Small Business Standards

European DIGITAL SME Alliance

VEJLEDNING TIL SMV'ER VEDRØRENDE

IMPLEMENTERING AF ISO/IEC 27001

OM STYRING AF INFORMATIONSSIKKERHED

European Commission

EFTA

Formand: Fabio Guasconi

Koordinator:
Guido Sabatini

Eksperter:

Georgia Papadopoulou

George I. Sharkov

David Bulavrishvili

Sergio Oteiza

Holger Berens

Sebastiano Toffaletti

Nanuli Chkhaidze Yuri

V. Metchev Thorsten

Dombach Alexander

Häußler

FORORD

European DIGITAL SME Alliance (DIGITAL SME) er Europas største netværk af små og mellemstore IKT-virksomheder, og repræsenterer omkring 20.000 digitale SMV'er. Det er et samarbejde mellem 28 nationale og regionale SMV-organisationer fra EU's medlemsstater og nabolande, og har til formål at placere digitale SMV'er centralt på dagsordenen i EU.

DIGITAL SME er medlem af Small Business Standards (SBS), den europæiske interesseorganisation, der repræsenterer SMV'er omkring standardisering, jf. bilag III til EU-forordning 1025/2012. For at komme videre med implementeringen af SBS' arbejdsprogram for 2017, som er samfinansieret af Europa-Kommissionen og Den Europæiske Frihandelssammenslutning, har DIGITAL SME udviklet denne vejledning til SMV'er om implementering af ISO/IEC 27001 standarden om styring af informationssikkerhed.

Denne vejledning er udarbejdet af arbejdsgruppen "WG27K" under DIGITAL SME. WG27K består af eksperter med viden om standardisering inden for ledelsessystemer til styring af informationssikkerhed, og viden om SMV'ernes behov på dette område. Eksperterne blev indstillet af SMV-organisationer fra forskellige EU-lande, og blev udvalgt ud fra deres kompetencer for at sikre diversitet i sammensætningen af arbejdsgruppen. SBS og DIGITAL SME er ophavsmænd til denne gratis og offentligt tilgængelige vejledning.

INDHOLDSFORTEG-

1. Introduktion til cybersikkerhed

I dag er information et kerneprodukt for de fleste organisationer, og for mange er det deres eneste produkt. Andre organisationer er stærkt afhængige af at behandle information for at opfylde deres forretningsformål.

Men der er mennesker med ondsindede hensigter, der prøver at vende behovet for information til deres egen fordel. Vi har for nylig set mange eksempler på deres ulovlige aktiviteter, såsom ransomware-angreb (WannaCry, Petya), læk af personoplysninger fra store virksomheder (f.eks. Equifax) og læk af efterretningsorganers spionværktøjer.

Efterhånden som antallet af trusler øges, bliver organisationer nødt til at tænke mere over, hvordan de kan beskytte den information, de behandler, f.eks. ved at træffe disse enkle forholdsregler:

- implementere adgangskoder til computere og systemer
- installere antivirussoftware på slutbrugernes arbejdsstationer og servermiljøer
- deaktivere USB-flashdrev i organisationen
- anskaffe mere avancerede og dyrere løsninger

Mens mange tiltag beskytter systemerne effektivt, kan andre være spild af både økonomiske og menneskelige ressourcer. Dette skyldes ikke nødvendigvis, at det enkelte værktøj er dårligt eller ikke fungerer. Det afgørende er at vælge de værktøjer, der er mest relevante for ens forretning, finde ud af, hvor meget de koster, og hvordan man implementerer dem effektivt.

HVORFOR ER DER BRUG FOR EN VEJLEDNING TIL SMÅ OG MELLEMSTORE VIRKSOMHEDER (SMV'ER)?

- **SMV'er udgør størstedelen af virksomhederne i Europa, og beskæftiger flere mennesker. De ses som en drivkraft for innovation i Europa.**
- **De fleste SMV'er undervurderer risikoen for cyberangreb, fordi de tror, at den information de behandler, ikke er værd at stjæle.**
- **Imidlertid har små virksomheder mange digitale aktiver sammenlignet med en individuel bruger, og de har ofte færre sikkerhedsforanstaltninger end store organisationer.**

På grund af kompleksiteten i informationsmiljøet og de komplicerede informationsstrømme forstår mange organisationer nu, at de har brug for særligt kvalificeret personale såsom informationssikkerhedschefer, cybersikkerhedseksperter og informationssikkerhedsudvalg. Nogle opretter også særlige afdelinger/teams for informationssikkerhed og håndtering af cybersikkerhedshændelser. Alligevel er mange organisationer usikre på, om deres investeringer i beskyttelsesforanstaltninger er umagen værd.

Huller i cybersikkerheden kan føre til alvorlige problemer, som groft kan inddeles i tre hovedkategorier:

- Tab af tilgængelighed, hvilket hæmmer forretningsaktiviteterne
- Tab af fortrolighed, der forårsager skade på organisationens omdømme eller endda fører til retssager
- Tab af integritet, hvilket fører til brug af forkerte eller endda forfalskede data

Cybersikkerhed er nøglen til at beskytte aktiverne i organisationer uanset type og størrelse. Men hvad er cybersikkerhed egentlig?

1.1 Definition af cybersikkerhed

Der findes ingen formel definition på **cybersikkerhed,** men i betydning ligner termen **informationssikkerhed**. Cybersikkerhed anses ofte for at omfatte de mest tekniske aspekter af informationssikkerhed – som i sig selv sigter mod at beskytte oplysninger, der kan opbevares på papir, på computere eller endda af mennesker. Cybersikkerhed handler primært om at beskytte elektronisk lagret information og behandlingen deraf. Det defineres som en tilstand, hvor risikoen forbundet med brug af informationsteknologi, under hensyntagen til eventuelle trusler og sårbarheder, reduceres til et acceptabelt niveau ved hjælp af passende foranstaltninger. Det menneskelige element, inklusive nationale interesser, spiller også en stadig vigtigere rolle for cybersikkerhed. Så cybersikkerhed kræver anvendelse af passende foranstaltninger til at beskytte fortroligheden, integriteten og tilgængeligheden af information og informationsteknologi.

1.2 Begreber og definitioner

For bedre at forstå denne vejledning følger her definitioner af de mest anvendte og specifikke begreber:

Aktiv
En komponent, som har værdi for organisationen. Der findes mange typer aktiver, herunder data, hardware, software, tjenesteudbydere, personale og fysiske lokationer.

Angreb
Tilsigtet form for fare, f.eks. en uønsket eller uberettiget handling med det formål at opnå fordele eller skade en tredjepart ved at udføre en handling på et sæt aktiver.

Tilgængelighed
Egenskaben at være tilgængelig og kunne bruges umiddelbart af en autoriseret enhed.

Fortrolighed
Det kun at gøre information tilgængelig eller videregive den til autoriserede personer, enheder eller processer.

Kontrol
En foranstaltning, der kan ændre en risiko. Kontroller omfatter processer, politikker, enheder, praksisser eller andre handlinger, der effektivt kan ændre risikoen.

Integritet
Nøjagtighed og fuldstændighed.

Informationssikkerhed
Bevarelse af fortrolighed, integritet og tilgængelighed af information.

Risiko (informationssikkerhed)
En informationssikkerhedsrisiko, som kan indebære, at trusler udnytter et informationsaktivs sårbarheder og derved skader en virksomhed.

Risikovurdering (informationssikkerhed)
Overordnet proces for risikoidentifikation, risikoanalyse og risikovurdering.

Risikohåndtering (informationssikkerhed)
Proces for ændring af risiko – omfatter normalt undgåelse, deling, begrænsning eller accept af en given risiko.

Trussel
Potentiel årsag til en uønsket hændelse, som kan resultere i skade.

Sårbarhed
Svaghed i et aktiv eller en kontrol, der kan udnyttes af en eller flere trusler.

2. Anvendelsesområde

Denne vejledning er skrevet til og er relevant for SMV'er, der er afhængige af teknologiske aktiver. Retningslinjerne i vejledningen kan implementeres af organisationer uanset størrelse og kompleksitet.

Vejledningen beskriver med udgangspunkt i indholdet i ISO/IEC 27001 en række praktiske aktiviteter, der kan hjælpe SMV'er med at etablere eller hæve deres informationssikkerhedsniveau. Dette vil styrke deres forretning og gøre det lettere for dem at indgå partnerskaber på deres lokale marked og EU-markederne.

Alle de nævnte aktiviteter sikrer en livscyklus for informationssikkerhed i organisationen. Dette omfatter etablering, planlægning, implementering, drift og forbedring af alle relaterede processer baseret på risikokulturen og løbende forbedring.

3. Styring af informationssikkerhed i en SMV

3.1 Trin 1: Etablering af grundlaget for informationssikkerhed

Styring af informationssikkerhed har meget til fælles med andre vigtige indsatser i en organisation. Før man tager hul på en aktivitet, er det en god ide at beslutte, hvad formen skal være, hvad tidshorisonten er, og hvem der skal inddrages. De allerførste, der skal deltage, er en ekspert på området og topledelsen: De skal etablere grundlaget for alle de andre aktiviteter.

Topledelsen skal involveres i dette første trin som ansvarlig for at etablere grundlaget for informationssikkerhedsledelse. Ansvaret for denne opgave ligger hos informationssikkerhedschefen. Systemejere og informationsejere bør også holdes opdateret om opgavens forløb. Nedenfor følger en detaljeret beskrivelse af det personale, der kan tildeles en rolle i virksomhedens informationssikkerhed.

3.1.1 Trin 1.1 Tildeling af roller og ansvar

Det er vigtigt i enhver virksomhed og for enhver aktivitet, at fordele roller og ansvar korrekt. Nystartede eller små virksomheder betragter ofte informationssikkerhed som en selvstændig proces og en proces, de ikke behøver at beskæftige sig med. Nogle vil måske endda helt ignorere den.

Når man beslutter at træffe foranstaltninger til at etablere eller ændre styringen af informationssikkerhed i en organisation, er det vigtigt at definere og formalisere roller og ansvar, før man går videre. Alle efterfølgende trin og roller har angivelse af, hvordan de skal involveres efter RACI-modellen: (Responsible (udførende), Accountable (ansvarlig), Consulted (konsulteres), Informed (informeres)) i parentes.

De vigtigste roller og relaterede ansvarsområder i forbindelse med styring af informationssikkerheden er overordnet beskrevet i dette afsnit. Bemærk, at mindre organisationer kan give mere end én rolle til den samme person eller outsource disse roller (bortset fra topledelsen). Som en forudsætning for at anvende denne vejledning skal alle organisationer specifikt og formelt tildele informationssikkerhedsroller og -ansvar i overensstemmelse med deres egen struktur og kultur.

Topledelsen
Det endelige ansvar for informationssikkerhedsledelse ligger hos topledelsen, som er en del af den overordnede styring af organisationen. Den primære opgave for topledelsen er at sørge for at informationssikkerheden understøtter opfyldelsen af forretningens mål, ved at sikre, at der er overensstemmelse med organisationens værdier, passende ressourcestyring og tilsvarende resultatmålinger. Topledelsen behøver ikke at kende hvert eneste aktiv i organisationen, men forventes at have en generel forståelse af de kritiske aktiver og deres værdi for virksomhedens drift.

