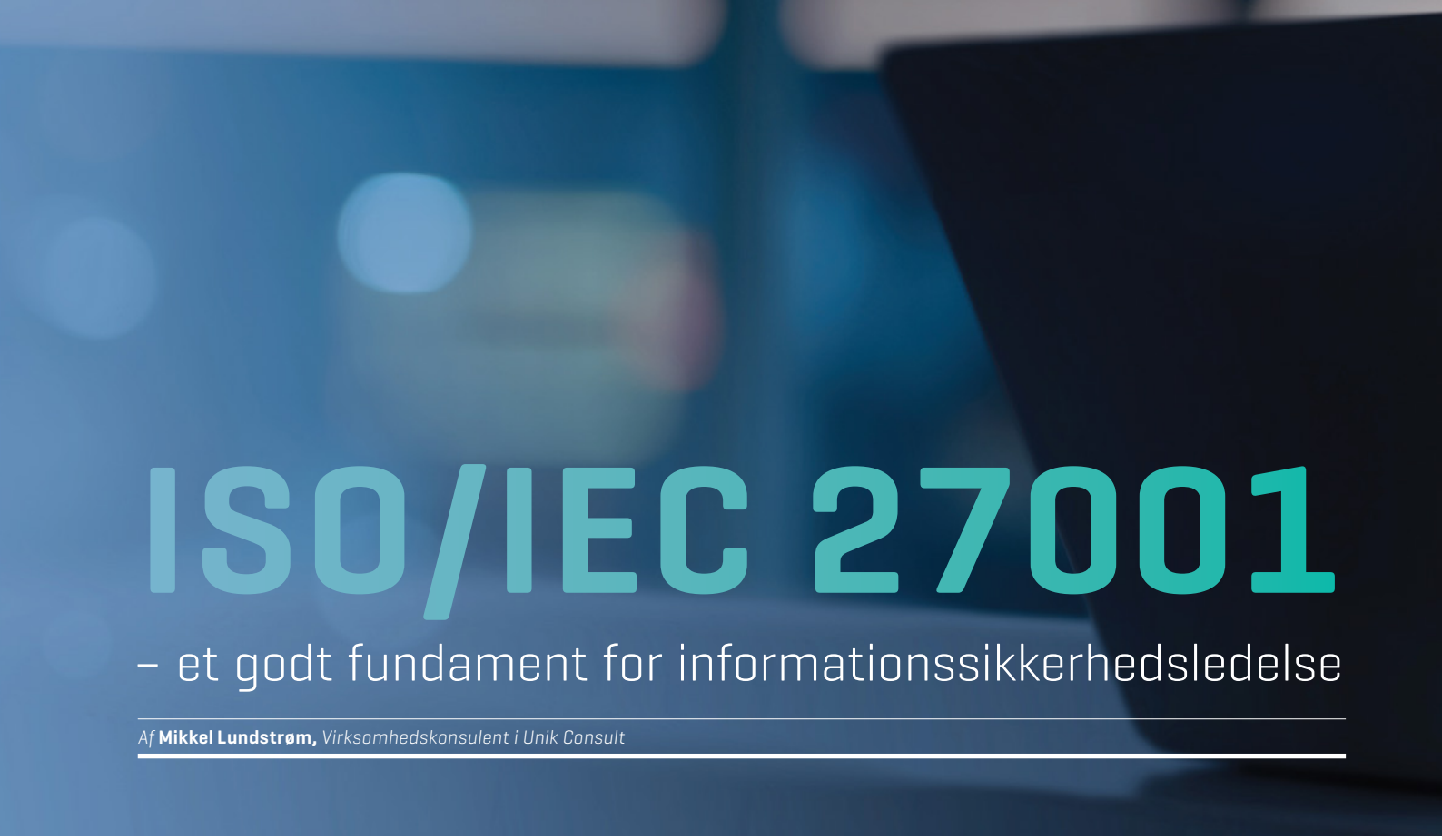

ISO/IEC 27001

– et godt fundament for informationssikkerhedsledelse

Af **Mikkel Lundstrøm,** *Virksomhedskonsulent i Unik Consult*

TRUSLER MOD INFORMATIONSSIKKERHED

Vi lever i dag en verden, hvor informationssikkerhed fylder stadig mere for virksomheder, offentlige myndigheder og borgere.

Først blev det kaldt EDB. Siden blev det til IT. Nu snakker vi om informationer og digitale services som understøtter vores liv med informationshåndtering på utallige områder inden for produktion, handel, administration, undervisning, kommunikation etc.

