

Veileder - Hvordan bruke Normens krav i anskaffelser.

Dette er en veiledning i hvordan en virksomhet kan benytte Excel-arket "Normens krav mappet mot krav i anskaffelser, krav i ISO 27001 og kontroller i ISO 27002" i forbindelse med anskaffelser. Veilederen inneholder informasjon om Excel-arket sin oppbygging og hvordan det kan brukes.

Excel-arket "Normens krav mappet mot krav i anskaffelser, krav i ISO 27001 og kontroller i ISO 27002" kan lastes ned fra [Normen.no](https://normen.no)

1. Innhold

1.	Innhold	1
2.	Veileder – hvordan bruke Normens krav i anskaffelser	2
2.1	Bakgrunn	2
2.2	Om anskaffelsesprosessen	2
2.2.1	Inndeling av ulike type krav.....	2
2.2.2	Hvordan beskrive krav som behov	3
2.2.3	Bruk av åpne spesifikasjoner	3
2.2.4	Kontrakt og kontraktsvilkår	3
2.2.5	Leverandøroppfølging	3
3.	Om Excel-arket	3
3.1	Om fanekortene (ark) i Excel arket.....	3
3.1.1	Om Excel arket.....	4
3.1.2	Alle Normens krav	4
3.2	Benytt Excel arket for å finne relevante krav i forbindelse med anskaffelser	4
3.2.1	Forberedelser og avklaringer før anskaffelser (eget ark)	4
3.2.2	Krav til leverandør og kvalifikasjonskrav (eget ark)	4
3.2.3	Krav til programvare (eget ark)	4
3.2.4	Krav til infrastruktur, plattform og it-drift (eget ark)	5
3.2.5	Krav til skytjenester (eget ark)	5
3.3	Om feltene i Excel arket	5
3.3.1	Referanse til krav i Norm for informasjonssikkerhet.	5
3.3.2	Referanse til ISO 27001.	6
3.3.3	Referanse til ISO 27002.	7
3.3.4	Lovspeil.....	7

2. Veileder – hvordan bruke Normens krav i anskaffelser

Det er utviklet et dokument "Normens krav mappet mot krav i anskaffelser, krav i ISO 27001 og kontroller i ISO 27002". Dokumentet er utarbeidet i Excel og kan sees som en plukklister med krav som gir støtte i arbeidet med anskaffelser og etablering av internkontroll. Dokumentet inneholder en oversikt over krav i Normen som kan være aktuelle i forbindelse med anskaffelser. I tillegg inneholder dokumentet en oversikt over Normens krav mappet mot krav i NS-EN ISO/IEC 27001:2023, kontroller i NS-EN ISO/IEC 27002:2022 og lovspeil.

Denne veilederen gir en beskrivelse av Excel-arket sin oppbygging og kort veiledning i hvordan det kan brukes.

2.1 Bakgrunn

Arbeidet med utvikling av Excel arket har tatt utgangspunkt i vedlegget "Oversikt over Normens krav" som tidligere var tilgjengelig i Word versjon (dette dokumentet er nå sanert). Målet er å gjøre det lettere for virksomheten å bruke Normens krav i anskaffelser.

2.2 Om anskaffelsesprosessen

Påvirkningsmuligheten er 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.

2.2.1 Inndeling av ulike type krav

Krav som kan være nyttig å vurdere i forbindelse med anskaffelser har blitt merket med følgende type kategori:

- Forberedelser og avklaringer (som bør gjøres) før anskaffelser
- Krav til leverandør og kvalifikasjonskrav
- Krav til programvare
- Krav til infrastruktur, plattform og it-drift
- Krav til skytjenester

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



Veiledning til hvordan bruke Normens krav i anskaffelser

2.2.2 Hvordan beskrive krav som behov

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,

Alle disse behovselementene vil til sammen dekke behovet i anskaffelsen.