Topledelsen omfatter normalt den administrerende direktør, driftsdirektøren eller bestyrelsen, afhængigt af organisationens struktur. I forbindelse med arbejdet med denne vejledning skal det besluttes, hvem der skal tildeles disse roller.

MEDARBEJDERE, DER ER TILDELT DE FORSKELLIGE INFORMATIONS-SIKKERHEDSROLLER, SOM ER RELEVANTE I ORGANISATIONEN, SKAL NOTERE OG ANERKENDE DERES ANSVAR OG OPGAVER.

En RACI-matrix kan hjælpe med til at klarlægge ansvarsfordelingen og kan omfatte følgende:

- **Bestemmelse af informationssikkerhedskrav og -klassificering**
- **Resultat af risikovurdering**
- **Definition, implementering og vedligeholdelse af sikkerhedsforanstaltninger**
- **Accept af residual risiko**
- **Dokumentation af systemsikkerhed (normer, procedurer osv.)**
- **Udarbejdelse og opdatering af sikkerhedspolitik**
- **Overvågning af systemsikkerhed**
- **Planer for forbedring af sikkerhed**
- **Planer for bevidstgørelse og træningsplaner**
  Forretningskontinuitetsplaner

For hver af disse opgaver skal følgende ansvar tildeles de identificerede roller:

- **Ansvarlig (benævnt "R" (Responsible)) for at udføre opgaven. Der skal være mindst én person, der er ansvarlig for hver opgave (som muligvis uddelegerer den);**
- **Ansvarlig (benævnt "A" (Accountable)), som skal godkende, at opgaven er udført korrekt**
- **Konsulteres (benævnt "C" (Consulted)), hvis mening kan være påkrævet for at udvikle opgaverne i en tovejskommunikation: De anses typisk for at være eksperter;**
- **Informeres (benævnt "I" (Informed)), der holdes ajour om opgaven forløb i en envejskommunikation.**

Styregruppe for informationssikkerhed
I nogle tilfælde kan SMV'er oprette en styregruppe for informationssikkerhed bestående af interessenter fra alle organisationens vigtigste afdelinger. Det er god praksis at have et kommissorium, der hovedsageligt fungerer som et redskab til at opnå enighed blandt de vigtigste beslutningstagere. Styregruppen for informationssikkerhed kan arbejde sammen med topledelsen og vil være ansvarlig for audit- og overvågningsaktiviteter.

Når der nedsættes en styregruppe for informationssikkerhed, er det en god ide at involvere de nederste ledelsesniveauer, der rapporterer til organisationens topledelse, samt at afholde kvartalsmøder. Komitéen bør mødes for at behandle forskellige spørgsmål vedrørende informationssikkerhed, såsom:

- sikkerhedsnormer og proceduregodkendelse
- gennemgang af risikoanalyse og plan for risikohåndtering
- auditresultater og relaterede handlinger
- overvågning af informationssikkerhedsplanen
- informationssikkerhedsmål og resultatindikatorer
- planlægning af kursusaktivitet for awareness og træning
- respons ved nødsituationer

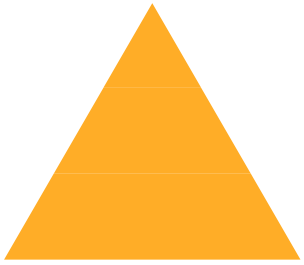
Informationssikkerhedsansvarlig/-chef
Selv om informationssikkerhed vedrører alle afdelinger i organisationen, bliver det stadig mere almindeligt at have en informationssikkerhedschef, der koordinerer relevante aktiviteter. Denne rolle kan udføres af enhver højtstående medarbejder (f.eks. IT-chefen eller teknologidirektøren) med solid viden om informationsstrømme.

Eftersom informationssikkerhed sjældent er en generel ledelsesdisciplin, orienterer informationssikkerhedschefen typisk topledelsen om vigtige aspekter, inden informationssikkerhedsstrategien accepteres. At få topledelsens opbakning er afgørende for informationssikkerhedsarbejdet. En af de vigtigste aktiviteter i denne forbindelse er afstemning af forretnings- og informationssikkerhedsmålene. Andre ansvarsområder omfatter ofte: opstilling af budgetter, anvendelse af risk/benefit-modeller til risikovurdering og -håndtering, udarbejdelse af informationssikkerhedspolitikker og -procedurer samt gennemgang af resultaterne af overvågningsaktiviteter.

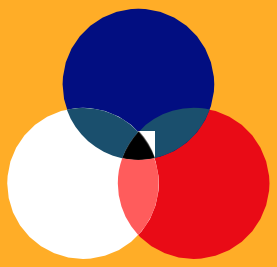
Informationssikkerhedschefen er normalt også ansvarlig for at sikre, at medarbejderne er bevidste om informationssikkerhed, og eventuelt også for etablering af kommunikationskanaler og rapportering. Hvor god en informationssikkerhed organisationen skaber afhænger meget af kommunikation, både internt og eksternt.

Den informationssikkerhedsansvarlige/informationssikkerhedschefen spiller en vigtig rolle i anvendelsen af denne vejledning og bør vælges på grundlag af sine kompetencer og erfaringer på området. Profilerne, hvis de kun beskæftiger sig med dette, kan spænde fra sikkerhedschef til direktør for. Der findes flere oplysninger om faglige profiler og de relaterede kompetencer i CWA 16458 om professionelle profiler i europæiske IKT'er.

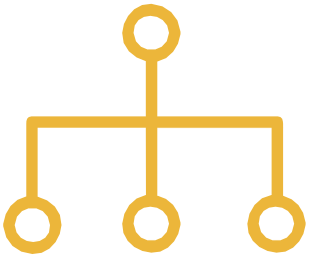
FORDELE VED AT OPRETTE EN STYREKOMITÉ FOR INFORMATIONSSIKKERHED:



Bedre koordinering mellem forskellige områder af organisationen



Mere effektiv udbredelse af en informationssikkerhedskultur, da flere afdelinger er direkte involveret



Bedre overblik når der skal træffes beslutninger, da alle relevante områder afhænger af komitéen

Etablering af en procedure for gennemgang og tjek af informationssikkerhedsstatus og -udvikling

FØLGENDE SKAL OVERVEJES VED NEDSÆTTELSE AF EN STYREGRUPPE FOR INFORMATIONSSIKKERHED:

- Hver afdeling bør være repræsenteret af den relevante beslutningstager for at undgå ubalance mellem forskellige afdelinger, hvis nogle områder ikke er repræsenteret af deres øverste ledere
- Mødedagsordener skal planlægges og udsendes på forhånd
- Møderne skal afholdes regelmæssigt (f.eks. hver tredje måned) og systematisk
- Der skal fastlægges møderegler, herunder hvem der leder mødet, og hvordan man løser potentielle konflikter
- Relevante beslutninger om informationssikkerhed bør træffes i denne komité
- Tidsplaner skal overholdes

Systemejere og informationsejere
I meget strukturerede organisationer kan der muligvis skulle udpeges medarbejdere til at udføre daglige opgaver for at beskytte de informationssystemer, de kontrollerer. Dette er "systemejere". De forretningsansvarlige, der er ansvarlige for processer og data, skal dog være involveret i at fastlægge kravene til beskyttelse deraf, uanset informationssystemerne. Dette er "informationsejere". Begge kategorier skal hjælpe organisationen ved at sikre, at der er etableret informationssikkerhedskontroller, som fungerer.

Normalt har ejerne ret til at foretage ændringer i det, de ejer, f.eks. systemforbedringer, oprette genveje osv. Disse beslutninger skal dog altid tage hensyn til konsekvenserne for informationssikkerheden. For at denne model skal fungere, skal det gøres klart, hvem system- og informationsejerne i organisationen er. Til en start involverer dette IT-chefen og driftsdirektøren. Derudover vil organisationen ofte skulle gøre en indsats for at finde system- og informationsejere på de lavere niveauer i ledelseshierarkiet – hvem træffer beslutningerne om forbedring af aktiver eller tastatur-genveje? Dette kræver uddelegering af beslutninger og en konsekvent kultur.

Personale
Vellykket informationssikkerhedsledelse kræver træning og uddannelse af personalet. Medarbejdere og leverandører skal have fuld forståelse af baggrunden for kontrolmiljøet omkring dem, så de kan være med til at opretholde informationssikkerheden på det rigtige niveau og ikke kompromittere den.

Medarbejdere og leverandører skal være i stand til at genkende usædvanlig opførsel og hurtigt gøre informationssikkerhedschefen opmærksom på enhver bekymring, så organisationens tab minimeres. Ofte er det medarbejdere og leverandører, der bliver mål for angreb. Derfor vil uddannede medarbejdere styrke det samlede informationssikkerhedsmiljø betydeligt. Disse medarbejdere kan muligvis også omsætte denne viden og ekspertise til organisationskultur.

3.2 Trin 2: Hvad skal beskyttes?

Fra dette kapitel vil der i denne vejledning blive givet eksempler (f.eks. figurer, tabeller osv.), der illustrerer de enkelte opgaver, der foreslås til sikker styring af information i en organisation. Disse eksempler hjælper læseren med at forstå vejledningen.

Før virksomheden iværksætter nogen som helst informationssikkerhedsforanstaltning, skal den skaffe sig et klart overblik over, hvad der virkelig har værdi for virksomheden. Dette defineres normalt som **aktiver**, og de kan generelt kategoriseres som enten information (se *Trin 2.1*), som typisk er immaterielle aktiver, og andre aktiver (se *Trin 2.2*), som typisk er materielle.

Hovedmålet med denne øvelse er, at identificere de vigtigste aktiver som organisationen kontrollerer, og som skal beskyttes. Dette er især vigtigt, når man fastlægger forbindelserne mellem aktiver, og når man definerer ansvar.

Typiske roller: topledelse (A), informationsejere (C), systemejere (C), informationssikkerhedschef/-ansvarlig (R).

3.2.1 Trin 2.1 Hvilken information bruger vi?

Det er nyttigt at udarbejde et **kort over aktiver**, der starter med de immaterielle aktiver: Organisationens information.

Top-down-tilgang

En organisation kan vælge at anvende en "top-down-tilgang", hvor information (de hvide felter nedenfor) identificeres, når den bevæger sig mellem processer (de farvede felter nedenfor).