På den ene side er digitaliseringen et stort fremskridt. På den anden side indebærer digitaliseringen at de enorme mængder af data risikerer at blive misbrugt af kriminelle personer og fjendtlige magter til aktiviteter, som skader borgere, virksomheder og offentlige myndigheder. Udfordringerne bliver ikke mindre i en verden, hvor hele jordkloden er bundet sammen i et omfattende digitalt netværk, hvor data flyder rundt mere eller mindre beskyttet.

Trusselsbilledet for informationssikkerhed er meget omfattende og udvikler sig hele tiden inden for de forskellige samfundsområder. Som eksempler kan fx nævnes trusler i forhold til misbrug af persondata, nedbrud af samfundskritisk infrastruktur, misbrug af kunstig intelligens, hvidvask af ulovlige midler etc. Trusselsbilledet giver anledning til at overveje, hvordan sikkerheden omkring anvendelsen af digitale services kan styrkes.

Det er kun fantasien som sætter grænser for hvordan kriminelle, terrorister og fjendtlige stater vil udnytte deres magt til at udføre destruktive handlinger, som kan skade borgere, virksomheder og offentlige myndigheder – også når det handler om informations- og cybersikkerhed.

Trusselsbilledet i forhold til informations- og cybersikkerhed ser ud til at vokse i variation og omfang. Der er derfor en særlig grund til at have stor opmærksomheden rettet mod hvordan risici på området kan håndteres.

KOM GODT I GANG MED ISO/IEC 27001 – HELT ENKELT

Virksomheder, som ønsker at efterleve krav til informationssikkerhed, cybersikkerhed og beskyttelse af persondata, kan med fordel basere indsatsen på implementering af ISO/IEC 27001.
Det anbefales at starte helt enkelt med at få fundamentet for ledelsessystemet på plads. Efterfølgende kan ledelsessystemet udbygges.

Omdrejningspunktet for standarden er etablering af ledelsessystem for informationssikkerhed der sikrer fortrolighed, integritet og tilgængelighed af informationer ud fra en risikobaseret tilgang.

På engelsk oversat til *CIA* (ikke at forveksle med efterretningstjenesten med samme forkortelse), hvor C står for *Confidence* (Fortrolighed), I for *Integrity* (Integritet) og A for *Availability* (Tilgængelighed).

ISO/IEC 27001 er – på samme vis som de øvrige ledelsesstandarder – opbygget efter principperne for High Level Structure i overensstemmelse med følgende hovedpunkter: Kontekst af organisationen, Lederskab, Planlægning, Support, Drift, Præstationsevaluering og Forbedringer

Vurdering og håndtering af risici er et vigtigt omdrejningspunkt i forbindelse med informationssikkerhed. Uønskede effekter af risici skal forebygges eller reduceres.

Med hensyn til risikovurdering skal virksomheden bl.a. fastlægge kriterier for accept af risici, sikre en konsistent proces for gennemførelse af risikovurderinger, afdække sandsynlighed og konsekvenser af risici, samt evaluere informationssikkerhedsrisici i forhold til de opstillede acceptkriterier.

OBS!
SE SEMINAR OM EMNET PÅ NÆSTE SIDE!

Med hensyn til *risikohåndtering* skal virksomheden gennemføre en proces, der tager hånd om risici på baggrund af risikovurderingen, samt udarbejde en *Statement of Applicability* (*SoA*), som indeholder en samlet oversigt over alle nødvendige kontroller (herunder også supplerende kontroller til Annex A), samt begrundelse for kontroller, som er medtaget eller udeladt, en plan for risikohåndtering, samt risikoejernes godkendelse af risikohåndteringsplanen, og deres accept af residualrisikoen.

ISO/IEC 27001 indeholder i *Annex A* en liste med 93 kontroller, som kan bringes i spil i forhold til at forebygge eller reducere risici.

Kontrollerne er opdelt i 4 grupper:

- Organisatoriske kontroller (i alt 37 kontroller)
- Menneske kontroller (i alt 8 kontroller)
- Fysiske kontroller (i alt 14 kontroller)
- Teknologiske kontroller (i alt 34 kontroller)

De 93 kontroller i Annex A er beskrevet i uddybet form i *ISO/IEC 27002* med angivelse af formål med kontrollen, vejledning til implementering af kontrollen og andre relevante informationer. Risikoanalysen og risikohåndteringen kan resultere i at der skal inddrages andre kontroller end de som fremgår af Annex A. Disse kontroller skal derfor også anføres.

SOA'en (Statement of Applicability) indeholder en oversigt over alle de kontroller som er vurderet som nødvendige i forhold til håndtering af de risici, som har betydning for virksomheden. SOA'en med versionsnummer fremgår af certifikatet sammen med virksomhedens scope og de adresser som certifikatet gælder for.

