DS/EN ISO/IEC 27001:2017-standarden og dens opbygning og indhold

Af Torben Abildgaard Pedersen

Titel

Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Krav

Anvendelsesområde

Et ledelsessystem for informationssikkerhed (ISMS) sikrer, at organisationen bliver stadigt bedre til kontinuerlig bevarelse af fortrolighed, integritet og tilgængelighed af informationer (herunder forskellige typer af data) ved hjælp af en risikostyringsproces således, at interessenter har tillid til, at alle former for risici forebygges på en forsvarlig måde.

Hvad er informationssikkerhed?

informationssikkerhed

forebyggelse af informationers (herunder datas) fortrolighed, integritet og tilgængelighed

fortrolighed

tilstand, hvor det sikres, at informationer ikke er tilgængelige for eller videregives til uautoriserede personer, enheder eller behandlingsprocesser

integritet

tilstand af nøjagtighed og fuldstændighed

tilgængelighed

tilstand, hvor informationer efter ordre eller forespørgsel fra en autoriseret person eller enhed kan genfindes og bliver vist på en anvendelig og meningsfuld måde

ISO/IEC 27001 er en ledelsesstandard, der stiller krav til et ledelsessystem, der skal kunne præstere, at en organisation iagttager den fornødne sikkerhed omkring etablering, opsamling, registrering, opbevaring, anvendelse, videregivelse og anden håndtering af informationer, herunder data. Data kan være af vidt forskellig art. I den mængde data, som en organisation har rådighed over og håndterer, indgår der ofte både persondata samt person- og helbredsfølsomme data.

Beskyttelse af persondata er objekt for regulering via persondataloven og EU's persondataforordning, som træder i kraft næste år - mere præcist den 25. maj 2018.

Overtrædelse af persondataforordningens bestemmelse kan i værste fald medføre bødestraf i størrelsesordener, der i praksis kan vanskeliggøre organisationens fortsatte ageren i markedet og dermed dens eksistens.

Læs om typisk forekommende trusler her [link indsættes]

Komplekset af ISO-ledelsesstandarder

ISO - den verdensomspændende standardiseringsorganisation har udgivet mange forskellige ledelsesstandarder, hvoraf de vigtigste er

- DS/EN ISO 9001:2015 - Kvalitetsledelsessystemer - Krav
- DS/EN ISO 14001:2015 - Miljøledelsessystemer - Krav og vejledning
- DS/EN ISO/IEC 17025:2005 - Generelle krav til prøvnings- og kalibreringslaboratoriers kompetence
- DSF/ISO 45001.2 - Arbejdsmiljøledelsessystemer - Krav og vejledning for brug (endnu kun et forslag)
- DS/EN ISO 22000:2005 - Ledelsessystemer for fødevaresikkerhed - Krav til virksomheder i fødevarekæden
- *DS/EN ISO/IEC 27001:2017 – Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Krav*
- DS/EN ISO 50001:2011 - Energiledelsessystemer - Krav og vejledning.
- DS/EN ISO 55001:2014 - Styring af aktiver (asset management) - Ledelsessystem - Krav

High Level Structure (HLS)