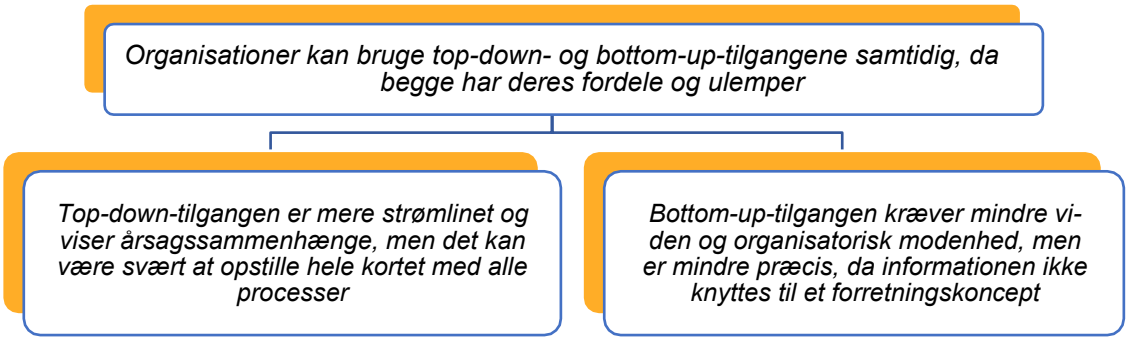
Figur 1: Eksempel på kort over aktiver med udgangspunkt i hypotetisk information i en organisation

For at få mest muligt ud af en top-down-tilgang skal organisationen have en god forståelse for processerne, herunder være opmærksom på deres indhold, vide, hvem der er ansvarlig for hver proces, osv. Forbindelsen mellem organisationens aktiviteter og information kan vises ved at starte med et fugleperspektiv på processerne og så bevæge sig nedad til informationsaktiverne. Informationsejere (normalt drifts- eller afdelingsledere) har det bedste udgangspunkt for at klassificere og vurdere relevansen af informationen i organisationen. Det er en god ide at afholde en kort samtale med hver enkelt informationsejer for at få et godt overblik over den information, organisationen håndterer.

Bottom-up-tilgang

Top-down-tilgangen kræver en god forståelse af de organisatoriske processer, hvorimod dette ikke er nødvendigt med en "bottom-up-tilgang". Sidstnævnte kan bruges af enhver organisation, uanset modenhedsniveau. Når en organisation anvender en bottom-up-tilgang, er det mest hensigtsmæssigt at besvare spørgsmålet "Hvilken slags information håndterer organisationen generelt?". Dette spørgsmål kan stilles til den/de personer, der har et overordnet overblik over organisationen. Nedenstående enkle liste kan bruges til at sikre, at man får al den vigtige information med:

a) personoplysninger (f.eks. navne, adresser, CPR-numre, lønningslister)
b) følsomme personoplysninger (f.eks. diagnoser, politisk overbevisning, betalingskortdata)
c) strategiske virksomhedsdata (f.eks. forretningsplaner, prognoser, budgetredegørelser før offentliggørelse)
d) projekt-/designdata (f.eks. produktdesign, beskyttet kildekode)
e) andre virksomhedsdata (f.eks. overvågningsdata, produktionsstatistik, skatteoplysninger)



Når kortet over aktiver er udarbejdet, bør organisationen have fået en god forståelse af sine informationsaktiver på et begrebsmæssigt niveau, uanset hvilket lagrings- eller behandlingsudstyr der bruges.

3.2.2 Trin 2.2 Hvilke andre aktiver bruger vi?

Identificeret information kan gemmes, behandles eller overføres ved hjælp af flere andre aktiver, for det meste (men ikke udelukkende) teknologiske. Disse aktiver er normalt lag af software, der kører på informationssystemer, men kan også være i papirform og på diske eller tjenester, der leveres af eksterne tjenesteudbydere. Det er normalt nødvendigt at bruge en bottom-up-tilgang for at identificere dem korrekt, dvs. involvere IT-personale og applikationsadministratorer (uanset om de formelt er udpeget som systemejere). Det anbefales kraftigt i hvert fald at overveje de nøgleaktiver, der hører til følgende aktivkategorier:

1) slutpunkter (laptops, desktops, tablets, smartphones), servere og apparater
2) slutbrugersoftware (bortset fra programpakker til kontorautomatisering eller operativsystemer)
3) tjenesteudbydere (herunder personale-, ejendoms-/hosting- og cloud-udbydere)
4) personale (direkte ansatte eller leverandørers medarbejdere)
5) fysiske lokationer (direkte ejede kontorer og computerrum)

Disse elementer kan også undersøges i starten i en top-down-tilgang i samarbejde med informationsejerne som beskrevet i det foregående trin, lige efter at man har defineret information relateret til processer, og derefter uddybes med systemejerne. På baggrund af eksemplet ovenfor kunne vi ende med en struktureret liste som denne:

SOFTWARE	HARDWARE	PERSONALE	LEVERANDØRER	LOKATIONER
CRM-software	Produktionsservere	Internt personale	Cloud-udbyder	Hovedkontorer
ERP-software	Testservere		Teknologiudbyder	
Delte mapper	Personalets pc'er			
	Personalets smart-phones			

Figur 2: Eksempel på et kort over aktiver med andre vigtige aktiver end information i en given organisation

3.2.3 Trin 2.3 Hvad er forbindelsen mellem information og andre aktiver?

Når alle nøgleaktiver er identificeret, skal det fastlægges, hvilke aktiver der bruges til hvilken information. Dette er en enkel, men effektiv metode til at finde ud af, hvad der skal beskyttes, og senere også, hvor meget det skal beskyttes. For at gøre dette kan der oprettes en simpel matrix som den nedenfor. Her viser de udfyldte celler en forbindelse mellem aktiver og information, mens de tomme celler viser, at der ikke er nogen forbindelse.

	Generelle kundedata	Reklamationer	Kilde-kode	Design-specifikationer	Anmodninger om tilbud
CRM-software					
Produktionsservere					
Testservere					
Personalets pc'er					
Personalets smart-phones					
Delte mapper					
ERP-software					
Internt personale					
Cloud-udbyder					
Teknologiudbyder					
Hovedkontorer					

Tabel 1: Eksempel på matrix til identifikation af forbindelsen mellem information og andre aktiver

Når disse forbindelser er klarlagt, er kortet over aktiver færdigt. Det vil være til stor hjælp i de følgende trin. Naturligvis kan der indsamles mere information for hvert aktiv, så man ender med en komplet aktivopgørelse, der kan bruges til at styre dem alle bedre. Husk at kortet over aktiver skal opdateres løbende, ellers bliver det hurtigt mindre brugbart.

3.3 Trin 3: Vurdering af informationssikkerhedsrisici

Risikovurdering af informationssikkerheden handler om, at finde ud af på forhånd, hvad der muligvis kan gå galt med aktiverne og medføre en negativ indflydelse på virksomhedens pengestrømme, juridiske forpligtelser eller omdømme. Dette trin er afgørende for at forstå de trusler, organisationen står over for, så den kan iværksætte passende kontroller for at undgå, forhindre eller begrænse dem eller sikre, at aktiver kan retableres, hvis truslerne bliver virkelighed. Ved at prioritere risici kan en organisation koncentrere sine defensive ressourcer, hvor de største tab mest sandsynligt vil ske, og dermed i sidste ende optimere effektiviteten af disse ressourcer.

Typiske roller: topledelsen/styregruppen for informationssikkerhed (A), informationsejere (C), systemejere (C), informationssikkerhedschef/-ansvarlig.

3.3.1 Trin 3.1 Hvad er værdien af aktiver?

For at sikre at kortet over aktiver (se *Trin 2.3*) kan bruges i risikovurderingsprocessen, er der ét vigtigt element, der skal med: en vurdering af vigtigheden af hvert aktiv i organisationen.

Den enkleste måde at foretage denne vurdering på er at starte fra den definerede information og tage stilling til mindst to af de vigtigste sikkerhedsrelaterede egenskaber for information: **Tilgængelighed og fortrolighed**. Integritet kan tilføjes, men hvis det skal være helt enkelt, kan integritet anses for at ligge tæt op ad tilgængelighed. Der skal foretages en grundlæggende vurdering af den information, der blev afdækket i *Trin 2.1*, hvor hver informationsejer bruger nedenstående tabel som reference og tildeler en værdi for tilgængelighed og fortrolighed til hver enkelt type information.

	Lav værdi	**Høj værdi**
Tilgængelighed (T)	Vil det få store konsekvenser for organisationens forretningsaktiviteter eller omdømme, hvis denne information ikke er tilgængelig?	
	Nej	**Ja**
Fortrolighed (F)	Vil uautoriseret formidling af denne information skade organisationens konkurrenceevne eller overtræde vigtige love/kontraktlige forpligtelser?	
	Nej	**Ja**

Tabel 2: Vurdering af aktiver med hensyn til tilgængelighed og fortrolighed

Anvendelse af tabellen ovenfor på eksemplet kunne give følgende værdier:

Gene-relle kun-dedata	Reklama-tioner	Kilde-kode	Design-specifikatio-ner	Anmod-ninger om tilbud	Indkøbs-ordrer
T: lav F: høj	T: lav F: lav	T: lav F: høj	T: lav F: høj	T: høj F: lav	T: lav F: høj

Tabel 3: Eksempel på vurdering af information med hensyn til tilgængelighed og fortrolighed

Da alle de materielle aktivers værdi er relateret til den information, de lagrer, behandler eller overfører, kan denne første vurdering overføres til disse aktiver, i kortet over aktiver, som vist nedenfor.

	Gene-relle kunde-data	Reklama-tioner	Kilde-kode	Design-specifi-katio-ner	Anmod-ninger om tilbud	
	T: lav F: høj	T: lav F: lav	T: lav F: høj	T: lav F: høj	T: høj F: lav	
CRM-software						**T: lav, F: høj**
Produkti-onsservere						**T: høj, F: høj**
Testservere						**T: lav, F: høj**
Personalets PC'er						**T: høj, F: høj**
Personalets smartphones						**T: lav, F: høj**
Delte mapper						**T: lav, F: høj**
ERP-software						**T: høj, F: lav**
Internt personale						**T: høj, F: høj**
Cloud-udbyder						**T: høj, F: høj**
Teknologiudbyder						**T: høj, F: høj**
Hovedkontorer						**T: høj, F: høj**

Tabel 4: Eksempel på matrix til afdækning af forbindelsen mellem aktiver og deres vurdering med hensyn til tilgængelighed og fortrolighed

Dette færdige og forbedrede kort over aktiver giver et godt svar på spørgsmålet om, hvad der skal gives informationssikkerhedsbeskyttelse til, og hvor meget beskyttelse der skal gives, afhængigt af aktivets egentlige rolle.

