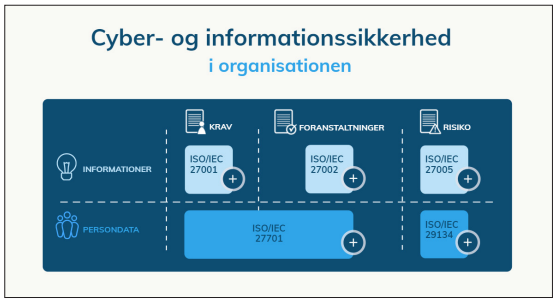
Cyber- og informationssikkerhed

September 2022

Indhold



DANSK STANDARD

Netværks- og systemsikkerhed for industri

(IEC 62443-series on Industrial communication networks – Network and system security)

Hvad er værdien af at anvende standarderne?

Med digitaliseringen af industrielle kontrolsystemer følger også cybersikkerhedstrusler, der kan have alvorlige konsekvenser for menneskeliv, miljø og økonomi, hvis der sker angreb eller fejl. Især de kontrolsystemer, der betegnes som kritisk infrastruktur, er særligt følsomme, og har stor værdi af standardserien IEC 62443.

Denne serie af standarder er udviklet for at sikre en overordnet tilgang til at håndtere cybersikkerhed for industrien. Hvor cybersikkerhed i ISO/IEC 27000-serien er struktureret omkring risikoanalyse og risikoledelse med fokus på databeskyttelse, så er det primære fokus i den industrielle sektor driftssikkerhed og tilgængelighed. Der arbejdes med forskellige niveauer af sikkerhed i et industrielt kontrolsystem. Overordnet er der defineret syv fundamentale krav til cybersikkerhed i industrielle kontrolsystemer:

a) **Adgangskontrol (AC), for beskyttelse mod uautoriseret adgang til systemet**
b) **Brugeradgang (UC), for beskyttelse mod uautoriseret anvendelse**
c) **Dataintegritet (DI) til beskyttelse mod uautoriseret ændring af data**
d) **Databeskyttelse (DC)**
e) **Begrænsning af datamængde (RDF) for beskyttelse mod udlevering af data til uautoriserede**
f) **Passende reaktionstid på IT-sikkerhedsbrud (TRE) med automatisk besked om kritiske situationer**
g) **Tilgængelighed af ressourcer (RA), så netværket ikke blokeres og fortsat drift kan opretholdes**

Standardserien introducerer metoder, begreber, systemer og værktøjer til at højne cybersikkerhed med et industrielt fokus. Standarderne opererer med et livscyklusperspektiv, der betyder, at alle processer og funktioner i et industrielt kontrolsystem adresseres. Standarderne indeholder designanbefalinger til, hvordan man opbygger og vedligeholder et kontrolsystem med fokus på cybersikkerhed; herunder risikoanalyse, håndtering af risici, overvågning og forbedring.

En klar værdi af IEC 62443-serien er, at den skaber et overblik over et industrielt kontrolsystems ansvarsområder og klarlægger rollefordelingen. På den baggrund fungerer standarderne som et effektivt kommunikationsredskab mellem alle relevante interessenter i et industrielt kontrolsystem.

Er standarderne relevante for dig?

IEC 62443-serien er relevant for industrien, herunder særligt procesindustrien, forsyningsanlæg (energisektoren), maskinanlæg mm. Standarderne er især relevante for de anlæg, der karakteriseres som kritisk infrastruktur.

Hvordan anvendes standarderne?

Standardserien kan anvendes som et samlet værktøj til systematisk at arbejde med cybersikkerhed i et industrielt kontrolsystem. Det er også muligt at udvælge enkelte standarder, og arbejde efter dem.

Grundlæggende krav for cybersikkerhed i forbrugerprodukter (IoT)

(ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements)

Hvad er værdien af at anvende standarden?