2.2.3 Bruk av 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 eller tjenesten som en skal anskaffe.

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

2.2.4 Kontrakt og kontraktsvilkår

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

2.2.5 Leverandøroppfølging

Kontrakten inneholder kundens krav og leverandørens svar og legger grunnlag for oppfølging av leverandør.

3. Om Excel-arket

Excel-arket "Normens krav mappet mot krav i anskaffelser, krav i ISO 27001 og kontroller i ISO 27002" kan lastes ned fra normen.no. Dokumentet inneholder en oversikt over krav i Normen som kan være aktuelle i forbindelse med anskaffelser. I tillegg inneholder dokumentet en oversikt over Normens krav mappet mot krav i NS-EN ISO/IEC 27001:2023, kontroller i NS-EN ISO/IEC 27002:2022 og lovspeil.

3.1 Om fanekortene (ark) i Excel arket

Vedlegget er utformet i Excel og inneholder 7 fanekort (ark).

1. Om Excel-arket
2. Alle Normens krav

Veiledning til hvordan bruke Normens krav i anskaffelser

3. Forberedelser og avklaringer før anskaffelser
4. Krav til leverandør og kvalifikasjonskrav
5. Krav til programvare
6. Krav til infrastruktur, plattform og it-drift
7. Krav til skytjenester

3.1.1 Om Excel arket

Her gis en kort oversikt over Excel-arket sin struktur og felter, bl.a. komplett oversikt over alle kravene og kontrollene i de nye standardene ISO 27001 og 27002.

3.1.2 Alle Normens krav

Her gis en komplett oversikt over alle normens krav mappet mot krav i anskaffelser, krav i ISO 27001, kontroller i ISO 27002 og lovspeil.

3.2 Benytt Excel arket for å finne relevante krav i forbindelse med anskaffelser

Excel-arket inneholder 5 fanter som angir krav i Normen som kan være relevante i forbindelse med anskaffelser. Dette kan sees på som "plukklister" som er ment å støtte virksomheten i å finne relevante krav i ulike faser i anskaffelsesprosessen og ulike type anskaffelser.

Norm for informasjonssikkerhet				ISO 27001		ISO 27002		Lovspeil
Krav.nr	Område/tema	Kapittel i Normen	Kravbeskrivelse	Plukklister	PDCA (Plan Do Check Act)	Hovdkapittel i ISO (High Level Structure, HLS)	Krav i NS-EN ISO/IEC 27001:2023	Type informasjonssikkerhetskontroller
				Krav i anskaffelser				Kontroller/tiltak i NS-EN ISO/IEC 27002:2022
								Hjemmel til kravet i lov eller forskrift

For hvert ark er satt på filter i henhold til metadataene angitt under slik det blir unike "plukklister" som kan benyttes som støtte i arbeidet.

Feltet inneholder følgende metadata:

Felt navn	Oversikt metadata
Krav ved anskaffelser	- Forberedelser og avklaringer før anskaffelser - Krav til leverandør og kvalifikasjonskrav - Krav til programvare - Krav til infrastruktur, plattform og it-drift - Krav til skytjenester

3.2.1 Forberedelser og avklaringer før anskaffelser (eget ark)

- Krav som er relevante når virksomheten planlegger og forbereder seg på å gjennomføre en anskaffelse.

3.2.2 Krav til leverandør og kvalifikasjonskrav (eget ark)

- Krav en stiller for å sikre at leverandøren er egnet til å gjennomføre kontraktsforpliktelsene i hele avtaleperioden. Dette kan være tekniske og faglige kvalifikasjoner. Det kan eksempelvis omfatte krav til teknologi, krav til kompetanse, krav til styringssystem, krav til hvordan databehandlere følges opp. Kravene kan fremmes som kvalifikasjonskrav og andre kan være en del av kravspesifikasjonen (bilag 1).