For at vurdere aktiverne kan der anvendes forskellige skalaer (vurderingen kan f.eks. være lav/mellem/høj). For at forbedre en sådan analyse kan virkningen af et sikkerhedsbrud vurderes under hensyntagen til yderligere kriterier som f.eks.:

- **Lovkrav**
- **Økonomiske eller kommercielle interesser**
- **Omdømme (offentligt image)**
- **Sikkerhed**

3.3.2 Trin 3.2 Vurdering af den type kontekst, organisationen arbejder i

En grundig forståelse af det miljø, som organisationen opererer i, er af central betydning, når man fastlægger krav til informationssikkerhed. ENISA, Det Europæiske Agentur for Net- og Informationssikkerhed, har udviklet en trusselsmodel for cybersikkerhed, som kan bruges til at tage stilling til alle de trusler, som organisationen sandsynligvis står over for. ENISA's model har følgende trusselskategorier:

a) Katastrofe (f.eks. jordskælv, oversvømmelse, brand)
b) Afbrydelse (f.eks. strejke, væsentlig utilgængelighed)
c) Fysisk angreb (f.eks. tyveri, sabotage)
d) Juridisk (f.eks. overtrædelse af regler, retslig afgørelse)
e) Utilsigtet skade (f.eks. læk af information, tab af enhed, f.eks. telefon/laptop)
f) Nedbrud/funktionsfejl (f.eks. i hardware)
g) Ondsindet handling/misbrug (f.eks. malware, social engineering, afkodning af adgangskode)
h) Aflytning/opsnapning/kapring (f.eks. spionage, "man in the middle"-angreb)

Relevansen af disse trusler skal vurderes på baggrund af historiske hændelsesdata (hvis disse data er tilgængelige) og personalets erfaring. En sådan vurdering vil som minimum kunne fastslå, hvorvidt f.eks. følgende forhold gælder for organisationens miljø:

1) Hvor udsatte er organisationens lokaler for naturkatastrofer eller -begivenheder (oversvømmelser, brande, jordskælv)?
2) Hvor udsatte er organisationens lokaler for afbrydelser (internetforbindelser, strømafbrydelser, strejker)?
3) Hvor stor er tilliden til personalet (lav personaleomsætning, ingen uro, holdånd)?
4) Hvor stærkt påvirker regler eller kontraktkrav organisationen?
5) Hvor udsat er organisationen for menneskelige fejl?

6) Hvor afhængig er organisationen af eksterne udbydere?
7) I hvilket omfang eksponerer IKT-tjenester organisationen for internettet?
8) Hvor vigtigt er organisations offentlige omdømme?

DE RELEVANTE EJERE AF INFORMATION OG AKTIVER TIL AT BESVARE DISSE SPØRGSMÅL KAN VÆRE:

- **IT-CHEF vedrørende trusselskategorierne: Utilsigtet skade, katastrofe, nedbrud/funktionsfejl, afbrydelser, aflytning/opsnapning/kapring, ondsindet handling/misbrug**
- **SIKKERHEDCHEF/FACILITY MANAGER vedrørende trusselskategorierne: Fysisk angreb, katastrofe, nedbrud/funktionsfejl**
- **JURIDISK CHEF vedrørende trusselskategorien: Juridisk**
- **HR-CHEF vedrørende trusselskategorien: Afbrydelser**

Svarene på disse spørgsmål (som udtrykkes i følgende værdier: Høj/Lav/Ingen) fås ved at konsultere de relevante ejere af information og aktiver, og kan virkelig hjælpe til at bestemme de sandsynlige trusler, som organisationen står over for, ved at relatere punkterne til hinanden (1 til a, 2 til b osv.). Disse overvejelser bør ske uden at tage hensyn til de forholdsregler, som organisationen allerede har truffet.

Denne vejledning kan også bruges til at håndtere andre typer trusler eller tilføje trusler til ENISA-truslerne. Dette kræver bare en ny kortlægning af kontrollerne.

Hvis et spørgsmål svarende til en given trussel har fået en anden værdi end "Ingen", og hvis den pågældende trussel gælder for bare et af de aktiver, der er anført i tabellen herunder, skal truslen altid behandles som en risiko for organisationen.

	Katastrofe	Afbrydelser	Fysisk	Juri-	Utilsigtet skade	Ned- brud/funkti-	Ondsindet handling/mis-	Aflytning/op- snapning/kap- ring
Hardware	X		X		X	X	X	
Software				X	X	X	X	X
Tjene- steudby- dere		X		X		X		X
Personale	X	X		X			X	X
Fysiske lokatio- ner	X		X					

Tabel 5: Eksempel på matrix, der bruges til at vurdere den type kontekst, som organisationen arbejder i

Hvis f.eks. svaret på spørgsmål 3) var "Lav", ville den tilsvarende trussel c) fysisk angreb gælde for aktiverne hardware og fysiske lokationer. I kortet over aktiver i eksemplet (figur 2) ville det dreje sig om produktionsservere, testservere, personalets PC'er, personalets smartphones og hovedkontorer.

3.3.3 Trin 3.3 Hvilke kontroller er allerede implementeret?

Informationssikkerhedskontroller er de vigtigste midler til at reducere risici. De kan virkelig gøre en forskel, hvis de implementeres rigtigt. Der findes ofte allerede flere kontroller, men mange flere kan være relevante, og de bør ikke kun betragtes fra det overordnede organisationsperspektiv, men også for de enkelte aktiver for at afdække eventuelle huller i beskyttelsen.

ISO/IEC 27001 Anneks A indeholder en omfattende liste over kontroller, som har til formål at hjælpe en organisation med at tjekke, om deres kontroller er fuldt dækkende. Denne liste er blevet forenklet for SMV'er i **Bilag A til denne vejledning,** med henvisning til de oprindelige kontroller i ISO/IEC 27001 Anneks A. For hver kontrol på listen markeres det, om den allerede anvendes fuldt ud eller ej (delvis anvendelse vil konservativt blive betragtet som manglende anvendelse) for hver gruppe af aktiver, der er relateret til information.

3.4 Trin 4: Udvikling, anvendelse og overvågning af informationssikkerhedskontroller

Så snart organisationen er fuldt ud klar over, hvad der skal beskyttes, og hvordan den i øjeblikket er beskyttet, kan der træffes beslutninger om, hvilke nye kontroller der skal implementeres, og hvilke der skal forbedres. Topledelsen/styregruppen for informationssikkerhed bør vurdere, hvad der skal gøres for at håndtere hver enkelt risiko, sammen med tidshorisont og finansiering af hver løsning. De fleste forslag kommer normalt fra informationssikkerhedschefen/den informationssikkerhedsansvarlige. De valgte beskyttelsesforanstaltninger skal være effektive og omkostningseffektive.

Typiske roller: topledelsen/styregruppen for informationssikkerhed (A), informationsejere (R), systemejere (R), personale (R), informationssikkerhedschef/-ansvarlig (R).

3.4.1 Trin 4.1 Afdækning af de kontroller, der skal implementeres, og udarbejdelse af en informationssikkerhedsplan

At beslutte, hvilke kontroller der skal implementeres i et specifikt miljø, er den vanskeligste beslutning overhovedet, når det drejer sig om informationssikkerhed. Ingen kombination af kontroller er perfekt til alle situationer, fordi det kan betyde uforholdsmæssigt store omkostninger, for mange kontroller samt uforudsigelige hændelser.

I overensstemmelse med de foregående trin og relevant god praksis foreslår denne vejledning i bilag A, at kontroller klassificeres i to hovedkategorier:

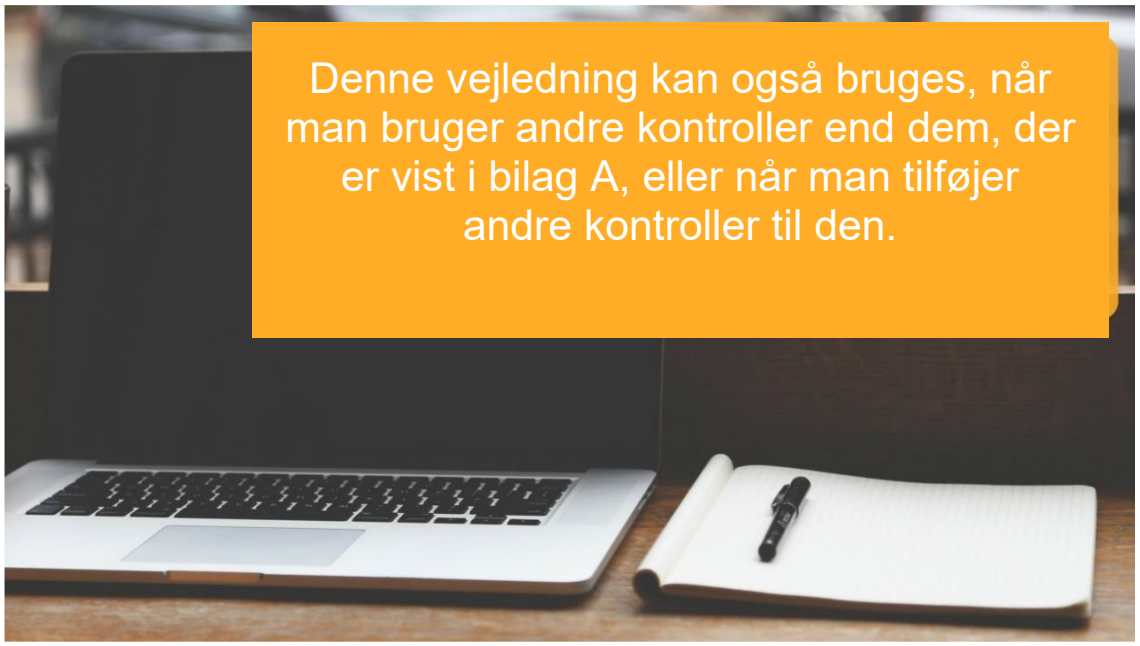
1) **basiskontroller** – kan bruges i alle situationer
2) **skønsmæssige kontroller** – kan bruges til at beskytte aktiver af høj værdi, som sandsynligvis er udsat for trusler

Basiskontroller beskrives i det første afsnit i bilag A (A.1), og medmindre særlige situationer opstår, skal de altid implementeres. Bilag X til denne vejledning er et godt eksempel på basiskontrol: **informationssikkerhedspolitik**. Når politikken er udarbejdet, skal den formelt godkendes af organisationens topledelse for at bestemme prioriteter og ressourcer for den pågældende organisation.

Andet afsnit i bilag A (A.2) indeholder en oversigt over skønsmæssige kontroller. Her forbindes hver kontrol med de trusler, som kontrollen begrænser i det tredje afsnit i bilag A (A.3). Hvis der ikke er angivet noget i den celle, der i afsnit A.3 angiver truslens værdi, begrænser kontrollen ikke truslen i væsentlig grad. Hvis værdien "Sekundær" er angivet, betyder det, at kontrollen til en vis grad begrænser truslen. Hvis værdien "Primær" er angivet, betyder det, at kontrollen i højere grad begrænser truslen. Da hvert aktiv har fået en værdi i *Trin 3.1* og er blevet forbundet med de relevante trusler i *Trin 3.2*, kan de således bruges til at beslutte, hvorvidt en kontrol skal anvendes eller ej. Hvis et aktiv har en høj værdi for fortrolighed eller tilgængelighed ELLER er en meget sandsynlig trussel, skal der kun anvendes kontroller, der er markeret som "Primær" for den specifikke trussel. Hvis et aktiv har både en høj værdi for fortrolighed eller tilgængelighed OG er en meget sandsynlig trussel, er det også værd at overveje de kontroller, der er markeret som "Sekundær" for den specifikke trussel.