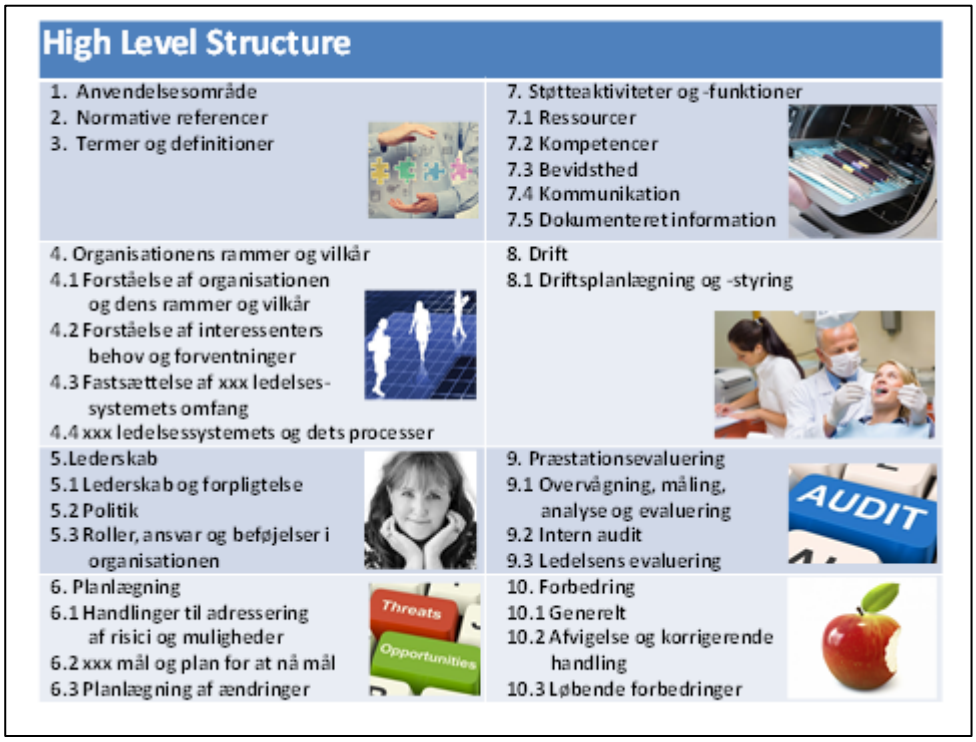
De fleste af disse standarder er allerede opbygget efter HLS, og de lidt ældre standarder fra 2005 og 2011 (laboratorieledelse, fødevaresikkerhed og energiledelse) vil følge efter, når en kommende revision gennemføres.

HLS dækker over en vedtagelse om alle ledelsesstandarderne skal være opbygget således, at teksten opdeles i 10 kapitler, herunder at flere af kapitlerne opledes i faste underpunkter, og at en stor del af kravene hørende til de respektive kapitler skal formuleres med ensartet ordlyd i overensstemmelse med en fast skabelon eller template.

De 10 kapitler, hvoraf kun kapitlerne 4-10 indeholder krav, er:

1	Anvendelsesområde
2	Normative referencer
3	Termer og definitioner
4	Organisationens rammer og vilkår
5	Lederskab
6	Planlægning
7	Støtteaktiviteter og -funktioner
8	Drift
9	Præstationsevaluering
10	Forbedring

De obligatoriske underkapitler illustreres på denne planche, som tit har været anvendt i **TAP**FREELANCE ApS i forbindelse med undervisning og foredragsvirksomhed inden for emnet:



Følgende udklip viser, at et udsnit af den ordlyd, som skal gå igen i alle ISO-ledelsesstandarder udformet efter HLS-principperne (her fra kapitel 4 om organisationens rammer og vilkår:

4. Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its XXX management system.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

— the interested parties that are relevant to the XXX management system;
— the relevant requirements of these interested parties.

4.3 Determining the scope of the XXX management system

The organization shall determine the boundaries and applicability of the XXX management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;
— the requirements referred to in 4.2.

"XXX" henviser til, at der de pågældende steder i teksten skal ske passende individualiseringer i afhængighed af ledelsesstandardens anvendelsesområde. "XXX management system" vil i dansk oversættelse skulle erstattes med kvalitetsledelsessystem, miljøledelsessystem, arbejdsmiljøledelsessystem eller informationssikkerhedsledelsessystem i afhængighed af, om man skriver på 9001, 14001, 45001 henholdsvis 27001.

De meget store individualiseringer fra ledelsessystemstandard til ledelsessystemstandard sker selvsagt i kapitel 8 - Drift. I en procesorienteret ledelsesstandard kan der ikke være meget fælles gods fra standard til

standard, for driftsprocesserne skal være i stand til at skabe netop den løbende forbedring, som er fastsat og beskrevet i standardens kapitel 1 - Anvendelsesområde.

Fra HLS - ISO/IEC Directives, Part 2, Rules for structure and drafting international standards, Annex SL - får man kun følgende skriveinstruktioner til udformningen af kapitel 8:

> **8. Operation**
>
> **8.1 Operational planning and control**
>
> *DRAFTING INSTRUCTION This subclause heading will be deleted if no additional subclauses are added to Clause 8.*
>
> The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by:
>
> — establishing criteria for the processes;
>
> — implementing control of the processes in accordance with the criteria;
>
> — keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.
>
> The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
>
> The organization shall ensure that outsourced processes are controlled.

