

Den nye ISO/IEC 27002- standard

Nye foranstaltninger serveret
i en helt ny struktur



En ny ISO/IEC 27002 har ramt hylderne i 2022, og der venter os en lille revolution. Ud over en ny struktur er bl.a. antallet af foranstaltninger reduceret, og der benyttes en række nye perspektiver til belysning af de enkelte foranstaltninger. Her får du et overblik over de væsentligste ændringer i den nye vejledning.

Baggrund

For organisationer, der i dag følger ISO/IEC 27001, indeholder ISO/IEC 27002 en uundværlig vejledning til det sæt af foranstaltninger¹, som organisationen skal forholde sig til. Sagt anderledes: vi kommer ikke udenom ISO/IEC 27002, når et ledelsessystem for informationssikkerhed (ISMS) efter ISO/IEC 27001 etableres eller vedligeholdes. Desuden forudsætter organisationers varetagelse af privatlivsbeskyttelse i GDPR-regi en stillingtagen til passende tekniske og organisatoriske foranstaltninger, og her fungerer ISO/IEC 27002 som en vigtig værktøjskasse til håndtering af de risici, som vedrører den registrerede².

Sidst standarden blev ændret var i 2013³, hvorfor informationssikkerhedseksperter i en årrække har set frem til en ny udgave med et frisk, opdateret sæt af sikkerhedsforanstaltninger. I det følgende præsenteres et overblik over de fundamentale ændringer, som følger med den nye ISO/IEC 27002⁴. Præsentationen inddeles i følgende afsnit:

1. **Tematisk struktur**
2. **Nye og ændrede foranstaltninger**
3. **Anvendelse af attributter**
4. **Supplerende annekser**
5. **Samlet vurdering**

1. Tematisk struktur

Tidligere var ISO/IEC 27002 inddelt i 14 kapitler, der tilsammen indeholdt 114 foranstaltninger fordelt på forskellige sikkerhedstemaer. Nu opdeles standarden i fire kapitler! Eller rettere fire temaer: Organisatorisk, adfærdsmæssig, fysisk og teknologisk⁵. Foranstaltningerne er placeret inden for det tema, som vurderes mest centralt for en given foranstaltning. (Se figur på næste side).