F.eks. er personalets smartphones – som i tabel 4 er vurderet til "T:lav, F:høj" – hardware, og derfor er trusselsniveauet med hensyn til fysisk angreb "Lav". Alle kontroller, der er markeret som "Primær" ud for truslen om fysisk angreb, skal anvendes på personalets smartphones samt på basiskontroller. Det betyder:

- A2.06 Styring af flytbare medier
- A2.10 Fysisk sikkerhed
- A2.11 Beskyttelse mod miljøtrusler
- A2.12 Vedligeholdelse af udstyr
- A.2.16 Sikkerhedskopiering



Der bør **for hvert enkelt aktiv** foretages et tjek af de anvendte kontroller, der blev påvist i det forrige trin, og kontroller, der er resultatet af de tre ovennævnte kategorier. Hvis den aktuelle situation medfører en kontrol, der er mindre effektiv end anbefalet eller mangler, skal denne situation noteres og analyseres nærmere. Listen over disse kontroller danner grundlaget for en **informationssikkerhedsplan**, som giver organisationen mulighed for selektivt at forbedre sin informationssikkerhedsbeskyttelse. Informationssikkerhedsplanen skal indeholde flere elementer end en simpel liste over kontroller. Den kan eksempelvis indeholde et sæt handlinger med tilknyttede ejere, tidspunkter, omkostninger og andre oplysninger. Det kan faktisk gøres i noget så enkelt som et regneark med følgende felter:

Kode	*ID*
Kilde	*Kildeaktivitet*
Handlingsbeskrivelse	*Beskrivende tekst*
Ejer	*Funktion eller person*
Årsag	*Begrundelse for aktiviteten*
Prioritet	*Lav*
Status	*Åben/Lukket*
% afsluttet	*0 %-100 %*
Ressource	*Omkostninger, personale*
Startdato	*dd/mm/åå*
Slutdato	*dd/mm/åå*
Bemærkninger	*Andre kommentarer*

Tabel 6: Skabelon til styring af handlinger, der skal foretages under en informationssikkerhedsplan

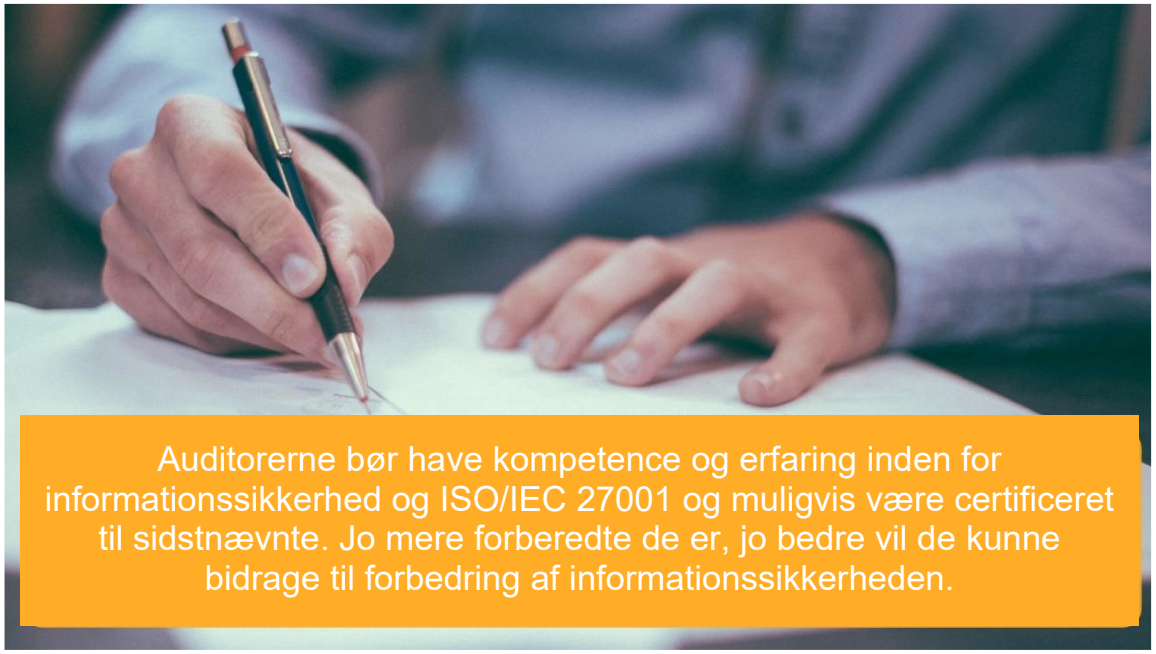
3.4.2 Trin 4.2 Administration af informationssikkerhedsplanen

Når informationssikkerhedsplanen er godkendt, skal informationssikkerhedschefen/den informationssikkerhedsansvarlige iværksætte periodisk (f.eks. månedlig eller kvartalsvis) overvågning for at vurdere, om planen skrider planmæssigt frem og i størst muligt omfang inddrager andre interessenter. Denne overvågning skal ske gennem et formelt udvalg (f.eks. styregruppen for informationssikkerhed), hvor alle involverede fagfolk skal rapportere om deres fremskridt, vanskeligheder og foreslåede ændringer til planen. Planen skal opdateres i overensstemmelse hermed, og hvis der sker væsentlige ændringer, der kræver nye ressourcer, skal den igen forelægges topledelsen til godkendelse. Hvis der ikke er nogen væsentlige ændringer, bør planen stadig godkendes af topledelsen med jævne mellemrum (mindst hvert år, muligvis inden det næste års budgetter er færdigbehandlet, for at sikre den rigtige fordeling af ressourcer).

Planen skal også omfatte resultaterne af nye handlinger, der foreslås eller på anden måde kræves på baggrund af aktiviteter, der udføres i det følgende *Trin 4.3*.

3.4.3 Trin 4.3 Kontrol af informationssikkerheden

En effektiv metode til at verificere, om der er styr på informationssikkerheden, er at planlægge og foretage **audit af informationssikkerheden** mindst én gang om året. Auditorerne bør udvælges blandt uvildige eksperter på området, som skal have til opgave at verificere, om informationssikkerhedsprocesserne udføres i overensstemmelse med interne og eksterne krav. Hvis auditten udføres af internt personale, bør auditøren ikke have noget driftsansvar inden for styring af informationssikkerhed, så eventuelle interessekonflikter undgås.



Auditorerne bør have kompetence og erfaring inden for informationssikkerhed og ISO/IEC 27001 og muligvis være certificeret til sidstnævnte. Jo mere forberedte de er, jo bedre vil de kunne bidrage til forbedring af informationssikkerheden.

Efter auditten bør organisationens topledelse modtage en rapport med:

- Afvigelser, dvs. aspekter, hvor organisationen ikke opfylder standarden
- Forbedringsmuligheder, dvs. henstillinger om, hvordan man kan arbejde på en mere sikker måde (selv om standarden er opfyldt)

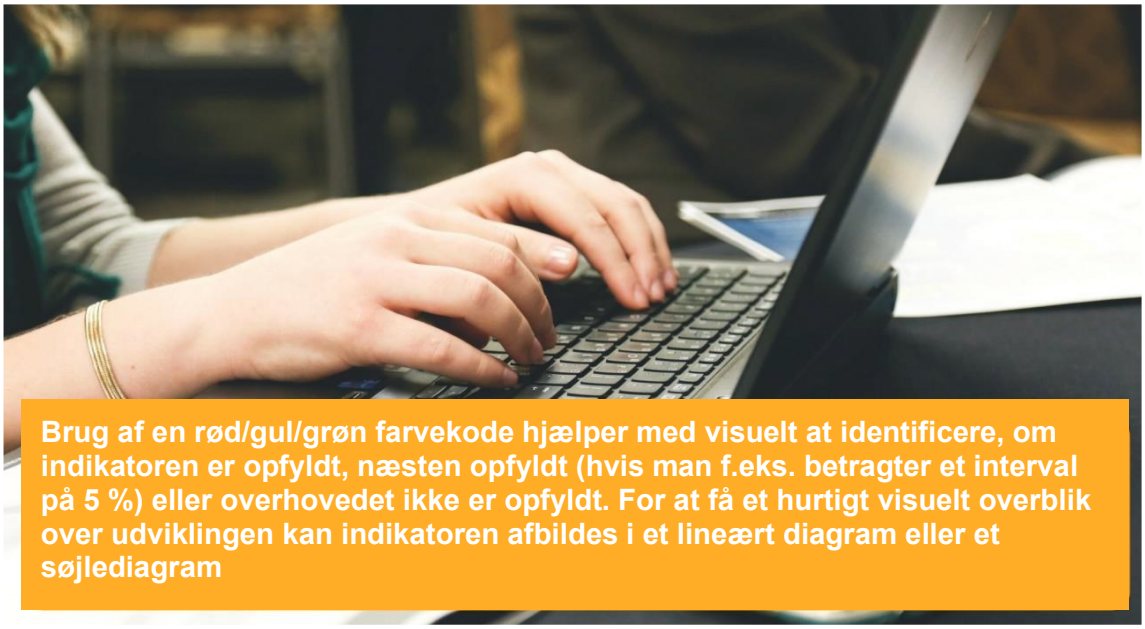
Afvigelser bør analyseres omhyggeligt, og der bør sættes ind med tiltag for at undgå, at de gentager sig. Sådanne tiltag skal medtages i en opdateret version af informationssikkerhedsplanen sammen med de tiltag, der er nødvendige for at rette afvigelser. Forbedringsmuligheder bør vurderes og om nødvendigt også indsættes i informationssikkerhedsplanen, hvis det anses for relevant, normalt med en mindre prioritet end for afvigelser.

3.4.4 Trin 4.4 Overvågning af informationssikkerheden

Efter at have defineret og udformet beskyttelsesforanstaltningerne i det foregående trin, kan organisationen "vende tilbage til hverdagen". For at sikre systemets effektivitet vil overvågningsaktiviteter bidrage til at begrænse afvigelser fra den oprindelige informationssikkerhedsplan.

Den mest praktiske måde at udføre overvågningsaktiviteter på er at opstille nogle enkle, men effektive mål- eller resultatindikatorer. Disse kan opdateres med jævne mellemrum. Sådanne indikatorer kan være baseret på mål eller kontroller: De består i det væsentlige af formler til beregning af tærskler, der skal udløse en vis handling, hvis de overskrides eller nås. Det er vigtigt at fastlægge, hvem der har ansvaret for med jævne mellemrum at beregne formlen for indikatoren. ISO/IEC 27004-standarden kan hjælpe med udviklingen af denne opgave.

Målindikatorer er lettest at sætte op. De kan bruges til at måle opnåelsen af et relevant mål for organisationen, såsom at overholde denne vejledning eller en relevant regel/standard, et sikkerhedsrelateret serviceniveau eller en sikkerhedsrelateret status. De skal verificeres med nogle måneders mellemrum.