Kombinerede ledelsessystemer

Fordi ISO-ledelsesstandarderne er skåret over den samme læst, er det forholdsvis oplagt og enkelt for en given organisation at udvikle et ledelsessystem, der kombinerer to eller flere sæt af krav. Har man fx et kvalitetsledelsessystem (9001) i forvejen, vil det være ret oplagt - hvis organisationen eksempelvis definerer eller bliver mødt med krav til øget informationssikkerhed - at integrere et informationssikkerhedsledelsessystem (27001) ind i det eksisterende.

Mange af de beskrevne procedurer fra tidligere vil (evt. efter tilpasning af terminologi etc.) fortsat kunne anvendes i det udvidede ledelsessystem, der i givet vil bygge på en kombination af kravene til kvalitetsledelse og informationssikkerhedsledelse (9001+27001). Det gælder navnlig procedurer af generisk art vedrørende fx styring af dokumenteret information, risikovurdering, intern audit, styring af afvigelser og korrigerende handlinger samt gennemførelsen af ledelsens evaluering. Men også procedurer for en række støtteaktiviteter og -funktioner, fx vedrørende ressource-, personale- og kompetencestyring samt styring af infrastruktur, miljø for drift af processer og organisatorisk videndeling, vil kunne genanvendes ved tilføjelse af det nødvendige i relation til de supplerende krav. På driftsområdet vil også procedurer vedrørende kunderelaterede processer, udvikling og styring ydelser leveret udefra (herunder indkøb) i reglen også kunne genanvendes med forholdsvis enkle tilpasninger.

Hertil må så føjes de informationssikkerhedsspecifikke dokumenter, som DS/EN ISO/IEC 27001 særskilt stiller krav om.

Ledelsesprincipperne

Det er yderligere befordrende for muligheden for kombination af kravene i ISO-ledelsesstandarderne, at de alle bygger på fælles ledelsesprincipper og - i væsentlig udstrækning - fælles terminologi. De syv fælles ledelsesprincipper, som er inspireret ud fra kvalitetsledelsesprincipperne beskrevet i DS/EN ISO 9000:2015, og som ikke vil blive gennemgået i detaljer i denne artikel, er:

Nr.	Ledelsesprincip	Princippets formulering	Rationale
1	Interessentfokus	Det primære fokus for ledelse er at opfylde interessentkrav og at stræbe efter at overgå interessenternes forventninger.	Vedvarende succes opnås, når en organisation tiltrækker og bevarer interessenternes tillid. Hvert aspekt af interaktion med interessenter giver mulighed for at skabe mere værdi for interessenterne. At forstå nuværende og fremtidige behov hos interessenter bidrager til vedvarende succes for organisationen.
2	Lederskab	Ledere på alle niveauer skaber en helhed af formål og udviklingsretning og sørger for betingelser, hvorunder medarbejdere er engagerede i at nå organisationens mål.	At skabe en helhed af formål og udviklingsretning samt medarbejderengagement giver en organisation mulighed for at samordne strategier, politikker, processer og ressourcer for at nå sine mål.
3	Personers engagement Når der står *personer* skyldes det, at der kan være tale om mange flere end de ansatte, fx konsulenter.	Kompetente, bemyndigede og engagerede medarbejdere på alle niveauer i organisationen er væsentlige for at forbedre organisationens evne til at skabe og levere værdi.	For at lede en organisation effektivt og hensigtsmæssigt er det vigtigt at respektere og involvere alle medarbejdere på alle niveauer. Anerkendelse, bemyndigelse og forbedring af kompetencer fremmer medarbejderes engagement i at nå organisationens mål.
4	Procesorientering	Konsekvente og forudsigelige resultater opnås mere effektivt og hensigtsmæssigt, når aktiviteter opfattes og håndteres som indbyrdes forbundne processer, der fungerer som et sammenhængende system.	Ledelsessystemet består af indbyrdes forbundne processer. At forstå, hvordan der frembringes resultater med dette system, sætter en organisation i stand til at optimere systemet og dets præstation.
5	Forbedring	Succesrige organisationer har løbende fokus på forbedring.	Forbedring er afgørende for, at en organisation kan opretholde de nuværende præstationsniveauer, reagere på ændringer af de interne og eksterne betingelser, og skabe nye muligheder.
6	Videnbaseret beslutningstagning	Der er større sandsynlighed for, at beslutninger baseret på analyse og evaluering af data og informationer giver de ønskede resultater.	Beslutningstagning kan være en kompleks proces og indebærer altid en vis usikkerhed. I beslutningstagning indgår ofte flere forskellige typer af og kilder til input samt fortolkning af input, som kan være subjektiv. Det er vigtigt at forstå forholdet mellem årsag og virkning og potentielle utilsigtede konsekvenser. Analyse af fakta, vidnesbyrd og data fører til større objektivitet og tillid til beslutningstagningen.
7	Styring af relationer	For at opnå vedvarende succes styrer organisationer deres relationer til relevante interessenter, fx leverandører.	Relevante interessenter har indflydelse på en organisations præstation. Der er større sandsynlighed for vedvarende succes, når organisationen styrer relationerne til alle interessenter for at optimere deres indvirkning på organisationens præstation. Styring af relationer til leverandør- og partnernetværk er af særlig betydning.