Den digitale udvikling betyder, at der er mulighed for at koble flere af de produkter, vi omgiver os med i dagligdagen, på internettet. De digitale assistenter vinder indpas, og smart TV, sundhedstrackere, robotstøvsugere mm. er blevet en del af vores hverdag. Men i takt med flere og flere forbrugerprodukter kobles på internettet, opstår der også nogle cybersikkerhedsmæssige udfordringer, som der er behov for at adressere.

Standarden ETSI EN 303 645 er udviklet med det overordnede formål at beskytte forbrugerne, når de anvender IoT (Internet of Things) produkter. Standarden hjælper producenterne af IoT forbrugerprodukter med at identificere og adressere henholdsvis cybersikkerhedsudfordringer og udfordringer, der relaterer sig til privatlivsbeskyttelse og håndtering af persondata.

Producenter af IoT forbrugerprodukter kan anvende standardens konkrete tjeklister som et redskab til at sikre, at et givent produkt lever op til et grundlæggende sikkerhedsniveau. Standarden indeholder bl.a. en guide til håndtering af passwords, softwareopdatering, anvendelse af kryptografi i kommunikationen, minimering af muligheder for angreb mm. Derudover indeholder standarden et kort afsnit med bestemmelser ift. databeskyttelse af IoT forbrugerprodukter. Her refereres der primært til Persondataforordningen (GDPR).

Standarden angiver ikke, hvilke løsninger producenterne skal anvende for at sikre deres produkter, men skaber rum for at man selv kan implementere de sikkerhedsløsninger, der passer til ens produkt. Standarden fremhæver således "Security by design" som et vigtigt princip, når der udvikles IoT forbrugerprodukter.

Er standarden relevant for dig?

Standarden er relevant for producenter af forbrugerprodukter, der kan kobles til internettet. Standarden kan dog også anvendes som inspiration for andre, der arbejder med cybersikkerhed og IoT generelt.

Hvordan anvendes standarden?

Standarden kan anvendes som en tjekliste af producenterne til at sikre produkternes cyber- og informationssikkerhed. Standarden indeholder blandt andet et skema, som producenter kan anvende til en praktisk gennemgang af deres produkter.

Derudover er hver af standardens temaer suppleret med konkrete eksempler, som gør det lettere for producenter at relatere standarden til deres praktiske arbejde med at sikre deres produkter. Det forventes, at standarden kommer til at danne grundlag for det fremtidige arbejde med en certificeringsordning i regi af EU's Cybersecurity Act.

Krav til et ledelsessystem for informationssikkerhed

(ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements)

Hvad er værdien af at anvende standarden?

Den internationale ledelsesstandard for informationssikkerhed, ISO/IEC 27001, hjælper organisationer med at strukturere arbejdet med forretningskritiske informationer og bidrager til at minimere risikoen for brud på informationssikkerheden, som kan true organisationens eksistensgrundlag.

Derudover kan standarden anvendes til at dokumentere organisationens arbejde med beskyttelse af følsomme oplysninger – internt såvel som eksternt.

Standarden er et styringsværktøj, der hjælper organisationer med at beskytte værdifulde informationer – på en sikker og troværdig måde. Standarden opstiller blandt andet krav til risikostyring, dokumentation af processer samt fordeling af roller og ansvar for informationssikkerhed. Formålet med ISO/IEC 27001 er at opnå effektiv informationssikkerhedsledelse, der passer til organisationens særlige behov og herefter opretholde effektiviteten ved at sikre løbende forbedringer. Det betyder, at informationssikkerheden hele tiden opdateres, så organisationen er i stand til at håndtere udfordringerne i en verden under konstant forandring.

Standarden er desuden et godt afsæt til at håndtere kravene i Persondataforordningen (GDPR) ISO/IEC 27001 er internationalt anerkendt og bliver brugt i hele verden. Standarden bidrager til at skabe tillid til de organisationer, der anvender den, da det vidner om, at man arbejder struktureret med informationssikkerhed og kan fremvise dokumentation for arbejdet.

