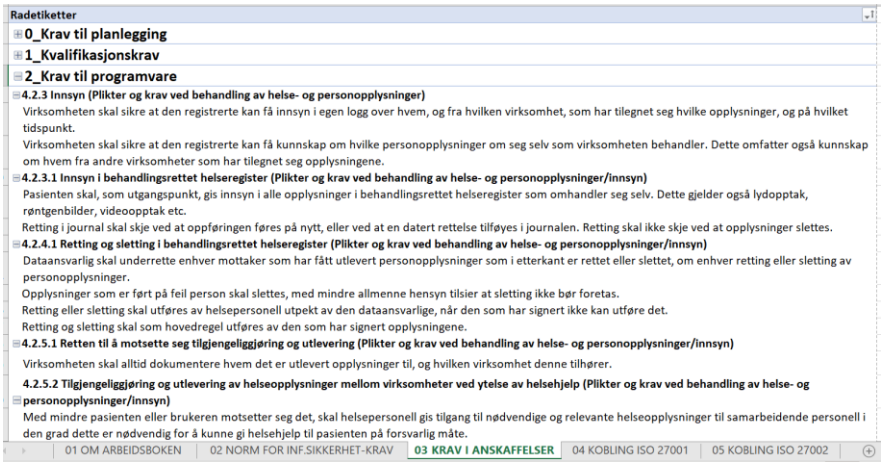


Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren Verjon 6.0								
Krav.nr	Overordnede kapittel i Normen	Kap. i Normen	Kravbeskrivelse	Krav i anskaffelser	HLS (ISO)	ISO 27001	ISO 27002 (Annex A)	Hjemmel til kravet i lov eller forskrift
001.	A. Ledelse og ansvar	1.5 Om Normens krav	Valg av egnede tekniske og organisatoriske tiltak skal vurderes i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet og risikobildet mv.		04_Planlegge. Kontekst	4.3 Bestemme omfang av ledelsessystemet for informasjonssikkerhet		PVF artikkel 32 PIL § 22 HRL § 21 FLK § 6
002.	A. Ledelse og ansvar	1.5 Om Normens krav	Valgte tiltak skal være basert på gjennomførte risikovurderinger.		08_Utføre. Drift	8.3 Håndtering av informasjonssikkerhetsrisikoene		PVF artikkel 32 PVF artikkel 35 (1) PIL § 22 HRL § 21
003.	A. Ledelse og ansvar	1.5 Om Normens krav	Valgte tiltak skal være forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger.		04_Planlegge. Kontekst	4.3 Bestemme omfang av ledelsessystemet for informasjonssikkerhet		PVF artikkel 32 PVF artikkel 35 (1) PIL § 22 HRL § 21
004.	A. Ledelse og ansvar	2 Ledelse og ansvar	Virksomhetens øverste ledelse har ansvaret for å sørge for at virksomheten følger gjeldende krav til informasjonssikkerhet og personvern.		05_Planlegge. Lederskap	5.1 Lederskap og forpliktelse		PIL § 22 HRL § 21 HTL § 5-10 første punktum PVF artikkel 24 FLK § 7
005.	A. Ledelse og ansvar	2 Ledelse og ansvar	Virksomhetens øverste ledelse skal ha bestemt et nivå for akseptabel risiko.		06_Planlegge. Planlegge	6.1.2 Risikovurdering av informasjonssikkerhet		PIL § 22 HRL § 21 PVF artikkel 32 FLK § 5 og 6
006.	A. Ledelse og ansvar	2 Ledelse og ansvar	Virksomhetens øverste ledelse skal ha bestemt regler for håndtering av risiko.		08_Utføre. Drift	8.1 Driftsplanlegging og kontroll		PIL § 23 HRL § 22 PLF § 6 (feil lov?) skal være PIF

- Inneholder følgende kolonner
    - Alle normens krav nummerert fra 1-294
    - Kravtabellen er strukturert iht. Overordnede kapittel i Normen (fargekode gul, grønn, blå og Orange) og iht. innholdsfortegnelsen i Normen (Kap. i Normen)
    - Krav i anskaffelser er strukturert i iht. 5 ulike type krav (krav til planlegging, kvalifikasjonskrav, krav til programvare, krav til forvaltning og drift)
    - ISO 27001, inneholder referansene til standardens kapittelinndeling
    - ISO 27002 (Annex A) inneholder referansene til standardens kapittelinndeling
    - I kolonnen HLS (ISO) struktureres kravene i henhold til ISO sin **overordnet struktur** High Level Structure (HLS). HLS-tilnærmingen er basert på en logisk og fornuftig idé om å harmonisere grunnstrukturen og innholdet i alle styringssystemer. Denne felles tilnærmingen vil spesielt være nyttig for organisasjoner som velger å bruke ett enkelt ledelsessystem (integrert ledelsessystem) som oppfyller kravene i to eller flere ledelsessystemstandarder.
    - Hjemmel til kravet i lov eller forskrift, referanser til lovkrav som danner grunnlaget for kravet i Normen.