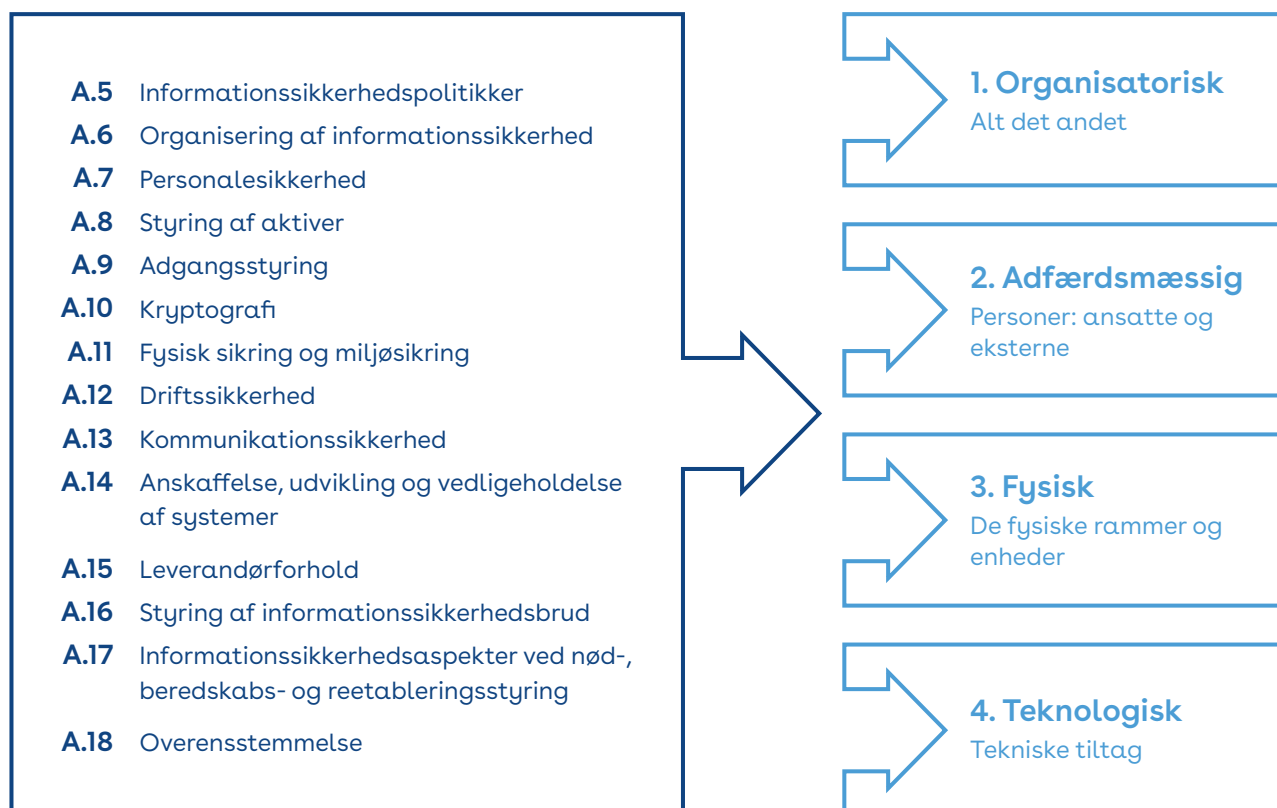
¹ Uheldigvis er "controls" i dag oversat til "kontroller" i ISO/IEC 27002. Fremadrettet vil oversættelsen hedde "foranstaltninger" for at indfange, at der er tale om handlinger til nedbringelse eller fastholdelse af risici: alt fra awareness-træning til kryptering.

² ISO/IEC 27701 (kravstandard til et ledelsessystem for privatlivsbeskyttelse) indeholder en supplerende vejledning til ISO/IEC 27002 ud fra et privatlivshensyn.

³ Den tidligere version af ISO/IEC 27002 har ganske vist titlen ISO/IEC 27002:2017 – dette skyldes dog alene den identiske europæiske udgivelse af standarden i 2017. Indholdsmæssigt er standarden ikke blevet revideret siden 2013-versionen.

⁴ Desuden følger der med den ny ISO/IEC 27002 en række ændringer i specifikke termer og definitioner, som af hensyn til overblik og præsentationslængde ikke er inkluderet.

⁵ Det bør nævnes, at også standardens titel er ny. Code of practice for information security controls er nu erstattet af et mere mundret Information security controls.



Figur 1: Fra 14 kapitler i ISO/IEC 27002:2013 til 4 kapitler i ISO/IEC 27002:2022⁶.

Til eksempel vil beskyttelse mod malware falde ind under kategorien 'teknologisk foranstaltning', hvor tekniske viruskontroller er den afgørende komponent, der dog kan tænkes suppleret med fx en adfærdsmæssig og organisatorisk dimension. Det kunne være etablering af tekniske viruskontroller i kombination med, at medarbejdere uddannes i at udvise sund fornuft, før de klikker på et link i en mail, og hvor der formuleres retningslinjer for virusscanning.

Det første tema dækker **organisatoriske foranstaltninger**, som indeholder dokumentation, fx politikker, regler, processer, procedurer, vejledninger, logs, referater, rapporter, testresultater, målinger, evalueringer mv.⁷

Det andet tema vedrører de **adfærdsmæssige foranstaltninger**. Her finder vi, med få justeringer, de foranstaltninger, som vi kender fra 7. *Personalesikkerhed*. Logisk nok har foranstaltninger vedrørende arbejde udenfor kontoret samt medarbejdernes rolle i forbindelse med rapportering af hændelser fundet vej til dette tema.

⁶ ISO/IEC 27002:2022 er endnu ikke oversat til dansk, hvorfor de benyttede titler for de nye temaer og alle øvrige oversættelser er foreløbige bud.