Procesorientering

Dette ledelsesprincip er særlig vigtigt for at forstå tankegangen bag en ISO-ledelsesstandard opbygget efter HLS.

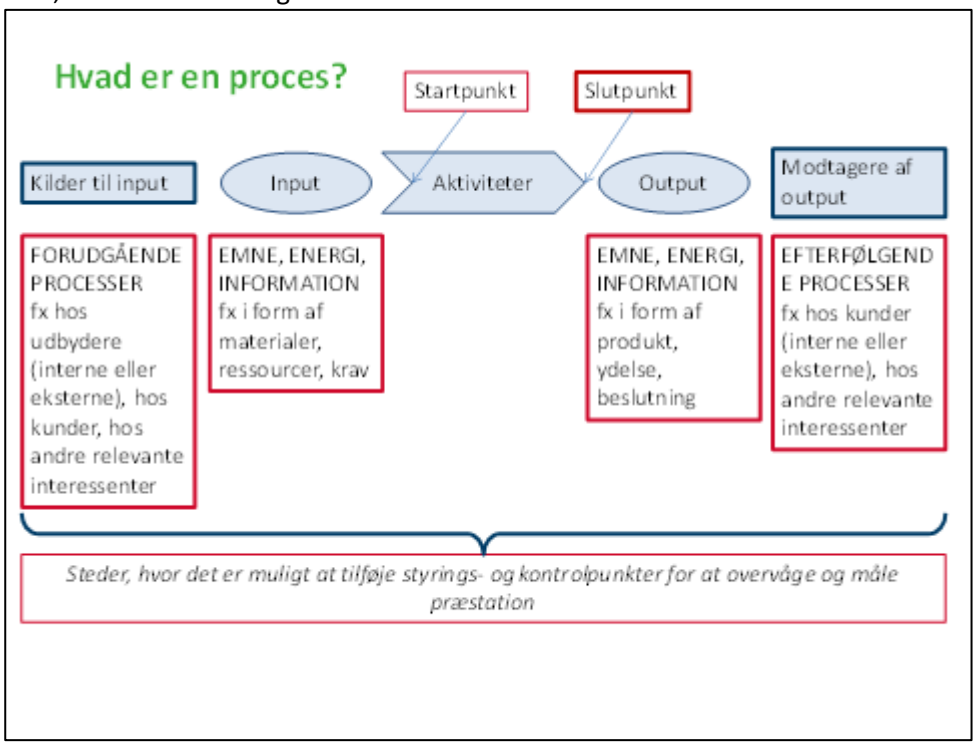
Procesorientering - nemlig det, at et ledelsessystem består af indbyrdes forbundne processer, der har til formål at skabe en løbende forbedring (dvs. skabe værdi, præstere resultater og frembringe vedvarende succes) - består af 3 ingredienser:

1. Procesmodellen
2. Plan-Do-Check-Act-cyklus
3. Risikobaseret tankegang

Procesmodellen

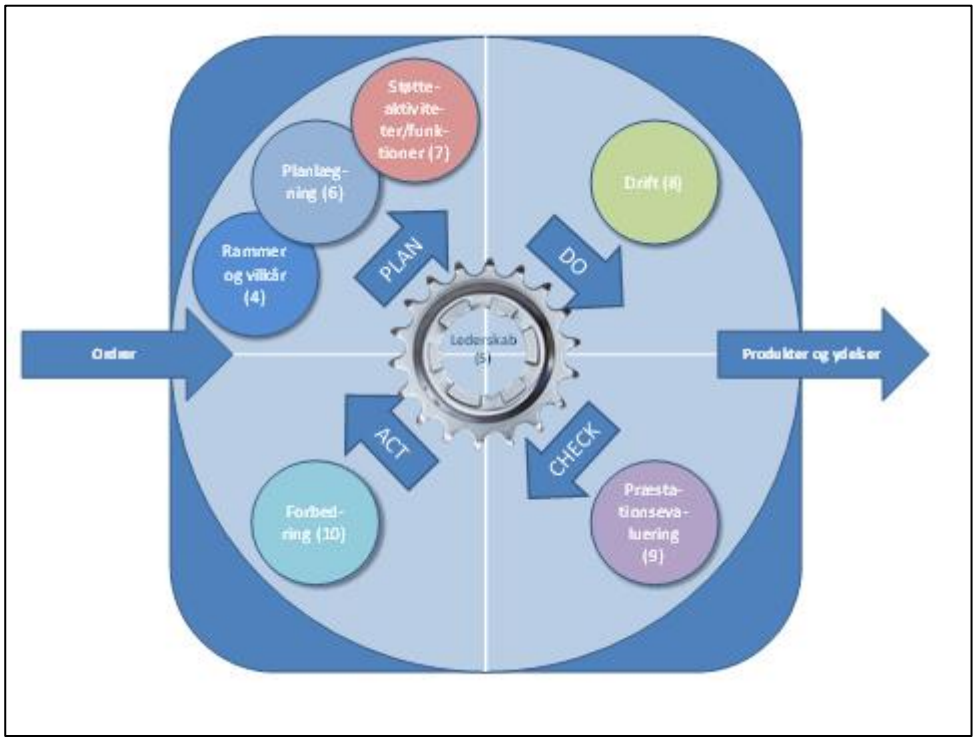
Procesmodellen viser i sin enkelthed, at når man lave risikovurdering af bestemt aktiv i form af driftsproces (fx udvikling af kildekode hos en softwareleverandør ved etablering af en ny webapplikation), kan det være nyttigt at se processen i et videre perspektiv, fordi der som regel ligger noget forud for selve processen, fx etablering af en kravspecifikation (= URS, User Requirement Specification), og at der også ligger noget efter selve kildekodeudviklingsprocessen, fx at der skal gennemføres forskellige former validering af løsningen, jf. V-modellen for softwareudvikling.

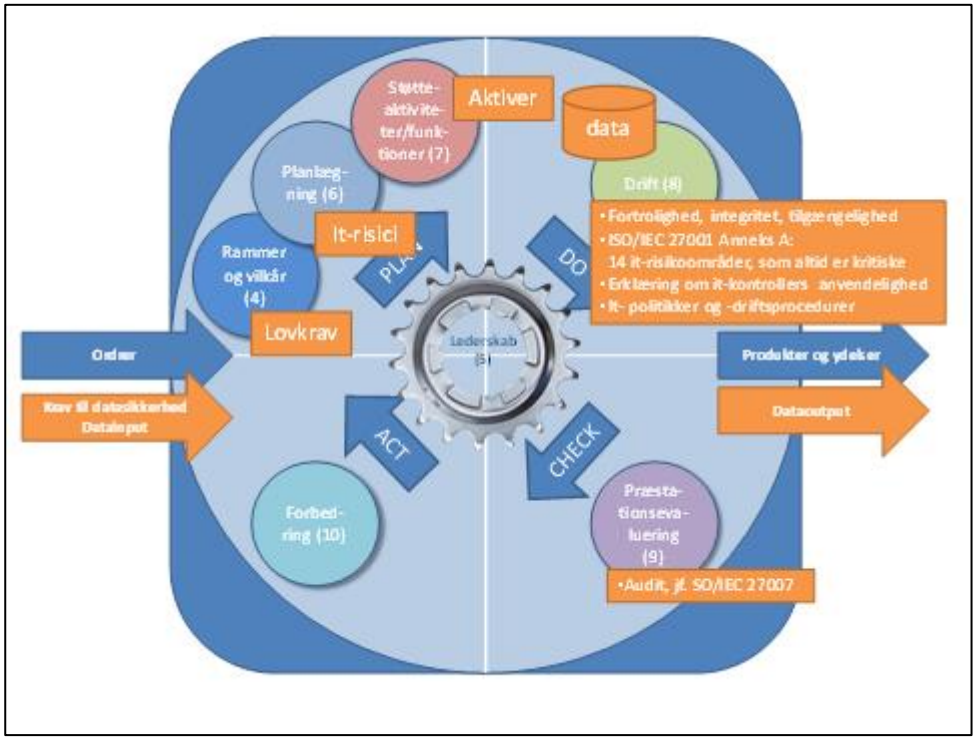
Og som det ses af skitsen, kan styrings- og kontrolpunkter for informationssikkerhed være knyttet til alle dele af den samlede proces - både det, der går forud, og det, der kommer efterfølgende. Man må med andre ord være for snæver i sine betragtninger, fordi det kan vise sig, at hunden ligger begravet et andet sted, end man måske lige kommer i tanker om.