Er standarden relevant for dig?

Standarden er relevant for alle, der ligger inde med informationer, som ved kompromittering kan få betydelige konsekvenser for både overholdelse af lovgivning, organisationens aktiviteter, succes samt troværdighed og image.

Statslige myndigheder er underlagt et krav om at implementere og arbejde systematisk efter ISO/IEC 27001, mens den øvrige del af den offentlige sektor er underlagt et krav om at følge principperne i standarden.

Hvordan anvendes standarden?

Standarden er en kravstandard til et ledelsessystem for informationssikkerhed. Har man i forvejen implementeret et ledelsessystem, som eksempelvis ISO 9001 for kvalitetsledelse, kan man drage fordel af, at man allerede kender opbygningen og ved hvordan man arbejder efter en ledelsesstandard. Der er en række tilhørende standarder inden for ISO/IEC 27000-serien, heriblandt de

vejledende standarder ISO/IEC 27002 og ISO/IEC 27005, som kan hjælpe med, hvordan man skal gribe udfærdigelsen af ledelsessystemet for informationssikkerhed an.

Det er desuden muligt at blive certificeret i ISO/IEC 27001. En certificering øger organisationens troværdighed og signalerer en seriøs tilgang til informationssikkerhed. En certificering kan også være med til at give en konkurrencefordel, da organisationen synliggør overfor potentielle kunder, at informationssikkerhed tages alvorligt.

Læs mere om certificering her.

Foranstaltninger til styring af informationssikkerhed

(ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls)

Hvad er værdien af at anvende standarden?

ISO/IEC 27002 er en vejledende standard, som knytter sig til den internationale ledelsesstandard for informationssikkerhed, ISO/IEC 27001. Formålet med standarden er, at organisationer kan anvende den til at udvælge de foranstaltninger, der er rigtige for organisationen, til at implementere et ledelsessystem for informationssikkerhed (ISMS) baseret på ISO/IEC 27001.

ISO/IEC 27002 indeholder 93 foranstaltninger, som omfatter anbefalinger til politikker, processer, procedurer, organisationsstrukturer samt software- og hardwarefunktioner. Standarden er bygget op over en struktur, der inddeler foranstaltningerne i fire temaer; organisatoriske, teknologiske, fysiske og adfærdsmæssige foranstaltninger. En organisation udvælger på basis af risikoprofilen de foranstaltninger, der er relevante for dem at implementere. De 93 foranstaltninger knytter sig til kontrolmålene i anneks A i ISO/IEC 27001. På den måde kan standarden anvendes som en tjekliste til at implementere ISO/IEC 27001. (ISO/IEC 27001 er i gang med en opdatering, hvor anneks A tilrettes så det afspejler foranstaltningerne i ISO/IEC 27002. Den opdaterede version af ISO/IEC 27001 forventes at udkomme i slutningen af 2023).

Er standarden relevant for dig?

Hvis din organisation har brug for en systematisk tilgang til at beskytte informationer, bør du overveje at kigge nærmere på ISO/IEC 27002.

ISO/IEC 27002 er relevant for alle, der gerne vil implementere den internationale ledelsesstandard for informationssikkerhed, ISO/IEC 27001, og har brug for vejledning til, hvordan man udvælger de korrekte foranstaltninger til at implementere et ledelsessystem for informationssikkerhed. Standarden kan samtidigt bruges som generel inspiration til, hvilke foranstaltninger man bør overveje at implementere, hvis man ønsker at forbedre sin organisations niveau af informationssikkerhed. Standarden henvender sig til alle typer og størrelser af organisationer, private såvel som offentlige.

Hvordan anvendes standarden?

ISO/IEC 27002 kan benyttes som inspirationskilde til at udpege og etablere de for organisationen relevante foranstaltninger. Standarden kan med fordel anvendes som værktøjskasse til risikohåndtering sammen med kravstandarden ISO/IEC 27001, og den vejledende standard for risikostyring ISO/IEC 27005.