3.2.3 Krav til programvare (eget ark)

- Krav som kan være relevante i forbindelse med anskaffelse av programvare. Behov er utledet fra krav i normen, som krav til tilgangsstyring, innebygd personvern, logging, samhandling mellom virksomheter, digital kommunikasjon til den registrerte, den registrertes rett til

Veiledning til hvordan bruke Normens krav i anskaffelser

innsyn, retting og sletting. Etc. Kravene besvares som beskrivelse av funksjonalitet i programmer og databaser inkludert brukergrensesnitt og programmeringsgrensesnitt mellom programmer.

3.2.4 Krav til infrastruktur, plattform og it-drift (eget ark)

- Kravene er relevante ved anskaffelser av infrastruktur, plattform, it-drift (datasenter/it-plattform, applikasjonsdrift og/eller basistjenester). Også disse kravene vil omhandle krav til tilgangsstyring og logging for driftspersonell. Vil omfatte krav til administratorer, konfigurasjon, endringsstyring (sikker it-drift), styring av nettverkssikkerhet og elektronisk samhandling, styring av leverandørforhold og avtaler/databehandlere,

3.2.5 Krav til skytjenester (eget ark)

- Disse kravene er relevante ved anskaffelser sky-løsning og omfatter leverandørforhold og avtaler. Ved anskaffelser av skytjenester vil en del av kravene til programvare og it-drift være relevante.

3.3 Om feltene i Excel arket

Alle arkene har samme felt i toppen.

Norm for informasjonssikkerhet				Plukklister	ISO 27001			ISO 27002		Lovspeil
Krav.nr	Område/tema	Kapittel i Normen	Kravbeskrivelse	Krav i anskaffelser	PDCA (Plan Do Check Act)	Hovdkapittel i ISO (High Level Structure, HLS)	Krav i NS-EN ISO/IEC 27001:2023	Type informasjons-sikkerhets-kontroller	Kontroller/tiltak i NS-EN ISO/IEC 27002:2022	Hjemmel til kravet i lov eller forskrift

3.3.1 Referanse til krav i Norm for informasjonssikkerhet.

Norm for informasjonssikkerhet				Plukklister	ISO 27001			ISO 27002		Lovspeil
Krav.nr	Område/tema	Kapittel i Normen	Kravbeskrivelse	Krav i anskaffelser	PDCA (Plan Do Check Act)	Hovdkapittel i ISO (High Level Structure, HLS)	Krav i NS-EN ISO/IEC 27001:2023	Type informasjons-sikkerhets-kontroller	Kontroller/tiltak i NS-EN ISO/IEC 27002:2022	Hjemmel til kravet i lov eller forskrift

Feltene under Norm for informasjonssikkerhet inneholder følgende metadata:

Felt navn	Oversikt metadata
Krav.nr	Alle normens krav nummerert fra 1-294
Område/tema	A. Ledelse og ansvar B. Risikostyring C. Grunnleggende om behandling av helse- og personopplysninger D. Informasjonssikkerhet
Kapittel i Normen	Kapittel 1 - 5
Krav beskrivelse	Kravtabellen inneholder krav med "skal" i Normen slik at det på en enkel måte er mulig å verifisere om virksomheten følger Normen og hva som er absolutte krav i forbindelse med anskaffelser.

Veiledning til hvordan bruke Normens krav i anskaffelser

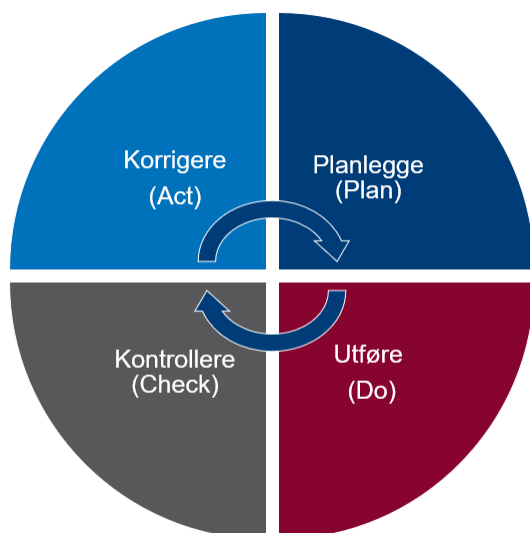
3.3.2 Referanse til ISO 27001.