Plan-Do-Check-Act-cyklus

Mere overordnet udgør de indbyrdes forbundne processer i et ISMS et kredsløb, Plan-Do-Check-Act, der udvikledes af amerikanske professor Walter A. Shewhart i 1939. Det betyder HLS-modellens kapitler fra 4 til 10 kan indplaceres på Shewhart-cirklen, som det er vist her for både ISO 9001 og ISO/IEC 27001:

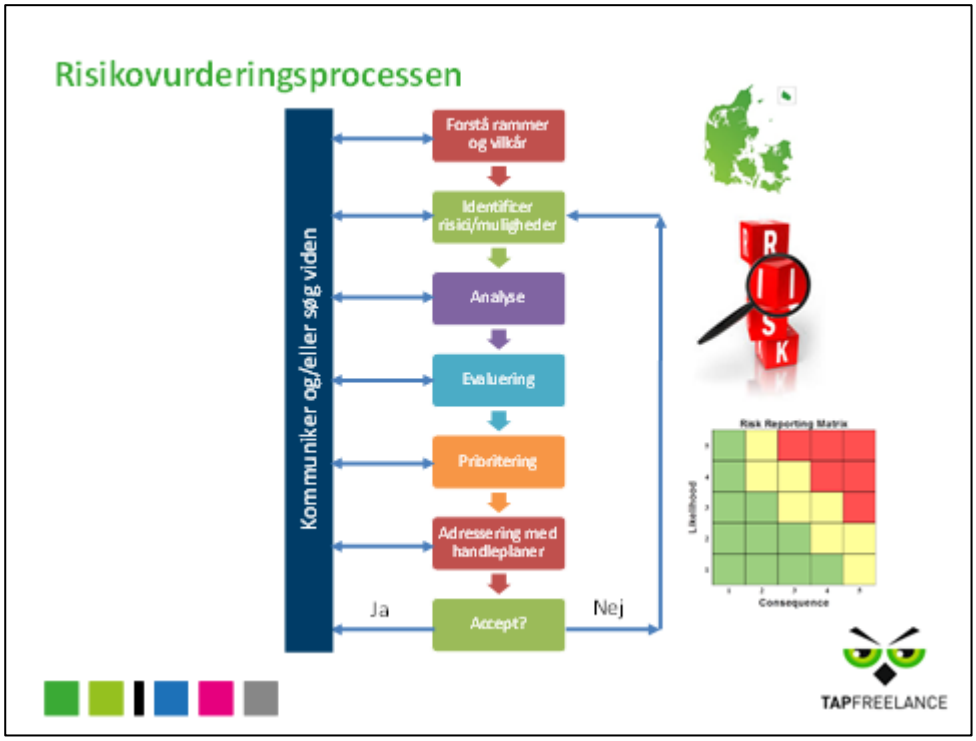

Støtte-aktivite-ter/funk-tioner (7)
Planlæg-ning (6)
Rammer og vilkår (4)
PLAN
DO
Drift (8)
Ordre
Leder-skab (5)
Produkter og ydelser
ACT
CHECK
Forbed-ring (10)
Præsta-tionseva-luering (9)