Vejledning i risikostyring for informationssikkerhed

(ISO/IEC 27005 Information technology – Security techniques – Information security risk management)

Hvad er værdien af at anvende standarden?

ISO/IEC 27005 er en vejledende standard, som knytter sig til den internationale ledelsesstandard for informationssikkerhed, ISO/IEC 27001.

Mens ISO/IEC 27001 stiller de overordnede krav til et ledelsessystem for informationssikkerhed (ISMS), kan ISO/IEC 27005 hjælpe med at vejlede i, hvordan man kan lave en risikovurdering, og dermed få et overblik over organisationens trusler, sårbarheder og hvordan risici kan håndteres ud fra organisationens risikovillighed. Standarden kan dermed være med til at sikre det optimale niveau af foranstaltninger i en organisation ift. værdien af den information, som skal beskyttes.

Standarden er en vejledning i risikostyring og giver indsigt i, hvordan man vurderer og håndterer risici vedrørende organisationens informationer ud fra en vurdering af sandsynligheden for, at en hændelse sker sammenstillet med den konsekvens, som hændelsen har for organisationen. Risikohåndtering kræver en stillingtagen til, hvordan organisationen skal agere overfor de identificerede risici.

Er standarden relevant for dig?

ISO/IEC 27005 er relevant for alle, der gerne vil implementere den internationale ledelsesstandard for informationssikkerhed, ISO/IEC 27001, og har brug for vejledning til, hvordan man laver en risikovurdering, så man kan etablere de rette foranstaltninger til at implementere et ISMS. Standarden kan desuden bruges som generel inspiration til, hvordan man vurderer risici ift. informationer knyttet til ens organisation.

Hvordan anvendes standarden?

Standarden er en vejledning i vurdering og håndtering af risici inden for rammerne af et ledelsessystem i informationssikkerhed. Der er en række tilhørende standarder, heriblandt kravstandarden ISO/IEC 27001 og den vejledende standard ISO/IEC 27002, som handler om etablering af foranstaltninger. Begge disse standarder kan med fordel anvendes sammen med ISO/IEC 27005.

Der er en opdateret version af ISO/IEC 27005 på vej, som forventes at blive publiceret i slutningen af 2022. I forbindelse med opdateringen af standarden, vil den også blive oversat til dansk. Den danske version forventes at være klar i løbet af 2023.

Udvidede krav og vejledninger for 27001 og 27002 til at omfatte persondatabeskyttelse

(ISO/IEC 27701 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines)

Hvad er værdien af at anvende standarden?

Organisationer, der behandler personoplysninger, oplever i dag en række udvidede krav til at sikre privatlivet for kunder, brugere, borgere, medarbejdere m.fl. Det skyldes ikke mindst Persondataforordningens (GDPR's) ikrafttræden. ISO/IEC 27701 er udarbejdet ud fra et behov om at adressere privatlivsbeskyttelse inden for rammerne af et ledelsessystem for informationssikkerhed. Standarden indeholder både krav og vejledning til etablering, implementering, vedligeholdelse og løbende forbedring af et sådant ledelsessystem.

ISO/IEC 27701 giver organisationer konkrete anvisninger til at integrere og forene arbejdet med persondatabeskyttelse med arbejdet for informationssikkerhed. Standarden kan hjælpe organisationer med at strukturere deres arbejde med personoplysninger og minimere risikoen for brud på privatlivsbeskyttelsen. Compliance er en udtalt udfordring blandt mange virksomheder og organisationer, og standarden ISO/IEC 27701 er her et nyttigt værktøj til netop at dokumentere, internt såvel som eksternt, hvordan organisationen sikrer privatlivsbeskyttelse i henhold til lov eller kundekrav. Som organisation kan det være komplekst at gennemskue, hvordan man får mappet disse krav og retningslinjer ift. organisationens håndtering af persondata. Her er standarden et værdifuldt redskab, blandt andet i kraft af et anneks, som er en direkte mapping af standardens krav og vejledning op imod Persondataforordningens (GDPR's) artikler. Det er dog vigtigt at understrege, at der ikke en 1:1 compliance med GDPR, hvis man følger standarden. Det er nødvendigt, at en organisation orienterer sig ift. øvrig lovgivning og yderligere retningslinjer.