ISO 27001 SOM RAMMEVÆRKTØJ FOR HÅNDTERING AF LEGALE KRAV

Når det handler om informationssikkerhed spiller legale krav en stor rolle. Her er ISO 27001 et godt rammeværktøj til at inkludere legale krav, som måtte være relevante for virksomheden.

Som eksempler på legale krav med relevans for informations- og cybersikkerhed kan bl.a. nævnes:

- **GDPR** (**General Data Protection Regulation**)
  – GDPR er en EU-forordning fra 2016, som på dansk er kendt som databeskyttelsesforordningen. GDPR er EU-reglerne for databeskyttelse og gælder når offentlige og private virksomheder behandler oplysninger om personer (personoplysninger).
  – Overholdelse af GDPR-kravene spiller en stor rolle for rigtig mange virksomheder. Størst betydning er i forbindelse med håndtering af følsomme personoplysninger inden for kategorierne race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske eller biometriske data, helbredsoplysninger, samt oplysninger om seksuelle forhold eller seksuelle orientering

- **NIS2** (**Net- og Informationssikkerhedsdirektivet, vers. 2**)
  – NIS2 er et EU-direktivet fra 2022 som fastlægger foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU. EU-direktivet træder via dansk lovgivning i krav d. 1. juli 2025. NIS2 skal styrke cybersikkerheden for virksomheder – både private og offentlige – inden for en række sektorer. som anses for at være kritiske for den samfundsmæssige forsyningssikkerhed.
  – NIS2 vil fra 1. juli 2025 'ramme' større virksomheder inden for

MIKKEL LUNDSTRØM
Virksomhedskonsulent i Unik Consult.
Læs mere på *www.unikconsult.dk*

Som konsulent løser Mikkel auditopgaver for MONTHE Certificering ApS med særlig fokus på ISO 27001 certificering Læs mere på *www.monthe-c.dk*
MONTHE-C's kunder på informationssikkerhedsområdet kommer fra bl.a. software-branchen, produktionsbranchen, entreprenør-branchen og advokat-branchen.

MONTHE-C samarbejder med C1 Certification AB, som er akkrediteret af Swedac til at udstede certifikater. Læs mere på *www.c1cert.se*
MONTHE-C samarbejder med auditorer fra C1, hvis der er behov for at tilføre flere person-ressourcer til håndtering af den enkelte auditopgave.

kritiske sektorer, som blandt andet omfatter sektorer som energi, transport, sundhed og finans m.fl. Et nedbrud eller et angreb kan have alvorlige konsekvenser for samfundet. Virksomheder kan indirekte blive omfattet af NIS2 ved at være underleverandører til NIS2-omfattede virksomheder.

- **DORA (Digital Operational Resilience Act)**
  – DORA er baseret på en EU-forordning fra 2022 med det formål at sætte finansielle virksomheder og IKT-tjenesteudbydere i stand til at modstå, reagere og reetablere sig fra påvirkningen af IKT-sikkerhedshændelse. (IKT Informations- og kommunikationsteknologi)
  – DORA finder i praksis anvendelse for alle finansielle virksomheder, herunder kreditinstitutter, betalingsinstitutter, investeringsselskaber, forsikringsselskaber, pensionskasser, værdipapircentraler, administrationsselskaber, udbydere af dataindberetningstjenester, kreditvurderingsbureauer, IT-leverandører m.fl.

- **Hvidvask**
  – Den nyeste version af 'hvidvaskloven' er fra 2024 og har fokus på forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme. Hvidvask sker, når man får eller forsøger at få et ulovligt udbytte fra en kriminel handling til at se ud som om, det er erhvervet på lovlig vis.
  – National enhed for Særlig Kriminalitet (NSK) har aktuelt rejst tiltale mod Nordea for en række omfattende brud på hvidvaskloven. Anklagen lyder på at mistænkelige transaktioner for 26 milliarder kroner er strømmet gennem banken. For et par år siden var Danske Bank gennem en tilsvarende proces. Finansielle virksomheder og advokatvirksomheder er i særlig grad berørt af hvidvask.

- **Kunstig intelligens**
  – EU-forordningen om kunstig intelligens blev vedtaget i 2023. Forord-

ningen har til formål at beskytte de grundlæggende rettigheder, demokratiet, retsstatsprincippet og den miljømæssige bæredygtighed mod negative påvirkninger fra kunstig intelligens, samtidig med at den skal styrke innovationen og bringe EU i førersædet inden for kunstig intelligens eller AI (Artificial Intelligence).
  – Anvendelsen af kunstig intelligens er de seneste år vokset hastigt på globalt plan. Teknologien kan komme borgere og virksomheder til gavn, hvis kunstig intelligens anvendes på en ansvarlig og sikker måde. Imidlertid er der også betydelige risici forbundet med kunstig intelligens i forhold til datasikkerhed. Borgere, virksomheder og myndigheder er alle eksponeret for risici i forhold fx troværdigheden af information frembragt med kunstig intelligens uanset om informationen er mundtligt, skriftligt eller i form af billeder (foto/video).