Norm for informasjonssikkerhet				Plukklister	ISO 27001			ISO 27002	Lovspeil	
Krav.nr	Område/tema	Kapittel i Normen	Kravbeskrivelse	Krav i anskaffelser	PDCA (Plan Do Check Act)	Hovdkapittel i ISO (High Level Structure, HLS)	Krav i NS-EN ISO/IEC 27001:2023	Type informasjons-sikkerhets-kontroller	Kontroller/tiltak i NS-EN ISO/IEC 27002:2022	Hjemmel til kravet i lov eller forskrift

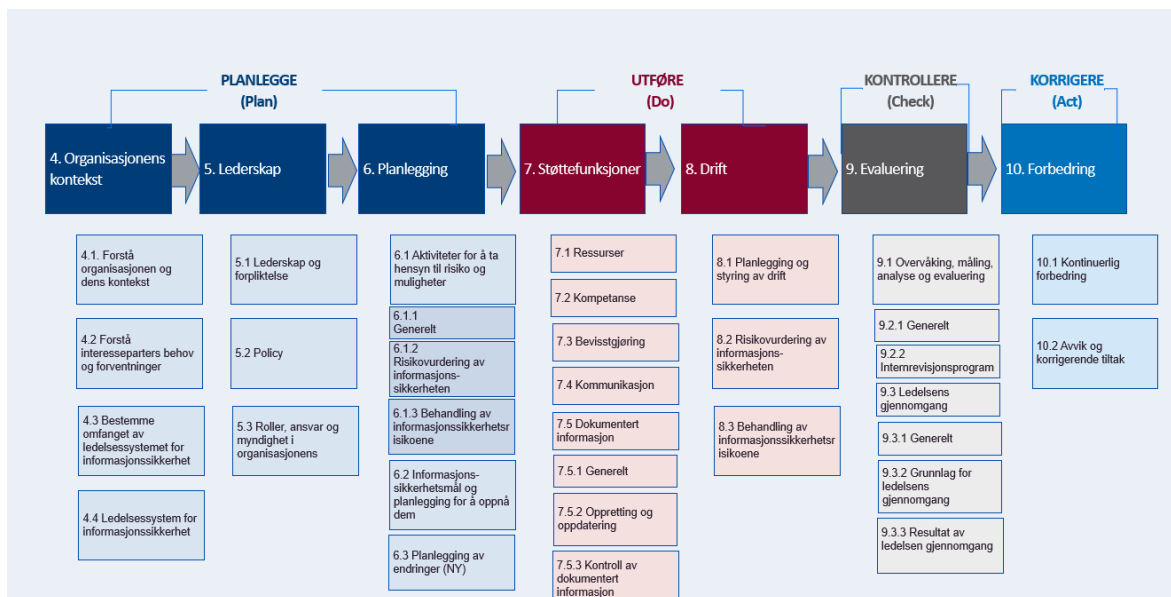
Feltene er strukturert iht. NS-EN ISO/IEC 27001:2023 (nyeste versjon) og inneholder informasjon strukturert i henhold til stadier i prosess for kontinuerlig forbedring (PDCA), standardens kapittelinndeling og konkrete krav.