Standarden bidrager også til en klar fordeling af roller og ansvarsområder, og er således et værdifuldt værktøj for både dataansvarlige og for databehandlere. For de dataansvarlige kan standarden især bidrage til at skabe gennemsigtighed og fungere som et redskab til at styre databehandlingsprocesserne. For databehandlerne kan standarden særligt bidrage til at dokumentere overfor kunder, borgere m.fl., at deres personoplysninger er håndteret korrekt. Samtidig kan standarden bidrage til at styrke kommunikationen mellem jurister og teknikere via en fælles referenceramme for informationssikkerhed og privatlivsbeskyttelse.

Sidst, men ikke mindst, er standarden med til at opbygge tillid. Standarden er internationalt anerkendt og spås at finde bred anvendelse globalt. Det bidrager til skabe tillid til de organisationer, der anvender standarden, da det vidner om, at man arbejder struktureret med persondatabeskyttelse og kan fremvise dokumentation for arbejdet.

Er standarden relevant for dig?

Hvis din organisation behandler personoplysninger, og I ønsker en struktureret tilgang til at integrere informationssikkerhed og persondatabeskyttelse, så vil standarden være værdifuld at orientere sig i. Standarden er især interessant for databehandlere og dataansvarlige, da den bidrager med vejledning i passende foranstaltninger for deres respektive roller. Standarden er relevant for alle typer og størrelser af organisationer.

Hvordan anvendes standarden?

For de organisationer, der allerede har opbygget og implementeret et ledelsessystem for informationssikkerhed, er ISO/IEC 27701 en udvidelse til også at omfatte persondatabeskyttelse. For organisationer, der ikke arbejder med ISO/IEC 27001 og ISO/IEC 27002, kan standarden give inspiration til overholdelse af de grundlæggende privacy-principper og til effektiv håndtering af personoplysninger i en organisation.

ISO/IEC 27701 er ligesom ISO/IEC 27001 en kravstandard bygget op omkring et ledelsessystem, hvilket betyder, at det er muligt for en organisation at blive certificeret i standarden. Certificering i ISO/IEC 27701 forudsætter dog tidligere eller samtidig certificering i ISO/IEC 27001.

Konsekvensanalyse vedrørende databeskyttelse

(ISO/IEC 29134 Information technology – Security techniques – Guidelines for privacy impact assessment (PIA))

Hvad er værdien af at anvende standarden?

ISO/IEC 29134 vejleder organisationer i at vurdere og håndtere potentielle risici vedrørende persondata som følge af et nyt system eller service, der behandler personoplysninger. Standarden giver vejledning i at gennemføre en privatlivsimplikationsanalyse (PIA), som i daglig tale også kaldes konsekvensanalyse vedrørende databeskyttelse. Standarden indeholder også et konkret forslag til, hvordan man strukturelt og indholdsmæssigt kan sammensætte virksomhedens PIA-rapport.

Fordelene ved at gennemføre en konsekvensanalyse er mange. Først og fremmest er alle organisationer pålagt at overveje behovet for en konsekvensanalyse i henhold til Persondataforordningen (GDPR), hvis der er ny eller ændret behandling af personoplysninger. Organisationer kan også frivilligt vælge at gennemføre en konsekvensanalyse.

Generelle fordele:

- **Identificering af privacy-konsekvenser, risiko og ansvar**
- **Evaluering af nye informationssystemers privacy-relaterede risici samt vurdering af sandsynlighed og konsekvens**
- **Deling og afbødning af privacy-risici med interessenter og bevis for overholdelse (compliance).**

Er standarden relevant for dig?