⁷ Under revisionsarbejdet arbejdede man med en definition af organisatoriske foranstaltninger som værende alt, hvad der ikke kunne indplaceres i de øvrige temaer.

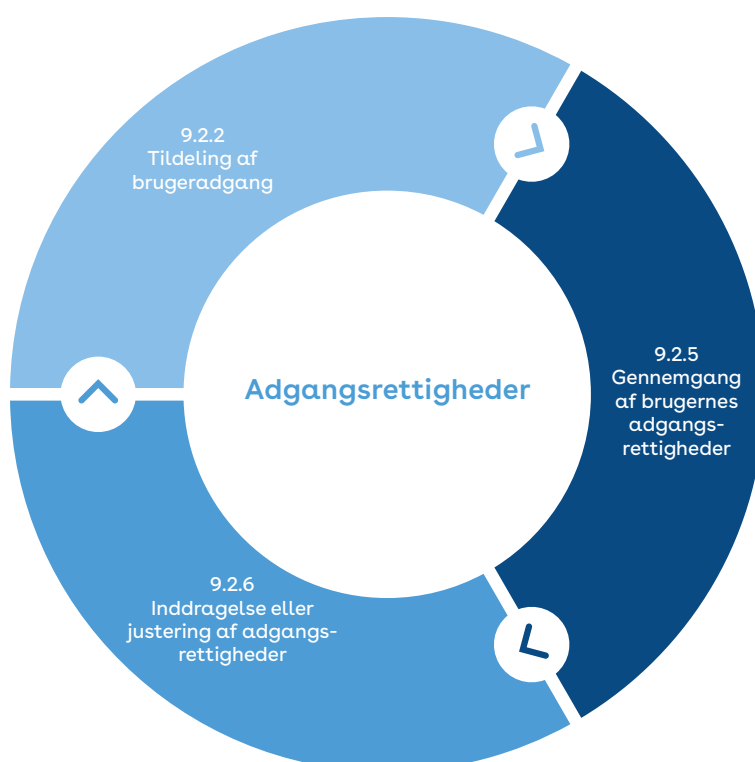
Genkendelsens glæde venter ligeledes i det tredje tema, som omfatter de **fysiske foranstaltninger**. Foranstaltningerne fra 11. Fysisk sikring og miljøsikring er at finde under dette tema, suppleret med en mindre del af fysisk beskyttelse af medier hentet fra 8. *Styring af aktiver*.

Teknologiske foranstaltninger danner rammen om fjerde og sidste tema. Et omfangsrigt kapitel, som dækker alle tekniske tiltag: styring af adgange, logning, back-up, kryptering og meget andet – herunder en række nye foranstaltninger, der redegøres for under 3. *Nye foranstaltninger*.

Tematiseringen af foranstaltningerne har ikke overraskende været et stort stridsspørgsmål under revisionen af standarden. Ikke mindst fordi der internationalt benyttes mange forskellige tilgange til strukturering af sikkerhedsforanstaltninger⁸. Mange af uenighederne er dog løst ved at benytte et særligt attribut-diagram ud for hver foranstaltning, som der kan læses mere om under 4. *Attributter*.

2. Nye og ændrede foranstaltninger

Færre foranstaltninger er en væsentlig konsekvens af den gennemførte ISO/IEC 27002-revision. Til trods for at der er kommet en række nye fokusområder til, reduceres det samlede antal af foranstaltninger fra 114 til blot 93. Det skyldes primært en sammenlægning af en lang række foranstaltninger, som vurderes at være forbundne i samme livscyklus, fx på området for adgangsstyring, hvor foranstaltninger vedrørende tildeling, gennemgang, inddragelse eller justering af adgangsrettigheder kan betragtes som dele af samme proces. Det fører derfor til en sammenlægning af tre foranstaltninger til én samlet under overskriften 'Adgangsrettigheder', jf. figur 2.



Figur 2: Eksempel på hvordan tre foranstaltninger sammenlægges til én i ISO/IEC 27002:2022.