ARK 03 KRAV I ANSKAFFELSER

En visning av kravene i ARK 2 gruppert på type krav (pivottabell)



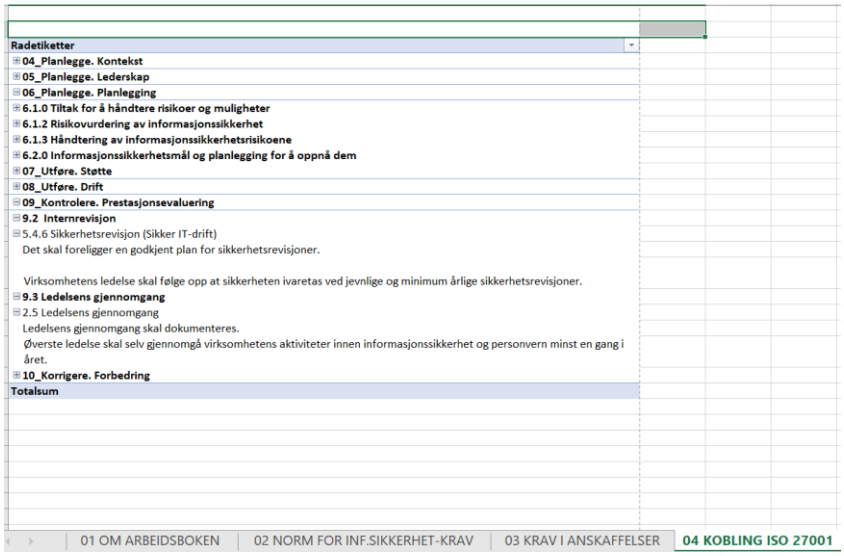
Radetiketter

- **0_Krav til planlegging**
- **1_Kvalifikasjonskrav**
- **2_Krav til programvare**
    - **4.2.3 Innsyn (Plikter og krav ved behandling av helse- og personopplysninger)**
      Virksomheten skal sikre at den registrerte kan få innsyn i egen logg over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt.
      Virksomheten skal sikre at den registrerte kan få kunnskap om hvilke personopplysninger om seg selv som virksomheten behandler. Dette omfatter også kunnskap om hvem fra andre virksomheter som har tilegnet seg opplysningene.
    - **4.2.3.1 Innsyn i behandlingsrettet helseregister (Plikter og krav ved behandling av helse- og personopplysninger/innsyn)**
      Pasienten skal, som utgangspunkt, gis innsyn i alle opplysninger i behandlingsrettet helseregister som omhandler seg selv. Dette gjelder også lydopptak, røntgenbilder, videoopptak etc.
      Retting i journal skal skje ved at oppføringen føres på nytt, eller ved at en datert rettelse tilføyes i journalen. Retting skal ikke skje ved at opplysninger slettes.
    - **4.2.4.1 Retting og sletting i behandlingsrettet helseregister (Plikter og krav ved behandling av helse- og personopplysninger/innsyn)**
      Dataansvarlig skal underrette enhver mottaker som har fått utlevert personopplysninger som i etterkant er rettet eller slettet, om enhver retting eller sletting av personopplysninger.
      Opplysninger som er ført på feil person skal slettes, med mindre allmenne hensyn tilsier at sletting ikke bør foretas.
      Retting eller sletting skal utføres av helsepersonell utpekt av den dataansvarlige, når den som har signert ikke kan utføre det.
      Retting og sletting skal som hovedregel utføres av den som har signert opplysningene.
    - **4.2.5.1 Retten til å motsette seg tilgjengeliggjøring og utlevering (Plikter og krav ved behandling av helse- og personopplysninger/innsyn)**
      Virksomheten skal alltid dokumentere hvem det er utlevert opplysninger til, og hvilken virksomhet denne tilhører.
    - **4.2.5.2 Tilgjengeliggjøring og utlevering av helseopplysninger mellom virksomheter ved ytelse av helsehjelp (Plikter og krav ved behandling av helse- og personopplysninger/innsyn)**
      Med mindre pasienten eller brukeren motsetter seg det, skal helsepersonell gis tilgang til nødvendige og relevante helseopplysninger til samarbeidende personell i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte.