ISO/IEC 29134 er relevant for alle organisationer, der behandler personoplysninger. Standarden er målrettet personer, der har ansvar for eller drifter systemer eller services, der behandler personoplysninger. Standarden er således relevant for ledere, medarbejdere, og databeskyttelsesrådgivere (DPO) med ansvar for at tilse eller udføre opgaver i forbindelse med konsekvensanalyser eller behandlingssikkerhed efter Persondataforordningen (GDPR).

Standarden kan anvendes af både offentlige myndigheder og private virksomheder, og den er relevant for alle typer og størrelser af organisationer.

Hvordan anvendes standarden?

Standarden er et konkret værktøj til at arbejde systematisk og kontinuerligt med konsekvensanalyse vedrørende databeskyttelse. Standarden kan tilpasses virksomhedens kontekst, og dermed kan omfanget af konsekvensanalysen justeres, så den modsvarer virksomhedens behandling af personoplysninger, samt hvor følsomme disse er. Mange anvender standarden, fordi den er nævnt

i Justitsministeriets betænkning nr. 1565, bind 1 vedr. Persondataforordningen (GDPR), da man dermed kan øge sandsynligheden for at afdække væsentlige risici og elementer i databehandling. Standarden tager læseren i hånden og beskriver, hvordan en virksomhed forbereder, planlægger, gennemfører og evaluerer en konsekvensanalyse. Herefter følger vejledning i, hvordan PIA-rapporten opstilles med planer og procedurer, risikovurdering, risikohåndteringsplaner og slutteligt en konklusion. Standarden indeholder desuden et eksempel på et workflowdiagram for behandling af personoplysninger og et eksempel på en prioriteret kortlægning af identificerede privacy-risici.

Hvordan kommer jeg videre med arbejdet?

De fleste organisationer vil kunne finde nyttig inspiration og vejledning i standarderne, som kan forbedre deres cyber- og informationssikkerhed, også uden at følge standarderne fra ende til anden. Alle standarderne kan købes i Dansk Standards webshop. Dansk Standard tilbyder desuden kurser og rådgivning i de fleste af de beskrevne standarder.

Behov for hjælp til de mange begreber?

Den engelsksprogede version af terminologistandarden ISO/IEC 27000 kan downloades gratis via dette link på ISO's hjemmeside. I denne standard kan du blive klogere på terminologien og definitionerne, der ligger til grund for ISO/IEC 27000-seriens ledelsessystem for informationssikkerhed. Hvis du ønsker standarden med danske oversættelser, kan den købes i vores webshop, hvor du selvfølgelig også finder de øvrige beskrevne standarder.

Mere om certificering

Certificering kræver en ekstern auditering, hvor organisationens efterlevelse af standardens krav gennemgås i dokumentationsform og med et fysisk besøg. Dansk Standard certificerer ikke, men bidrager gerne med rådgivning og viden om certificering.

Dansk, europæisk eller international standard?

De internationale standarder (ISO/IEC), er alle udgivet som danske standarder, der er fuldstændig identiske med de internationale. De har på Dansk Standards webshop derfor betegnelsen "DS ISO/IEC" foran nummeret på standarden. Flere af standarderne er oversat til dansk – hvilke fremgår af webshoppen. Nogle af standarderne er ligeledes identisk implementeret på europæisk niveau, og har derfor også tilføjet "EN" i titlen; DS EN ISO/IEC. Den europæiske implementering betyder, at ingen EU-lande må have nationale standarder, der er overlappende eller i modstrid med de internationale standarder.

Hvis du har spørgsmål, er du altid velkommen til at kontakte vores informationscenter.

Dansk Standard har et udvalg for cyber- og informationssikkerhed, hvor medlemmerne får indsigt i kommende standarder og mulighed for at påvirke det internationale standardiseringsarbejde. Du kan læse mere om udvalget her.