⁸ Andre tilgange er fx en opdeling i ledelse-administration-jura-teknik eller en opdeling i hhv. administrative/processuelle og fysiske/tekniske tiltag.

Reduktionen i antallet af foranstaltninger skyldes i andre tilfælde, at der foreligger et væsentlig indholdsmæssigt overlap, fx hvor der i dag tales sikkerhed i forbindelse med slutbrugernes enheder (mobiltelefoner, pc'er, laptops osv.)⁹, eller hvor informationssikkerhed introduceres i hhv. projektledelse og IT-anskaffelse¹⁰.

Det er otte år¹¹ siden, ISO/IEC 27002 sidst blev opdateret, og derfor har mange foranstaltninger fået et tiltrængt ansigtsløft. Samtidig er der kommet 11 helt nye foranstaltninger til, hvoraf hovedparten – ikke overraskende – findes i kapitlet vedrørende nye teknologiske foranstaltninger. *Web filtering*, *Secure coding* og *Configuration Management*¹² er eksempler på tekniske tilføjelser, som gør standarden mere up-to-date. Nedenfor er en oversigt over de nye foranstaltninger¹³.

Adfærdsmæssig	Fysisk Physical security monitoring
Organisatorisk Threat intelligence Information security for use of cloud services ICT readiness for business continuity	Teknologisk Configuration management Information deletion Data masking Data leakage prevention Monitoring activities Web filtering Secure coding

Figur 3: Illustration af de nye foranstaltninger indplaceret i deres tilhørende tema.

Nye best practices i forbindelse med brug af cloud-løsninger, begreber indenfor forretningsrobusthed¹⁴ og ikke mindst privatlivshensyn har sat deres tydelige aftryk på den nye version. Sidstnævnte aflæses af nye foranstaltninger som *information deletion*, *data masking* og *data leakage prevention*. Her er det dog vigtigt at understrege, at der ganske vist er tale om et indspark fra privatlivssiden, men dog sådan at forstå, at alle tre repræsenterer handlinger, som beskytter informationer over en bred kam – ikke alene personoplysninger.

⁹ 6.2.1 Politik for mobilt udstyr sammenlægges med 11.2.8 Brugerudstyr uden opsyn.

¹⁰ 6.1.5 Informationssikkerhed ved projektstyring sammenlægges med 14.1.1 Analyse og specifikation af informationssikkerhedskrav.

¹¹ Sådan gik det pudsigt nok tidligere: ISO/IEC 27002 udkom i en opdateret version i 2005, 2013 og nu 2022.

¹² Det betyder, at standarden nu tydeligere får sondret imellem change og configuration management med hver deres foranstaltning under det tekniske tema.

¹³ De engelske titler benyttes, mens vi venter på den danske oversættelse.

¹⁴ Inspireret af EN ISO 22300-serien for Business Continuity.

3. Anvendelse af attributter

Anvendelsen af attributter er anden lille revolution. Ud for hver enkelt foranstaltning er der indsat et diagram med fem attributter, som gør os klogere på de egenskaber, som følger med den pågældende foranstaltning. Attributterne kan siges at udgøre alternative perspektiver til den tematiske inddeling af foranstaltninger. Samtlige fem attributter figurerer i et diagram som indledning på beskrivelsen af hver foranstaltning. Nedenfor er et eksempel i tilknytning til foranstaltningen *Use of Cryptography*:¹⁵

Type af foranstaltning (Se 4.1)	Egenskaber for informations-sikkerhed (Se 4.2)	Cyber-sikkerheds-koncept (Se 4.3)	Operationelle ressourcer (Se 4.4)	Sikkerheds-domæne (Se 4.5)
#Forebyggende	#Fortrolighed #Integritet	#Protect	#Secure_configuration	#Protection

Figur 4: Eksempel på anvendelsen af attributter som inddeling på foranstaltningen *Use of Cryptography*.