01 OM ARBEIDSBOKEN | 02 NORM FOR INF.SIKKERHET-KRAV | **03 KRAV I ANSKAFFELSER** | 04 KOBLING ISO 27001 | 05 KOBLING ISO 27002

ARK 04 KOBLING ISO 27001

En visning av kravene i ARK 2 gruppert på kapittel i ISO 27001 (pivottabell)

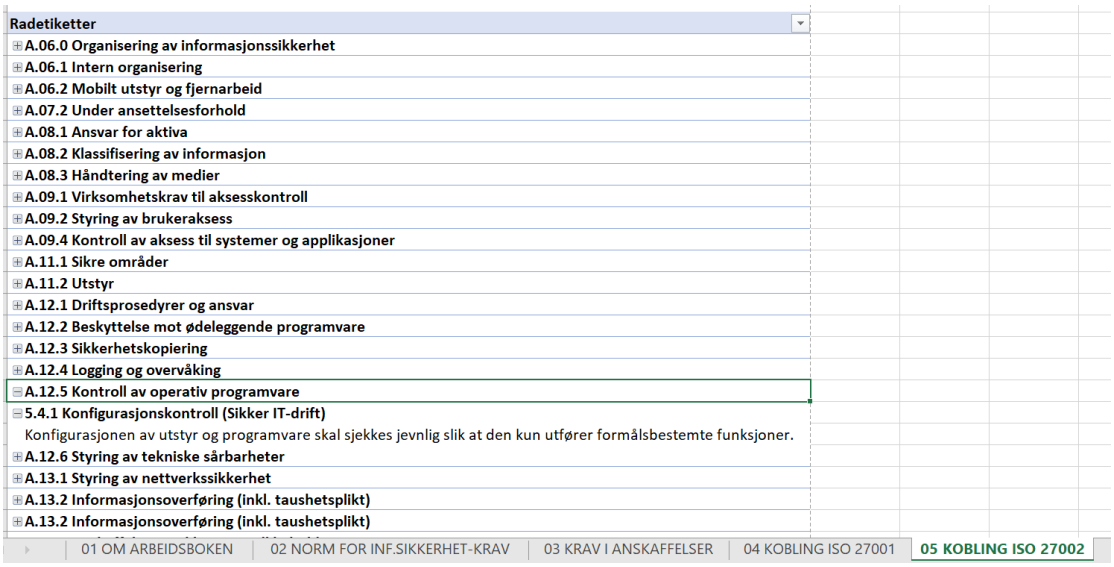


Radetiketter
04_Planlegge. Kontekst
05_Planlegge. Lederskap
06_Planlegge. Planlegging
6.1.0 Tiltak for å håndtere risikoer og muligheter
6.1.2 Risikovurdering av informasjonssikkerhet
6.1.3 Håndtering av informasjonssikkerhetsrisikoene
6.2.0 Informasjonssikkerhetsmål og planlegging for å oppnå dem
07_Utføre. Støtte
08_Utføre. Drift
09_Kontrolere. Prestasjonsevaluering
9.2 Internrevisjon
5.4.6 Sikkerhetsrevisjon (Sikker IT-drift)
Det skal foreligger en godkjent plan for sikkerhetsrevisjoner.
Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner.
9.3 Ledelsens gjennomgang
2.5 Ledelsens gjennomgang
Ledelsens gjennomgang skal dokumenteres.
Øverste ledelse skal selv gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året.
10_Korrigere. Forbedring
Totalsum

01 OM ARBEIDSBOKEN | 02 NORM FOR INF.SIKKERHET-KRAV | 03 KRAV I ANSKAFFELSER | 04 KOBLING ISO 27001

ARK 05 KOBLING ISO 27002

En visning av kravene i ARK 2 gruppert på kapittel i ISO 27002 (pivottabell)



Radetiketter
A.06.0 Organisering av informasjonssikkerhet
A.06.1 Intern organisering
A.06.2 Mobilt utstyr og fjernarbeid
A.07.2 Under ansettelsesforhold
A.08.1 Ansvar for aktiva
A.08.2 Klassifisering av informasjon
A.08.3 Håndtering av medier
A.09.1 Virksomhetskrav til aksesskontroll
A.09.2 Styring av brukeraksess
A.09.4 Kontroll av aksess til systemer og applikasjoner
A.11.1 Sikre områder
A.11.2 Utstyr
A.12.1 Driftsprosedyrer og ansvar
A.12.2 Beskyttelse mot ødeleggende programvare
A.12.3 Sikkerhetskopiering
A.12.4 Logging og overvåking
A.12.5 Kontroll av operativ programvare
5.4.1 Konfigurasjonskontroll (Sikker IT-drift)
Konfigurasjonen av utstyr og programvare skal sjekkes jevnlig slik at den kun utfører formålsbestemte funksjoner.
A.12.6 Styring av tekniske sårbarheter
A.13.1 Styring av nettverkssikkerhet
A.13.2 Informasjonsoverføring (inkl. taushetsplikt)
A.13.2 Informasjonsoverføring (inkl. taushetsplikt)

01 OM ARBEIDSBOKEN | 02 NORM FOR INF.SIKKERHET-KRAV | 03 KRAV I ANSKAFFELSER | 04 KOBLING ISO 27001 | 05 KOBLING ISO 27002

Veiledning i bruk av vedlegg til Normen - Hvordan bruke Normens krav i anskaffelser