Brug af en rød/gul/grøn farvekode hjælper med visuelt at identificere, om indikatoren er opfyldt, næsten opfyldt (hvis man f.eks. betragter et interval på 5 %) eller overhovedet ikke er opfyldt. For at få et hurtigt visuelt overblik over udviklingen kan indikatoren afbildes i et lineært diagram eller et søjlediagram

Resultatindikatorer kan relateres til nogle resultatværdier fra informationssikkerhedsprocesser (f.eks. risikovurdering) eller kontrollernes effektivitet. I sidstnævnte tilfælde kan de grundlæggende kontroller, der blev beskrevet i *Trin 3.1*, forbindes med indikatorer som i disse eksempler:

Kontrol	Indikatorformel	Mål	Hyppighed
Informationssikkerhedspolitik	% af medarbejderne, der har modtaget politikken	100 %	årligt
Informationssikkerhedsorganisation	# møder i styregruppen for informationssikkerhed	4	årligt
Bevidsthed om samt uddannelse og træning i informationssikkerhed	% af medarbejderne, der har fået træning, # initiativer vedrørende bevidsthed om sikkerhed	100 %	årligt
Aktivopgørelse	% af aktiver, der er medtaget i aktivopgørelsen inden for en måned efter erhvervelsen	100 %	kvartalsvist
Beskyttelse mod malware	# inficerede arbejdsstationer/rensede arbejdsstationer	1	månedligt
Rettelse af sårbarheder i software	# udestående kritiske sikkerhedsrettelser	0	månedligt
Sikkerhed i leverandøraftaler	% af kontrakter med særlige klausuler om informationssikkerhed	100 %	kvartalsvist
Hændelsesrespons	# informationssikkerhedshændelser, der er lukket/informationssikkerhedshændelser, der er åbnet samme dag	95 %	månedligt

Tabel 7: Foreslået hyppighed af overvågning af kontroller

Dette er blot nogle enkle eksempler. Hver enkelt organisation skal konsekvent fastlægge sine egne indikatorer. Disse indikatorer, der kan registreres i et simpelt regneark, kan periodisk undersøges af den informationssikkerhedsansvarlige/informationssikkerhedschefen eller fremlægges for styregruppen for informationssikkerhed.

Der bør sættes tidsfrister for hvert mål. Andre tærskler kan variere i tid og i starten sættes til en lavere værdi og senere hæves, efterhånden som processen eller kontrollen modnes. Styregruppen for informationssikkerhed kan med jævne mellemrum overvåge status på og udviklingen i styringen af informationssikkerheden.

4. ISO/IEC 27001-certificering

Den tilgang, der er foreslået her, ligger tæt op ad ISO/IEC 27001-kravene, hvilket fremgår af nedenstående sammenligningstabel. Hvor der mangler overensstemmelse mellem den internationale standard og denne vejledning, er forklaringen, at vejledningens forfattere har valgt en forenklet tilgang, som udelader de mest formelle og metodologiske aspekter og fokuserer på de mest praktiske aspekter.

Hovedkapitler i ISO/IEC 27001:2013		Trin i vejledningen for digitale SMV'er
4.1	Forståelse af organisationen og dens kontekst	Trin 3
4.2	Forståelse af interesserenters behov og forventninger	Trin 2
4.3	Bestemmelse af omfanget af ledelsessystemer til styring af informationssikkerhed	Ikke relevant
4.4	Ledelsessystem til styring af informationssikkerhed	Ikke relevant
5.1	Lederskab og engagement	Ikke relevant
5.2	Politik	*Basiskontrol A1.01*
5.3	Roller, ansvar og beføjelser i organisationen	Trin 1
6.1	Handlinger til håndtering af risici og muligheder	Trin 2 Trin 3
6.2	Informationssikkerhedsmålsætninger og planlægning for opnåelse heraf	Ikke relevant
7.1	Ressourcer	Ikke relevant
7.2	Kompetencer	Ikke relevant
7.3	Bevidsthed	*Basiskontrol A1.03*
7.4	Kommunikation	*Skønsmæssig kontrol A2.01*
7.5	Dokumenteret information	Ikke relevant
8.1	Driftsplanlægning og -kontrol	Trin 4
8.2	Risikovurdering af informationssikkerheden	Trin 2 Trin 3
8.3	Risikohåndtering af informationssikkerhed	Trin 4
9.1	Overvågning, måling, analyse og vurdering	Trin 4
9.2	Intern audit	Trin 4
9.3	Ledelsesgennemgang	
10.1	Afvigelser og korrigerende handlinger	Trin 4
10.2	Løbende forbedring	

Tabel 8: Hovedindhold i ISO/IEC 27001:2013

Ikke desto mindre er det nødvendigt at se på disse aspekter også,, hvis man ønsker en formel certificering i henhold til ISO/IEC 27001-standarden efter at have baseret sin styring af informationssikkerheden på denne vejledning i en periode. Mere specifikt skal følgende yderligere tiltag udføres efter *Trin 1.1*, jf. kapitel 3:

4.1.1 Trin 1.2: Etablering af et ledelsessystem til styring af informationssikkerhed (ISMS)

Et ledelsessystem til styring af informationssikkerhed (Information Security Management System, ISMS) bør betragtes som en mere formel tilgang til styring af informationssikkerhed end den tilgang, der er beskrevet i denne vejledning. Et ISMS omfatter politikker, procedurer, vejledninger og forbundne ressourcer og aktiviteter, som en organisation anvender samlet for at beskytte sin information. Topledelsen skal involveres direkte i planlægningen af et ISMS, der omfatter flere formaliteter, men også giver mulighed for at bevæge sig i retning af en internationalt anerkendt certificering for en del af organisationen. Udpegning af andelen af organisationen bør overvejes nøje, fordi det vil få en ret stor betydning for certificeringsomkostningerne. Det er muligt at vælge hele organisationen, men det er ikke det eneste alternativ, da de vigtigste tjenester eller processer kan prioriteres i tråd med organisationens forretningsstrategier. Bemærk, at det også er muligt kun at certificere en del af et bredere ISMS.

Tidlig involvering af topledelsen vil være vigtig, når man bestemmer omfanget samt for at få yderligere tilsagn (og derefter ressourcer), der skal bruges i de følgende trin. Status for gennemførelsen bør rapporteres med jævne mellemrum, og der bør fastsættes tidsfrister for denne gennemførelse.

Målbare og forretningsrelaterede mål bør foreslås og vælges i denne fase. Disse mål, ligesom resten af ISMS, bør altid have fokus på kontinuerlig forbedring, version for version.

4.1.2 Andre elementer

Den dokumentstyringsmetode, der skal følges under et formelt ISMS (og for hvert ledelsessystem), kræver også, at hvert dokument, der udarbejdes:

- indeholder komplette metadata (titel, dato, forfatter som minimum)
- er baseret på godkendte formater og modeller
- er underlagt ændrings-/versionskontrol
- formidles til den tilsigtede målgruppe

Et "statement of applicability" i henhold til ISO/IEC 27001 krav 6.1.3 d) skal udarbejdes og ajourføres. Den foreslåede skabelon til valg af kontrol i denne vejledning er et godt udgangspunkt, men der skal som minimum angives en begrundelse for valget om at medtage eller udelade de enkelte kontroller.

En formel ledelsesgennemgang, der omfatter alle de elementer, der er beskrevet i ISO/IEC 27001 krav 9.3, bør også udføres med jævne mellemrum. Den bør bruge den samme tilgang som beskrevet i *Trin 3.2*, men den skal ledsages af en tekst.

Den formelle tredjepartscertificeringsaktivitet kan også tilføjes. Dette kan gøres på samme måde som en intern audit, samtidig med at man får et eksternt og kompetent syn på ISMS.

5. Referencer og frit tilgængelige ressourcer

Referencer

- ISO/IEC 27000-familien – Ledelsessystemer til styring af informationssikkerhed. Tilgængelig online på: https://www.iso.org/isoiec-27001-information-security.html

- "CEN Workshop Agreement (CWA) 16458 on European ICT Professional Profiles". Tilgængelig online på: ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA%2016458.pdf

Frit tilgængelige ressour-

- BSI. "ISO/IEC 27001 for small and medium-sized businesses (SMEs)". Tilgængelig online på: https://www.bsigroup.com/en-GB/iso-27001-information-security/ISO- 27001-for-SMEs/

- Centre for Cyber Security, Belgien. "Cyber Security Guide for SMEs". Tilgængelig online på: https://ccb.belgium.be/en/document/guide-sme

- Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA). *"Information security and privacy standards for SMEs.* Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises". Tilgængelig online på: https://www.enisa.europa.eu/publications/standardisation-for- smes/at_download/fullReport

- ENISA. *"Security guide and online tool for SMEs when going Cloud".* Tilgængelig online på: https://www.enisa.europa.eu/news/enisa-news/enisa2019s-security- guide-and-online-tool-for-smes-when-going-cloud

- ENISA. *"A simplified approach to Risk Management for SMEs"*. Tilgængelig online på: https://www.enisa.europa.eu/publications/archive/RMForSMEs

- ETSI. *"NIS Directive Implementation" – ETSI TR 103 456 – teknisk rapport fra ETSI's tekniske udvalg om cybersikkerhed (TC CYBER)*. Tilgængelig online på: http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_1034 56v010101p.pdf

- ISO. *Offentligt tilgængelige standarder (herunder ISO/IEC 27000*). Tilgængelig online på: http://standards.iso.org/ittf/PubliclyAvailableStandards/

BILAG A

A.1 Basiskontroller

ID	Kontrolnavn	Ref. til ISO/IEC 27001 Anneks A	Kontrolbeskrivelse og -vejledning
01	**Informationssikkerhedspolitik**	5.1.1 5.1.2	En informationssikkerhedspolitik skal vedtages, aftales, offentliggøres og formidles til alle ansatte og til relevante tredjeparter. Informationssikkerhedspolitikken skal gennemgås med regelmæssige mellemrum eller i tilfælde af væsentlige ændringer for at sikre, at den til enhver tid er relevant, dækkende og effektiv. *Foreslået hyppighed af gennemgang: årligt*
02	**Informationssikkerhedsorganisation**	6.1.1 6.1.2	Medarbejderes, leverandørers og andre parters roller og ansvar i forhold til informationssikkerhed skal defineres og dokumenteres, mens pligter og ansvarsområder holdes adskilt for at begrænse skader, der opstår som følge af en enkelt persons uhensigtsmæssige adfærd.
03	**Bevidsthed om samt uddannelse og træning i informationssikkerhed**	7.2.2	Alle medarbejdere og relevante tredjeparter skal med jævne mellemrum modtage uddannelse og informeres om trusler mod informationssikkerheden. De bør også regelmæssigt gennemgå træning i henhold til informationssikkerhedspolitikken og procedurer, der er fastlagt af organisationen. *Foreslået hyppighed af træning: årligt*
04	**Aktivopgørelse**	8.1.1 8.1.2 8.1.3 8.1.4	En centraliseret aktivopgørelse skal etableres, vedligeholdes og gennemgås ofte. Ejerskab og ansvar for alle aktiver skal identificeres, dokumenteres, accepteres og implementeres. Der bør etableres en klar procedure til håndtering af alle aktiver, der er tildelt ansatte eller en tredjepart, og sikrer sporbarheden af disse aktiver i hele deres livscyklus. *Foreslået hyppighed af gennemgang: månedligt*
05	**Klassificering, mærkning og håndtering af information**	8.2.1 8.2.2 8.2.3	Information bør klassificeres, mærkes og håndteres i overensstemmelse med dens direkte værdi for organisationen såvel som den gældende lovgivning. En procedure til informationsmærkning og -håndtering bør udarbejdes og anvendes af alle informationsejere i organisationen. *Foreslåede klassificeringsniveauer: offentlig, intern, fortrolig*
06	**Brugeridentifikation**	9.2.1 9.2.2	Brugere af informationssystemer og -tjenester skal have unik identifikation via en formel registrerings- og afregistreringsprocedure for tildeling og tilbagekaldelse af adgang.
07	**Brugerrettigheder**	9.2.3 9.2.5 9.2.6	Tildelingen og brugen af rettigheder til brugere af informationssystemer og -tjenester skal kontrolleres og gennemgås regelmæssigt. Brugere bør kun få de minimumsrettigheder, der er nødvendige for at udføre deres opgaver. Alle ændringer af adgangsrettigheder skal håndteres efter en streng procedure, og de skal godkendes af informationsejeren.
08	**Brugergodkendelse**	9.2.4 9.3.1 9.4.1 9.4.2	Brugere af informationssystemer og -tjenester skal tildeles loginoplysninger på en fortrolig måde. Disse loginoplysninger og de informationssystemer, der verificerer dem, skal være robuste nok til at sikre, at uautoriserede medarbejdere ikke kan gætte dem.