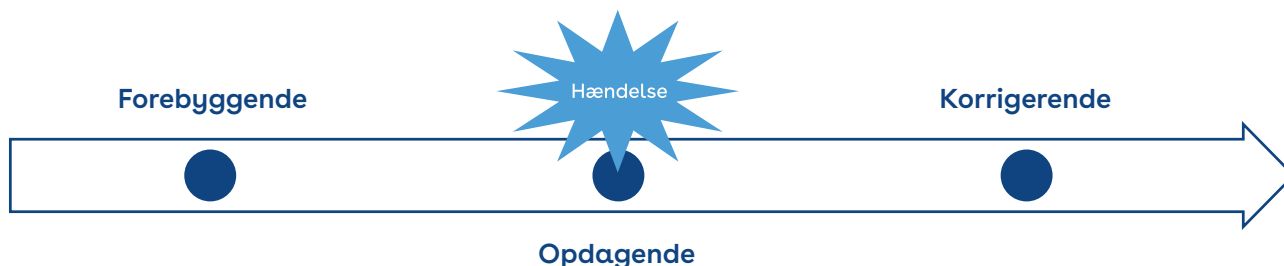
Organisationer kan bruge attributværdierne til at skabe forskellige perspektiver på informationssikkerhedsindsatsen afhængig af formål eller målgruppe¹⁶. I det følgende gives et overblik over indholdet og formålet med de fem attributter.

¹⁵ Efter attributdiagrammet følger beskrivelsen af foranstaltningen, formålet, selve vejledningen og supplerende informationer. I den forbindelse er det nyt, at der følger ét formål med hver foranstaltning: i den nuværende 2013-version angives formål alene ud for sikkerhedskategorierne, en slags underkapitler til de 14 sikkerhedsområder, som nu udfases.

¹⁶ Dette muliggøres især af de tilhørende annekser beskrevet under 5. *Annekser*.

3.1 Type af foranstaltning

Her betragtes foranstaltninger ud fra, hvornår og hvordan de påvirker risikoen i forhold til forekomsten af en informationssikkerhedshændelse. Attributten opererer med tre velkendte værdier:



Figur 5: Attribut som angiver, om en foranstaltning er forebyggende, opdagende og/eller korrigerende¹⁷.

- **Forebyggende:** foranstaltningen er præventiv og har indvirkning på årsagen til, at en uønsket¹⁸ hændelse opstår.
- **Opdagende:** foranstaltningen muliggør at søge, opdage og identificere uønskede hændelser, der opstår.
- **Korrigerende:** foranstaltningen virker udbedrende i kølvandet på, at en hændelse er opstået.

Det følger heraf, at visse foranstaltninger i ISO/IEC 27002 både angives med forebyggende og opdagende og korrigerende værdier. Attributten må forventes at kunne spille en central rolle i organisationers risikoarbejde som hjælp og inspiration til, hvordan der mest effektivt sættes ind overfor specifikke risikoscenarier, herunder fx om sandsynlighed og/eller konsekvens bør nedbringes.

3.2 Egenskaber for informationssikkerhed

Denne attribut repræsenterer krumtappen for informationssikkerhed, hvor foranstaltninger vurderes ud fra, hvad de bidrager til at bevare:

- **Fortrolighed:** beskyttelse af informationer mod uautoriseret adgang eller videregivelse
- **Integritet:** beskyttelse af informationer mod uautoriseret ændring eller ødelæggelse
- **Tilgængelighed:** beskyttelse af informationer mod uautoriseret adgangsforbud for de personer, som har retmæssig adgang.

Dermed definerer den ny ISO/IEC 27002 mere konkret, hvilke værdier en given foranstaltning bevarer. Det kan hjælpe organisationer med at forstå og synliggøre koblingen mellem ledelsens overordnede politikker for informationssikkerhed og de konkrete handlinger, som håndterer risici. Dog bør det noteres, at attributten i mere begrænset omfang fungerer som en "diskriminerende faktor", da næsten samtlige foranstaltninger potentielt kan tilføje alle tre værdier¹⁹.