Fordele ved ISO 27001-certificering
ISO 27001- certificering kan indebære mange fordele for en virksomhed, herunder

- **Forbedret informationssikkerhed**
  – ISO 27001-certificeringen sikrer, at virksomheden har et robust informationssikkerhedsledelsessystem (ISMS) med fokus på behandling af data i forhold til fortrolighed, integritet og tilgængelighed. Ved at implementere ISO 27001-standardens krav er virksomheden bedre rustet til at forsvare sig mod cyberangreb, hacking og andre sikkerhedstrusler.

- **Risikoledelse og kontinuerlig forbedring**
  – ISO 27001-certificering kræver en systematisk tilgang til risikovurdering og risikostyring. Dette hjælper virksomheden med at identificere potentielle trusler og sårbarheder og implementere passende kontroller for at mindske risici. Certificeringen fremmer også en kultur af kontinuerlig forbedring gennem regelmæssige audits og opdateringer af sikkerhedsforanstaltningerne.

- **Øget tillid og troværdighed**
  – En ISO 27001-certificering demonstrerer virksomhedens engagement i informationssikkerhed overfor kunder, partnere og andre interessenter. Dette øger tilliden til virksomheden og kan være et afgørende salgsargument, især når man handler med sikkerhedsbevidste kunder.

- **Konkurrencefordel**
  – ISO 27001-certificeringen kan differentiere virksomheden fra konkurrenterne. Mange virksomheder og offentlige institutioner kræver, at deres leverandører og partnere er ISO 27001-certificerede, hvilket kan åbne døre til nye markeder og forretningsmuligheder.

INFO OM 27000-SERIEN AF STANDARDER FOR INFORMATIONSSIKKERHED

ISO 27001-serien om informationssikkerhed er meget omfattende. I Danmark står Dansk Standard for oversættelse og publicering af bl.a. følgende standarder vedr. informationssikkerhed:

- DS/EN ISO/IEC 27000:2020 Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Oversigt og anvendt terminologi
- DS/EN ISO/IEC 27001:2023 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Ledelsessystemer for informationssikkerhed – Krav
- DS/EN ISO/IEC 27002:2022 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Foranstaltninger til informationssikkerhed
- DS/ISO/IEC 27003:2017 Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Vejledning
- DS/ISO/IEC 27004:2016 Informationsteknologi – Sikkerhedsteknikker – Informationssikkerhedsledelse – Monitorering, måling, analyse og evaluering
- DS/EN ISO/IEC 27005:2024 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Vejledning i styring af informationssikkerhedsrisici
- DS/EN ISO/IEC 27006:2020 Informationsteknologi – Sikkerhedsteknikker – Krav til organer, der foretager audit og certificering af ledelsessystemer for informationssikkerhed
- ISO/IEC 27006:2024 specificerer krav og giver vejledning til organer, der udfører revision og certificering af et informationssikkerhedsstyringssystem (ISMS)
- DS/EN ISO 27007:2022 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Vejledning i auditering af ledelsessystemer for informationssikkerhed
- DS/EN ISO/IEC 27017:2021 Informationsteknologi – Sikkerhedsteknikker – Regelsæt for styring af informationssikkerhed baseret på ISO/IEC 27002 for cloudtjenester
- DS/ISO/IEC 27021:2017 Informationsteknologi – Sikkerhedsteknikker – Kompetencekrav til fagligt personale vedrørende ledelsessystemer for informationssikkerhed
- DS/ISO/IEC 27031:2025 Informationsteknologi – Cybersikkerhed – IKT-parathed til business continuity
- DS/ISO/IEC 27035-1:2023 Informationsteknologi – Styring af informationssikkerhedshændelser – Del 1: Principper og proces
- DS/ISO/IEC 27035-2:2023 Informationsteknologi – Styring af informationssikkerhedshændelser – Del 2: Retningslinjer til planlægning og forberedelse hændelsesrespons
- DS/ISO/IEC 27036-1:2021 Cybersikkerhed – Leverandørrelationer – Del 1: Overblik og koncepter
- DS/ISO/IEC 27036-2:2022 Cybersikkerhed – Leverandørforhold – Del 2: Krav