ID	Kontrolnavn	Ref. til ISO/IEC 27001 Anneks A	Kontrolbeskrivelse og -vejledning
		9.4.3	*Foreslået styrke for loginoplysninger: 8 tegn og ikke fra ordbogen*
09	**Placering af aktiver**	11.2.1 11.2.2 11.2.3 11.2.6	Alle aktiver, der indeholder data eller understøttende informationstjenester, skal placeres på en måde, så de er beskyttet mod utilsigtede og miljømæssige trusler og altid være forsynet med passende hjælpeværktøjer, både hvis de placeres i selve organisationen eller uden for organisationen.
10	**Beskyttelse mod malware**	12.2.1	Software til beskyttelse mod malware skal installeres og holdes løbende ajour på alle aktiver, der kan inficeres med malware.
11	**Procedurer for informationssikkerhed**	12.1.1	Procedurer for informationssikkerhed skal anvendes, dokumenteres, vedligeholdes og være tilgængelige for alle brugere.
12	**Rettelse af sårbarheder i software**	12.5.1 12.6.1	Sikkerhedsrettelser, der gøres tilgængelige af leverandører for at afhjælpe sårbarheder i software, bør løbende vurderes og installeres i rette tid på alle systemer. *Foreslået hyppighed af rettelse: månedligt*
13	**Netværkssikkerhed**	13.1.1 13.1.2	IKT-netværk skal være designet, så de begrænser muligheden for aflytning eller ændring af trafikken, og de skal derudover begrænse tilladt kommunikation til kun at omfatte nødvendig kommunikation og blokere al anden kommunikation.
14	**Sikkerhed i leverandøraftaler**	15.1.1 15.1.2 15.1.3	Alle leverandører, med hvilke der udveksles information, skal være opmærksomme på organisationens gældende sikkerhedspolitikker og være kontraktmæssigt forpligtet til at overholde dem. De skal samtidig give tilladelse til, at dette verificeres af organisationen. Denne tilgang bør også omfatte deres underleverandører.
15	**Hændelsesanalyse og -respons**	16.1.2 16.1.3 16.1.4 16.1.5	Alle brugere af informationssystemer og -tjenester skal notere og rapportere alle observerede eller mistænkte sikkerhedssvagheder, så de kan analyseres. Specifikke procedurer for hændelsesrespons bør iværksættes, afhængigt af analyseresultaterne, og fuld sporbarhed skal sikres gennem hele forløbet.
16	**Identifikation af lovgivning og kontraktlige krav**	18.1.1 18.1.4	Alle gældende krav til informationssikkerhed i henhold til national, international eller sektorbestemt lovgivning samt krav, der stammer fra kontrakter med tredjeparter, bør holdes under konstant kontrol med særligt fokus på beskyttelse af personoplysninger.

A.2 Skønsmæssige kontroller

ID	Kontrolnavn	Ref. til ISO/IEC 27001 Anneks A	Kontrolbeskrivelse og -vejledning
01	**Eksterne kontakter og kommunikationsstyring**	6.1.3 6.1.4	Organisationen bør etablere tilstrækkelig kontakt med myndighederne til hurtigt at kunne reagere på udbredte trusler og med særlige interessegrupper, fora eller foreninger hovedsageligt for at få information om den faktiske trussel og kontrol.
02	**Fjernarbejde**	6.2.2	Der bør udvikles redskaber til fjernarbejde under hensyntagen til behovet for yderligere sikkerhedsbeskyttelse for at undgå lækager og misbrug af information. Fjernadgang, der bruges til dette formål, bør beskyttes mod uautoriseret adgang.
03	**Styring af mobile enheder**	6.2.1	Mobile enheder, der bruges til arbejdsformål, skal være sikkert konfigureret og strengt kontrolleret.
04	**Personalescreening**	7.1.1	Alle medarbejdere og eksternt personale, der regelmæssigt får adgang til organisationens lokaler, skal have deres straffeattest og relevante baggrund tjekket i overensstemmelse med relevante love, regler og etiske principper. Screeningen skal stå i et rimeligt forhold til forretningskravene.
05	**Ansættelseskontrakter**	7.1.2 7.2.3 7.3.1 13.2.4	Alle medarbejdere og eksternt personale skal underskrive fortrolighedsaftaler, før de får adgang til organisationens information, og deres kontrakt skal indeholde en forpligtelse til at overholde organisationens informationssikkerhedspolitik. Konsekvenserne ved ikke at opfylde disse forpligtelser, også efter stillingsændringer eller opsigelse, bør også være klart defineret.
06	**Styring af flytbare medier**	8.3.1 8.3.3 13.2.1 13.2.2 18.1.3	Der bør fastlægges og implementeres specifikke begrænsninger for håndtering af alle flytbare og bærbare medier. Medier, der indeholder information, skal beskyttes mod uautoriseret misbrug af adgang eller ødelæggelse i tilfælde af, at de tages ud af organisationen.
07	**Bortskaffelse af information**	8.3.2 11.2.7	Der bør anvendes strenge procedurer for sikker bortskaffelse af medier, der skal overflyttes eller bortskaffes for at sikre, at de data, der tidligere var lagret på, dem, ikke kan gendannes. *Foreslået bortskaffelse af information: fuld overskrivning*
08	**Politik for adgangskontrol**	9.1.1 9.1.2	En formel adgangskontrolpolitik, der dækker organisationens system og netværk, skal dokumenteres, vedligeholdes og gennemgås i overensstemmelse med sikkerhedskravene, informationsklassificering og -styring og medarbejderrettigheder.

09	**Kryptering**	10.1.1 10.1.2	Kryptografiske kontroller, der bruger stærke algoritmer, bør udvikles, dokumenteres, implementeres, vedligeholdes og gennemgås for at sikre, at al information, der sendes eller lagres, holdes fortrolig. Kryptografiske nøgler skal bruges, beskyttes og opbevares i henhold til strenge og dokumenterede procedurer i hele deres livscyklus. *Foreslåede krypteringsalgoritmer: AES128+, SHA512+, RSA2048+*

ID	Kontrolnavn	Ref. til ISO/IEC 27001 Anneks A	Kontrolbeskrivelse og -vejledning
10	**Fysisk sikkerhed**	11.1.1 11.1.2 11.1.3 11.1.6	Fysisk beskyttede barrierer og sikre områder for at minimere uautoriseret adgang til organisationens lokaler og dens informationssystemer bør defineres og udstyres med adgangskontrolsystemer. Adgangspunkter, herunder til lastning og losning, skal holdes på et minimum og sikres lige så godt.
11	**Beskyttelse mod miljøtrusler**	11.1.4	Fysisk beskyttelse mod skader, der har naturlige årsager, eller som skyldes enhver anden form for naturkatastrofe eller menneskeskabt katastrofe, skal udformes og anvendes i bygninger og i informationssystemerne i bygninger, startende med brand-, vand- og jordskælvssikring. *Foreslåede trusler, der skal imødegås: brand, vand, jordskælv*
12	**Vedligeholdelse af udstyr**	11.2.4	Alt udstyr skal vedligeholdes i forbindelse med organisationens informationssikkerhedsplan. Vedligeholdelsesadgang til informationssystemer skal kontrolleres.
13	**Uovervåget arbejdsplads og udstyr**	11.2.8 11.2.9	Uovervåget udstyr skal altid efterlades med den passende beskyttelse mod fysisk uautoriseret adgang og tyveri. Alle sessioner skal låses, når udstyr forlades, og forbindelsen skal frakobles automatisk efter en nærmere bestemt periode med inaktivitet. Intet medie bør efterlades uovervåget på en arbejdsplads. *Foreslået timeout/pauseskærm: 15 minutter*
14	**Ændringsstyring**	12.1.2 12.6.2 14.2.2 14.2.4	Alle ændringer i organisationen, forretnings- og informationsprocesser eller -systemer, der påvirker informationssikkerheden, skal registreres, godkendes behørigt og testes. System- og softwareændringer bør kun kunne foretages af autoriseret personale.
15	**Adskillelse af udviklings- og testmiljøer**	12.1.4 14.3.1	Udviklings-, test- og driftsmiljøer skal være så adskilt som muligt for at reducere risikoen for uautoriseret adgang eller ændringer i operativsystemet. Data, der bruges til udvikling og test, skal desuden være forskellige fra produktionsdata (anonymiseret eller ikke relateret til virkelige personer/fakta). *Foreslået adskillelse: forskellige systemer og netværk*
16	**Sikkerhedskopiering**	12.3.1	Sikkerhedskopier af information og software skal oprettes og testes regelmæssigt i overensstemmelse med en defineret sikkerhedskopipolitik. *Foreslået hyppighed af sikkerhedskopiering: dagligt/ugentligt*
17	**Event-logning og -lagring**	12.4.1 12.4.2 12.4.3	Event-logs for de fleste sikkerhedsrelevante handlinger skal produceres, lagres sikkert, beskyttes mod både adgang og ændringer samt gennemgås regelmæssigt. Alle systemadministrator- og systemoperatøraktiviteter skal logges som gennemførte og forsøgte login/logout. *Foreslået opbevaring af logs: 6+ måneder*
18	**Tidssynkronisering**	12.4.4	Systemure skal konstant synkroniseres i alle områder af organisationen eller i et sikkerhedsdomæne med en aftalt og pålidelig nøjagtig tidskilde.
19	**Netværksadskillelse**	13.1.3	Informationstjenester, brugere og informationssystemer skal adskilles inden for forskellige netværksområder med homogene sikkerhedskrav. Adskillelsen skal udføres ved hjælp af firewalls eller tilsvarende enheder.