Felt navn	Oversikt metadata
PDCA (Plan Do Check Act)	• Planlegge (Plan) • Utføre (Do) • Kontrollere (Check) • Korrigere (Act)
ISO (High Level Structure, HLS)	• 04. Organisasjonens kontekst • 05. Lederskap • 06. Planlegging • 07. Støtte • 08. Drift • 09. Evaluering av prestasjon • 10. Forbedring
Krav i NS-EN ISO/IEC 27001:2023	• Kapittel 04 – 10 i standarden for informasjonssikkerhet - ISO 27001

Stadier i prosess for kontinuerlig forbedring (PDCA)



ISO (High Level Structure, HLS) og kapittel i NS-EN ISO/IEC 27001:2023



3.3.3 Referanse til ISO 27002.

Norm for informasjonssikkerhet				Plukklister		ISO 27001		ISO 27002		Lovspeil
Krav.nr	Område/tema	Kapittel i Normen	Kravbeskrivelse	Krav i anskaffelser	PDCA (Plan Do Check Act)	Hovdkapittel i ISO (High Level Structure, HLS)	Krav i NS-EN ISO/IEC 27001:2023	Type informasjons-sikkerhets-kontroller	Kontroller/tiltak i NS-EN ISO/IEC 27002:2022	Hjemmel til kravet i lov eller forskrift

Den nye utgaven av ISO 27002 har 93 kontroller i 4 seksjoner (klausul 5-8)

Felt navn	Oversikt metadata
Type informasjons-sikkerhetskontroller	- Organisasjonskontroller - Personkontroller - Fysiske kontroller (adgangskontroll) - Teknologiske kontroller
Kontroller/tiltak i NS-EN ISO/IEC 27002:2022	Kontroller 5 - 8

3.3.4 Lovspeil

Norm for informasjonssikkerhet				Plukklister		ISO 27001		ISO 27002		Lovspeil
Krav.nr	Område/tema	Kapittel i Normen	Kravbeskrivelse	Krav i anskaffelser	PDCA (Plan Do Check Act)	Hovdkapittel i ISO (High Level Structure, HLS)	Krav i NS-EN ISO/IEC 27001:2023	Type informasjons-sikkerhets-kontroller	Kontroller/tiltak i NS-EN ISO/IEC 27002:2022	Hjemmel til kravet i lov eller forskrift

Følgende akronymer for hjemmel er benyttet i tabellen

Felt navn	Oversikt metadata
Lovspeil	EFF: Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
	FEP: Forskrift om etablering og gjennomføring av psykisk helsevern (§49) (https://lovdata.no/dokument/SF/forskrift/2011-12-16-1258)
	FIKT: Forskrift om IKT-standarder i helse- og omsorgstjenesten (https://lovdata.no/dokument/SF/forskrift/2015-07-01-853)

Veiledning til hvordan bruke Normens krav i anskaffelser

	• FLK: Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten (https://lovdata.no/dokument/SF/forskrift/2016-10-28-1250)
	• HFL: Helseforskningsloven (https://lovdata.no/dokument/NL/lov/2008-06-20-44)
	• HPL: Helsepersonelloven (https://lovdata.no/dokument/NL/lov/1999-07-02-64)
	• HTL: Helse- og omsorgstjenesteloven (https://lovdata.no/dokument/NL/lov/2011-06-24-30)
	• HTIL: Helsetilsynsloven (https://lovdata.no/dokument/NL/lov/2017-12-15-107)
	• PBL: Pasient- og brukerrettighetsloven (https://lovdata.no/dokument/NL/lov/1999-07-02-63)
	• PJF: Pasientjournalforskriften (https://lovdata.no/dokument/SF/forskrift/2019-03-01-168)
	• FMU: Forskrift om håndtering av medisinsk utstyr (https://lovdata.no/dokument/SF/forskrift/2013-11-29-1373?q=Forskrift%20om%20h%C3%A5ndtering%20av%20medisinsk)
	• PJL: Pasientjournalloven (https://lovdata.no/dokument/NL/lov/2014-06-20-42)
	• POL: Personopplysningsloven (https://lovdata.no/dokument/NL/lov/2018-06-15-38)
	• PVF: Personvernforordningen (GDPR) (https://lovdata.no/dokument/NL/lov/2018-06-15-38)