Støtte-aktivite-ter/funk-tioner (7)
Aktiver
data
Planlæg-ning (6)
Drift (8)
• Fortrolighed, integritet, tilgængelighed
• ISO/IEC 27001 Annex A:
14 it-risikoområder, som altid er kritiske
• Erklæring om it-kontrollers anvendelighed
• It- politikker og -driftsprocedurer
It-risici
Rammer og vilkår (4)
Lovkrav
Ordre
Leder-skab (5)
Produkter og ydelser
Krav til datasikkerhed
Dataoutput
Dataindput
ACT
CHECK
Forbed-ring (10)
Præsta-tionseva-luering (9)
• Audit, jf. SO/IEC 27007

Risikovurderingsprocessen

Procesorientering omfatter risikovurdering til fastlæggelse kritiske styringspunkter (her: it-kontroller), og i DS/EN ISO/IEC 27001:2017 er det på mange måder gjort let for organisationen, fordi man reelt kan nøjes med - ud fra egen risikovurdering - at tage stilling til, hvilke af it-kontrollerne med form af prædefinerede politikker og driftsprocedurer der relevante. Det sker i det såkaldte Statement of Applicability (SoA; Erklæring om it-kontrollers anvendelighed).

Det betyder i praksis, at handleplanerne, der resulterer af risikovurderingens adresseringsfase, vil komme til at dreje sig om it-kontrollernes implementering. Er der fx ikke en velafprøvet total disaster recovery-procedure fra starten, vil man antagelig kunne blive certificeret på en detaljeret handleplan, der går ud på - inden for rimelig tid - at beskrive og implementere en sådan.



Informationssikkerheds systemets politikker og driftsprocedurer

Driftskapitlet - kapitel 8 - i DS/EN ISO/IEC 27001:2017 indeholder ikke mange selvstændige krav, men udgør i reelt en beskrivelse af, hvordan fortegnelsen over aktiver danner grundlag for en risikovurdering, der har form af en stillingtagen til relevansen og implementeringen af de i Anneks A listede it-kontroller (politikker og driftsprocedurer) i medfør af anneksets 14 it-risikoområder. De 14 områder er opdelt i godt 100 it-kontroller (= kritiske styringspunkter), der - hvis de er anvendelige - alle skal implementeres, evt. via de nødvendige handleplaner.

Det er i denne sammenhæng rimeligt, at opfatte de krævede *it-politikker* i annekset som *regler*. Et krav om fx en adgangsstyringspolitik betyder slet op ret, at der skal være veldefinerede regler for adgangsstyring, at der eksempelvis skal være regler for dannelse, meddelelse, anvendelse, opbevaring, brug, hemmeligholdelse, forældelse, fornyelse og anden administration af passwords.

Tilsvarende er kravene til it-kontroller at opfatte som driftsprocedurer i relation til informationssikkerhed. Fx i A.12.3.1 hedder det, at der skal være implementeret en it-kontrol, der skal sikre, at der "tages