ID	Kontrolnavn	Ref. til ISO/IEC 27001 Anneks A	Kontrolbeskrivelse og -vejledning
20	**Sikkerhed for beskeder**	13.2.3	Information der overføres i elektroniske beskeder og hjælpesystemerne, skal sikre fortrolighed og opdage angreb gennem disse kanaler.
21	**Indbygget sikkerhed**	6.1.4 14.1.1 14.2.5	Informationssikkerhed skal være en integreret del af informationssystemer i hele deres levetid og starte med kravene til informationssystemerne i den tidlige designfase. Alle organisationens projekter bør så tidligt som muligt tage højde for informationssikkerhed.
22	**Sikkerhed for applikationstjenester**	14.1.2 14.1.3	Informationssystemer, der bruges til at levere tjenester, skal være beskyttet mod almindelige angreb gennem en sikker og hærdet konfiguration, der er designet til at kunne bruge yderligere sikkerhedskontroller, og som konstant overvåges/beskyttes gennem enheder, der kun tjener sikkerhedsformål. Dette skal stå i et rimeligt forhold til, hvor meget de eksponeres. *Foreslået sikkerhedsenheder: firewalls og IDS/IPS*
23	**Sikker udviklingslivscyklus**	14.2.1 14.2.6 14.2.7	Organisationer bør opstille kriterier for en sikker udviklingslivscyklus for deres applikationer, og de også skal anvendes til eksterne kundeprojekter for at minimere applikationers sårbarheder.
24	**Sikkerhedstest**	14.2.3 14.2.8 14.2.9 18.2.3	Sikkerheds- og acceptkriterier for nye informationssystemer, opgraderinger og nye versioner bør opstilles, og der bør udføres passende tests af systemet under udviklingen, før accept og regelmæssigt derefter, hvilket kræver forudgående afhjælpning af konstaterede sårbarheder. *Foreslået hyppighed: hver sjette måned internt, hvert kvartal eksternt*
25	**Leverandørs sikkerhedsovervågning**	15.2.1 15.2.2	Implementeringen af ændringer af leverandørtjenester skal overvåges, kontrolleres og gennemgås ved hjælp af formelle procedurer for ændringskontrol. Overholdelsen af sikkerhedsklausuler og sikkerhedsserviceniveauer bør konstant overvåges.
26	**Politik for hændelsesstyring**	16.1.1	Informationssikkerhedshændelser skal kontrolleres, registreres, håndteres og afhjælpes i henhold til specifikke ansvarsområder, der er godkendt og fastlagt af ledelsen. Der bør også etableres passende kommunikations- og eskaleringsprocedurer.
27	**Erfaringsopsamling efter hændelser**	16.1.6	Viden, der er opnået ved analyse og løsning af informationssikkerhedshændelser, bør bruges til at reducere sandsynligheden for eller virkningen af fremtidige hændelser og muligvis til at tilpasse procedurerne for hændelsesrespons.
28	**Redundansstyring**	17.2.1	Informationsbehandlingsfaciliteter bør implementeres med redundans, der er tilstrækkelig til også at opfylde tilgængelighedskravene i tilfælde af nedbrud.
29	**Beskyttelse af intellektuel ejendom**	18.1.2	Der bør implementeres passende procedurer for at sikre overholdelse af lovgivningsmæssige og kontraktlige krav til brug af materiale, der er omfattet af intellektuel ejendomsret, og om brug af beskyttede softwareprodukter.

30	**Vurdering og audit af informationssikkerhed**	18.2.1 18.2.2	Informationssikkerhedssystemer bør regelmæssigt gennemgås af uafhængige auditorer. Ledere skal sikre, at alle sikkerhedsprocedurer inden for deres ansvarsområde udføres korrekt, for at sikre overholdelse af sikkerhedspolitikker og -standarder. Informationssystemer bør regelmæssigt gennemgås for at sikre kontinuerlig overensstemmelse med sikkerhedsimplementeringsstandarder.

A.3 Forbindelser mellem skønsmæssige kontroller og trusler (begrænsning)

ID	Kontrol	Fysisk angreb	Utilsigtet skade	Kata-strofe	Nedbrud/funktionsfejl	Afbry-delser	Aflytning/opsnap-ning/kapring	Juridisk	Ondsindet handling/mis-brug
A2.01	**Eksterne kontakter og kommunikationsstyring**	Sekundær		Primær		Sekundær	Primær		Sekundær
A2.02	**Fjernarbejde**			Sekundær		Sekundær	Primær		
A2.03	**Styring af mobile enheder**	Sekundær	Sekundær	Sekundær		Sekundær	Primær		Sekundær
A2.04	**Personale-screening**				Sekundær		Primær	Primær	Sekundær
A2.05	**Ansættelseskontrakter**	Sekundær	Sekundær		Sekundær		Primær	Primær	Primær
A2.06	**Styring af flytbare medier**	Primær	Primær	Sekundær	Sekundær	Sekundær	Primær	Sekundær	
A2.07	**Bortskaffelse af information**	Sekundær	Sekundær		Sekundær		Primær		
A2.08	**litik for adgangskontrol**						Primær		Primær
A2.09	**Kryptering**						Primær	Primær	
A2.10	**Fysisk sikkerhed**	Primær	Sekundær				Primær		
A2.11	**Beskyttelse mod miljøtrusler**	Primær	Sekundær	Primær		Primær	Sekundær		
A2.12	**Vedligeholdelse af udstyr**	Primær	Primær		Primær	Sekundær			

ID	Kontrol	Fysisk angreb	Utilsigtet skade	Kata-strofe	Nedbrud/funktionsfejl	Afbrydel-ser	Aflytning/opsnap-ning/kapring	Juridisk	Ondsindet handling/misbrug
A2.13	Uovervåget ar-bejdsplads og ud-styr	Sekundær					Primær		
A.2.14	Ændringsstyring		Sekundær		Sekundær		Primær		Sekundær
A.2.15	Adskillelse af ud-viklings- og test-miljøer				Sekundær		Sekundær		
A.2.16	Sikkerhedskopie-ring	Primær	Primær	Primær	Primær	Sekundær		Sekundær	Sekundær
A.2.17	Event-logning og -lagring		Sekundær		Sekundær		Primær	Sekundær	Primær
A.2.18	Tidssynkronise-ring		Sekundær		Sekundær		Primær	Sekundær	Primær
A.2.19	Netværksadskil-lelse		Sekundær			Sekundær	Primær		Sekundær
A.2.20	Sikkerhed for be-skeder		Sekundær				Primær	Sekundær	Sekundær
A.2.21	Indbygget sikker-hed		Sekundær		Sekundær	Sekundær	Primær		Primær
A.2.22	Sikkerhed for ap-plikationstjenester		Sekundær				Primær	Sekundær	Primær
A.2.23	Sikker udviklings-livscyklus		Primær				Primær		Sekundær
A.2.24	Sikkerhedstest		Sekundær				Primær		Primær
A.2.25	Leverandørs sik-kerhedsovervåg-ning				Sekundær	Primær		Sekundær	
A.2.26	Politik for hændel-sesstyring	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær
A.2.27	Erfaringsopsam-ling efter hændel-ser	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær	Sekundær

ID	Kontrol	Fysisk angreb	Utilsigtet skade	Kata-strofe	Nedbrud/funktionsfejl	Afbry-delser	Aflytning/opsnap-ning/kapring	Juridisk	Ondsindet handling/mis-brug
A.2.28	**Redundanssty-ring**			Primær	Primær	Primær		Sekundær	Primær
A.2.29	**Beskyttelse af intellektuel ejen-dom**							Primær	
A.2.30	**Vurdering og audit af informa-tionssikkerhed**		Sekundær				Sekundær	Primær	Sekundær

BILAG X

Informationssikkerhedspolitik		
Politik #:	**Ikrafttrædelsesdato:**	**E-mail:**
Version:	**Kontaktperson:**	**Telefon:**

Formål

Organisationens informationssikkerhedspolitik, relaterede politikker og procedurer er beregnet til at beskytte fortrolighed, integritet og tilgængelighed (FIT) for alle organisationens kritiske data og aktiver i henhold til dens forretningsinteresser.

Anvendelsesområde

Denne politik gælder for ansatte, leverandører, konsulenter, midlertidigt ansatte og andre arbejdstagere i organisationen, herunder alt personale tilknyttet tredjeparter. Denne politik gælder for alle aktiver, både materielle og immaterielle, der ejes eller bruges af organisationen.

Politik

Organisationens topledelse betragter informationssikkerhed som en af de vigtigste faktorer til at understøtte dens forretning, og den arbejder aktivt for at fremme og finansiere alle initiativer, der omkostningseffektivt reducerer informationssikkerhedsrisici, sikrer overholdelse af relevante love og kontraktmæssige krav og følger god praksis i sektoren. Alle organisationens interne og eksterne medarbejdere forventes nøje at respektere hensigten bag og forskrifterne i denne politik samt i alle relaterede politikker og procedurer. Der kan træffes disciplinære foranstaltninger ved undladelse heraf. Mere specifikt er det følgende informationssikkerhedsprincipper, som alle forventes at forstå og overholde:

1) Informationssikkerhed er ikke et absolut begreb, men skal altid stå i forhold til de risici, den skal imødegå.
2) Al adgang skal begrænses til det strengt nødvendige for medarbejderne og deres arbejdsbehov.
3) Ressourcerne skal adskilles og beskyttes i forhold til deres informationssikkerhedskrav.
4) Brug af åbne standarder og løsninger foretrækkes altid frem for beskyttede og ukendte alternativer.
5) Et enkelt lag af informationssikkerhedskontroller er muligvis ikke tilstrækkeligt i alle tilfælde, da det kan fejle: Der kan anvendes flere lag, hvis et nedbrud vil være kritisk.
6) Undersøgelse og test af samt øvelse i informationssikkerhedsrelevante situationer er nøglen til at sikre et effektivt responsberedskab.
7) Informationssikkerhed er alles ansvar og pligt – det er ikke en andens problem.

Organisationen definerer og måler en række specifikke informationssikkerhedsmålsætninger, som konstant overvåges og forbedres. Disse målsætninger skal danne grundlag for de taktiske beslutninger om informationssikkerhed, ligesom ovennævnte principper styrer de strategiske beslutninger. Løbende forbedringer er en vigtig faktor, der gør det muligt at holde de stadigt stigende informationssikkerhedsrisici i skak, og som sætter organisationen i stand til at nå sine forretningsmæssige mål i det komplekse miljø, som den i dag opererer i.

Godkendelse og ejerskab

Ejer	Titel	Dato	Underskrift
Forfatter	Titel	MM/DD/ÅÅÅÅ	
Godkendt af	**Titel**	**Dato**	**Underskrift**
Ledelsesteam	Titel	MM/DD/ÅÅÅÅ	

European Commission

EFTA

Small Business Standards

European DIGITAL SME Alliance

sbs-sme.eu
@SBS_SME

digitalsme.eu
@EUdigitalsme

Co-financed by the European Commission and EFTA