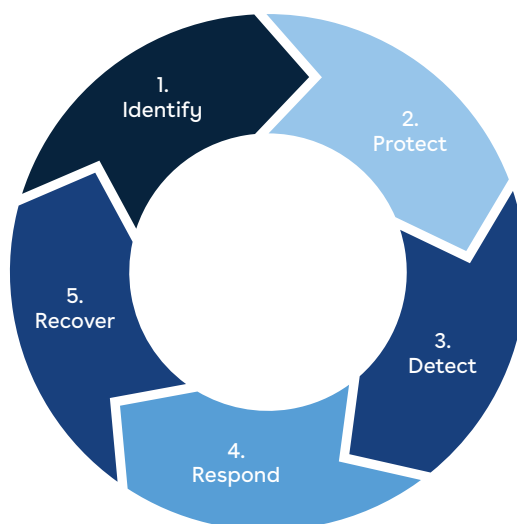
¹⁷ Her har man fravalgt den mere detaljerede model, hvor forebyggende foranstaltninger tilføjes yderligere to kategorier: kompenserende/lagdelte foranstaltninger samt afskrækkende foranstaltninger.

¹⁸ Med "uønsket" menes en informationssikkerhedshændelse, som organisationen har bestemt er uacceptabel i forhold til opnåelse af en relevant informationssikkerhed

¹⁹ Blot 14 af de 93 foranstaltninger indvirker ikke på både fortrolighed, integritet og tilgængelighed.

3.3 Cybersikkerhedskoncept

Her vurderes foranstaltninger ud fra deres tilknytning til cybersikkerhedsbegreberne i den nye tekniske standard, ISO/IEC 27110. Der er imidlertid tale om nogle gamle kendinge, da man har skelet til de mest udbredte modeller – ikke mindst NIST's begrebsramme, NIST Cyber Security Framework²⁰.



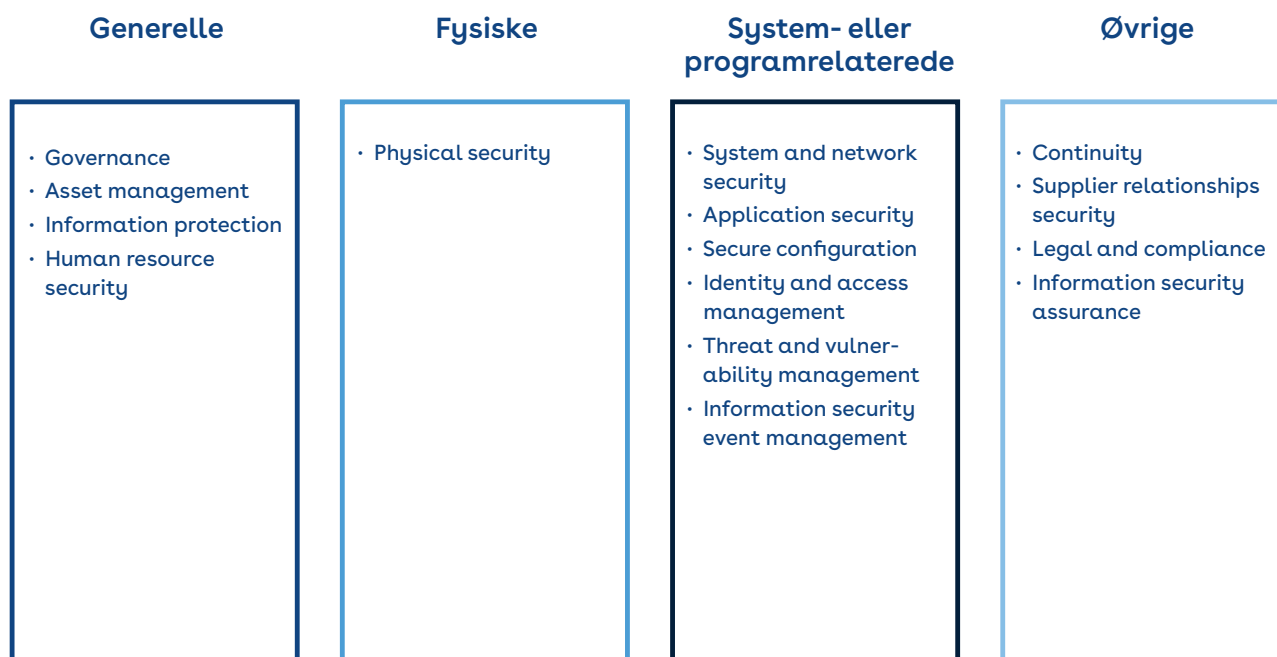
- **Identify:** etablering af en organisatorisk forståelse og kontekst til styring af cybersikkerhedsrisiko med fokus på forretningsmål, forretningsmiljø, interesser, aktiver, forretningsprocesser, love, regler, trusselmiljø og cyberrisici.
- **Protect:** udvikling af passende foranstaltninger til opbygning af organisationens cyberprofil, samt kontrol af at forebyggende foranstaltninger fungerer i forhold til forretningens behov.
- **Detect:** fastlæggelse af aktiviteter til at identificere cybersikkerhedshændelser. Aktiviteterne gør det muligt for organisationen at observere ændringer i adfærd, tilstande, trafik, konfiguration eller behandling af nøgleressourcer.
- **Respond:** tilrettelæggelse af aktiviteter til at kvalificere og reagere på en opdaget cyber-sikkerhedshændelse og inddæmme konsekvensen heraf.
- **Recover:** identifikation af passende aktiviteter til at vedligeholde beredskabsplaner og genetablere systemer eller services, der blev påvirket af en cybersikkerhedshændelse.