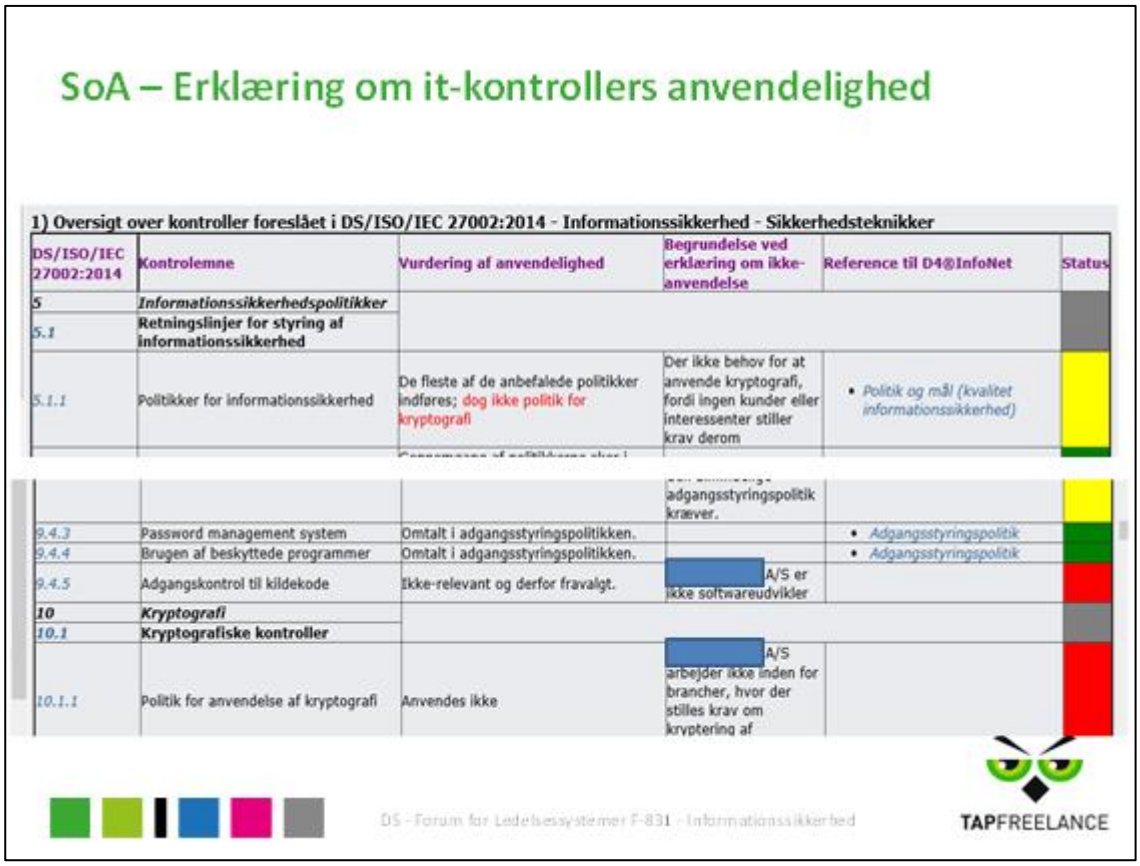
backupkopier af information, software og systembilleder, … ". Altså en driftsprocedure, som beskriver backup-processerne.

Det engelske ord *control* er oversat til dansk med *(it-)kontrol* vel vidende, at *control* egentlig betyder *styring*, *styringspunkt* eller *kritisk styringspunkt*, der ofte stiller krav om etablering og implementering af enten en politik (= regler) eller en driftsprocedure.

Arbejdsgangen ved etablering og implementering af regler og driftsprocedurer kan illustreres ved dette kredsløb i forhold til PDCA-cyklussen:

Anneks A - it-risikoområderne opdelt i it-kontroller med krav om politikker (regler) og driftsprocedurer

Vi slutter rundgangen i DS/EN ISO/IEC 27001: 2017 ved at liste de 14 it-risikoområder og et eksempel på et etableret Statement of Applicability (= SoA; Erklæring om it-kontrollers anvendelighed). Den bedste beskrivelse af it-kontrollernes indhold ses i hjælpestandarden DS/ISO/IEC 27002:2014


SoA – Erklæring om it-kontrollers anvendelighed
1) Oversigt over kontroller foreslået i DS/ISO/IEC 27002:2014 - Informationssikkerhed - Sikkerhedsteknikker
DS/ISO/IEC 27002:2014
Kontrolemne
Vurdering af anvendelighed
Begrundelse ved erklæring om ikke-anvendelse
Reference til D4®InfoNet
Status
5
Informationssikkerhedspolitikker
5.1
Retningslinjer for styring af informationssikkerhed
5.1.1
Politikker for informationssikkerhed
De fleste af de anbefalede politikker indføres; dog ikke politik for kryptografi
Der ikke behov for at anvende kryptografi, fordi ingen kunder eller interessenter stiller krav derom
Politik og mål (kvalitet informationssikkerhed)
adgangsstyringspolitik kræver.
9.4.3
Password management system
Omtalt i adgangsstyringspolitikken.
Adgangsstyringspolitik
9.4.4
Brugen af beskyttede programmer
Omtalt i adgangsstyringspolitikken.
Adgangsstyringspolitik
9.4.5
Adgangskontrol til kildekode
Ikke-relevant og derfor fravalgt.
A/S er ikke softwareudvikler
10
Kryptografi
10.1
Kryptografiske kontroller
10.1.1
Politik for anvendelse af kryptografi
Anvendes ikke
A/S arbejder ikke inden for brancher, hvor der stilles krav om krypterin af
DS - Forum for Ledelsessystemer F-831 - Informationssikkerhed
TAPFREELANCE

Slut.