Ovenstående fem attributværdier kan siges at komplimentere ledelsessystemet for informationssikkerhed (ISMS) og giver organisationer mulighed for at vurdere foranstaltningers relevans i en kontekst af cybersikkerhed.

²⁰ <https://www.nist.gov/cyberframework>.

3.4 Operationelle ressourcer

Attributten operationelle ressourcer (eller operationelle kapaciteter²¹) iagttager foranstaltninger ud fra den praktiserende persons perspektiv. Attributværdierne taler derfor ind i de forskellige informationssikkerhedsfunktioner, som varetages i organisationen, og er dermed et muligt redskab til i organisationens respektive afdelinger at placere ansvar for tilvalgte foranstaltninger. Nedenfor er en oversigt over de benyttede attributværdier.



Figur 6: De 15 attributværdier under operationelle ressourcer²².

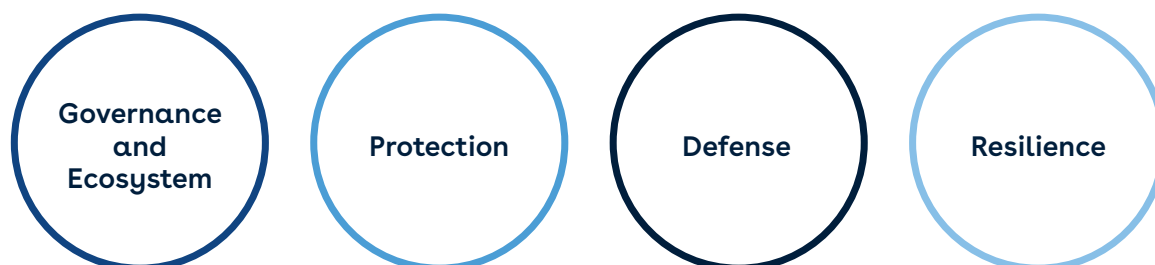
For medarbejdere, der varetager en rolle i forbindelse med implementering af forskellige sikkerhedstiltag, vil attributværdierne formentlig give god mening, mens almindelige brugere måske vil opleve de operationelle begreber som mindre genkendelige.

²¹ I den engelske version: *operational capabilities*.

²² De fire benyttede emner anvendes ikke i ISO/IEC 27002:2022, men bruges her til at give et bedre overblik over attributten.

3.5 Sikkerhedsdomæner

Sidste attribut omhandler sikkerhedsdomæner. Her er tale om en last minute-tilføjelse til porteføljen af attributter med det formål at vise foranstaltningerne ud fra den ramme, som i EU-regi benyttes ved fastsættelse af sikkerhedskrav til kritiske informationssystemer og netværk²³.



Figur 7: Ovenfor de fire attributværdier, som angiver sikkerhedsdomæner.

4. Supplerende annekser

Som et sidste nyhedsindslag er der tilføjet to nye annekser til standarden. Det første (Anneks A) redegør for, hvordan de fem gennemgåede attributter kan benyttes, fx ved at knytte foranstaltninger og attributter til specifikke risikoscenarier og dermed bidrage til risikovurderingsprocessen efter ISO/IEC 27001. Her leveres desuden et samlet diagram over foranstaltningerne og de tilhørende attributværdier – noget som kan gøre det lettere for organisationer at filtrere, sortere eller præsentere foranstaltningerne i forskellige visninger afhængig af målgruppe eller opgave²⁴. Det andet anneks (Anneks B) bliver en kærkommen hjælp til det forestående revisionsarbejde i organisationer, der følger ISO/IEC 27001 og 27002. Her får vi nemlig en mapping af foranstaltninger fra den eksisterende ISO/IEC 27002:2013 til den nye udgave; ISO/IEC 27002:2022. Dermed et fuldt overblik over, hvor en given foranstaltning er endt, hvad enten den er bibeholdt, opsplittet eller er smeltet sammen med øvrige foranstaltninger²⁵.

²³ Mapping af minimumssikkerhedskrav for operatører af væsentlige tjenester (OES'er) til internationale standarder, NIS-direktivet: <https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services>.

²⁴ Det er vigtigt at notere sig, at de nuværende attributter er ikke en udtømmende liste, ligesom organisationer heller ikke er forpligtet til at benytte de nuværende fem.

²⁵ Anneks B vil derfor gøre arbejdet med opdateringen af organisationers SoA-dokument til en noget mere håndgribelig opgave.

5. Samlet vurdering

Med 2022-udgaven af ISO/IEC 27002 er der fundet et nyt sæt byggeklodser frem. Den nye tematiske struktur vil utvivlsomt forblive et debateme, både i forhold til om alternative perspektiver havde været mere værdifulde og i overvejelser af, om de adfærdsmæssige og/eller fysiske temaer burde sløjfes og indarbejdes i de øvrige temaer. Imidlertid bør tematikken ses i sammenhæng med anvendelse af nye attributter og annekser, som netop giver organisationer frihed til at benytte alternative perspektiver til tema-strukturen²⁶. Hertil kommer, at de mange attributter giver en større indsigt i de enkelte foranstaltningers egenskaber, hvilket må forventes at blive en hjælp til at kvalificere foranstaltningernes relevans og værdi for forretningen. På den måde kan standarden blive et mere anvendeligt værktøj, når investeringer i informationssikkerhed skal forklares og forstås af topledelsen. Det bliver med de overordnede temaer nemmere at forklare sammenhænge mellem konkrete sikkerhedstiltag og organisationens målsætninger for informationssikkerhed. Derudover vurderes de nytilkomne og mange sammenlagte foranstaltninger at have skabt en mere aktuel og anvendelig standard, i og med at indholdet formentlig lettere kan spejles i de processer og retningslinjer, som organisationer i dag driver.

²⁶ Et ønske til næste revision ville være at tage spædestikket dybere i forhold til anvendelsen af attributter, fx ved at inkorporere kompetencekrav fra fx ISO/IEC 27021 (kompetencekrav) eller DS EN 16234-1 (e-Competence Framework).

Har du spørgsmål?

Hvis du har spørgsmål eller ønsker at vide mere om standarderne for informationssikkerhed, er du velkommen til at tage kontakt til:

Standardiseringskonsulent, Astrid Bækby Knudsen

E: abk@ds.dk

T: 39 96 62 06

eller

Seniorkonsulent Berit Aadal

E: baa@ds.dk

T: 39 96 62 96

Dette whitepaper er udarbejdet af Anders Linde, der er ekspert og ekstern underviser i informationssikkerhed hos Dansk Standard.