Målepunkter for informationssikkerhed

Marts 2013

Indholdsfortegnelse

1. Forord

Virksomheder, som beskæftiger sig med kritisk informations- og kommunikations teknologi (IKT-infrastruktur) har i stigende grad behov for at styre og dokumentere, at deres indsats for at beskytte infrastrukturen har et passende niveau. Med kritisk IKT-infrastruktur forstås: anlæg, udstyr og systemer, som er nødvendige for at opretholde vitale samfundsmæssige interesser.

Center for Cybersikkerhed har et ønske om at tilvejebringe et værktøj, der kan hjælpe disse virksomheder med styring og rapportering på deres arbejde med informationssikkerhed. Denne vejledning er derfor bestilt til udarbejdelse hos Deloitte.

Vejledningen er tænkt som et praktisk værktøj, der kan hjælpe virksomheder i gang med at foretage konkrete målinger af deres indsats på informationssikkerhedsstyring. Sådanne målinger kan bidrage til at fastslå det aktuelle sikkerhedsniveau samt, over tid, anvendes som indikatorer for udviklingen af modenheden af informationssikkerhedsstyringen.

Målgruppen for vejledningen er primært virksomheder i energi-, tele- og den finansielle sektor. De opstillede målepunkter vil dog også være relevante for virksomheder i en bred vifte af andre brancher.

Virksomheder, der driver samfundskritisk infrastruktur kan have en særlig interesse i informationssikkerhedsstandarder med et specialiseret sigte. Det kan f.eks. være NERC 1300 for produktions-it inden for el-forsyningsbranchen. Nærværende vejledning giver ikke eksempler på den type specialiserede produktions målepunkter, men disse kan med fordel hentes i de branchespecifikke standarder og opstilles indenfor samme ramme som i denne vejledning.

Center for Cybersikkerhed, den 1. marts 2013

2. Indledning og formål

Vejledningen beskriver 22 målbare indikatorer eller målepunkter, der er meningsfulde for virksomheder, som beskæftiger sig med kritisk infrastruktur. Ca. halvdelen af målepunkterne er udvalgt med direkte inspiration i COBIT-standardens *Security-specific Process Goals and Metrics*[1], idet netop denne standard har en lang tradition for at anvende målepunkter som en integreret del af sine it-procesbeskrivelser. Resten af indikatorerne er knapt så procesorienterede men har fokus på at måle konkrete faktorer af informationssikkerhedsmæssig betydning samt indsatsen fra medarbejderne i virksomheden.

Anvendelsen af mange af indikatorerne forudsætter, at virksomheden har nået et vist modenhedsniveau i styringen af informationssikkerhed, da der kræves en passende organisatorisk og teknologisk platform for at kunne etablere måling af nogle af de foreslåede indikatorer. En del af indikatorerne er nemmere at gå til og kan anvendes af alle virksomheder.

De forretningsmæssige fordele ved at foretage målinger er typisk følgende:

- Målingerne kan bruges som redskab til at følge fremdrift i aktiviteter og handlingsplaner på informationssikkerhedsområdet.
- Målingerne er konkret anvendelige som indikatorer på virksomhedens aktuelle beskyttelsesniveau.
- Målinger udgør en enkel og overskuelig måde at generere ledelsesinformation, som der direkte kan styres efter. På den måde adskiller målepunkter indenfor informationssikkerhed sig ikke nævneværdigt fra f.eks. virksomhedens økonomiske nøgletal i deres anvendelsesmuligheder.
- Målinger kan bruges som compliance-"barometer" i forhold til de love, aftalekrav og standarder, som virksomheden er underlagt.
- Målinger kan bruges som aktivt risikostyringsredskab på det taktiske og operationelle niveau, fordi de, ved at vise tendenser, kan bidrage til at fastægge sandsynligheden for uønskede hændelser.

3. Den overordnede ramme

Som overordnet ramme til at beskrive målepunkterne er valgt nogle sikkerhedsområder, der er defineret med udgangspunkt i ISO/IEC27002:2005. Områderne udgør en alment accepteret ramme til at beskrive sikringsforanstaltninger og kontroller på informationssikkerhed. Rammen er i forlængelse heraf også velegnet til at kategorisere målepunkter for sikringsforanstaltningernes effektivitet. Virksomheder, der arbejder efter andre informationssikkerhedsstandarder kan som regel mappe sikkerhedsområderne indbyrdes mellem de anvendte standarder. I denne vejledning har alle målepunkter referencer til både ISO/IEC27002 og COBIT.

[1] COBIT for Informations Security, Appendix B.

Sikkerhedsområder	
1)	Politik og Strategi
2)	Styring og organisering af informationssikkerhed
3)	Risikostyring
4)	Styring af aktiver
5)	Medarbejdersikkerhed
6)	Fysisk sikkerhed
7)	Styring af netværk og drift
8)	Adgangsstyring
9)	Styring af udvikling
10)	Hændelsesstyring
11)	Beredskabsstyring
12)	Compliance
13)	Privatlivsbeskyttelse

Når man som virksomhed vælger at iværksætte et måleprogram for informationssikkerhed, så udgør den aktivitet en kontrol i sig selv. Den er også beskrevet i f.eks. ISO/IEC27002 (jf. f.eks. pkt. 6.18, 12.2). Derfor bør virksomheden også beskrive sine *retningslinjer for udførelse af målinger* på samme måde som alle andre retningslinjer for informationssikkerhed.

4. Kategorier af målepunkter

For at sikre at målepunkterne har den bredest mulige dækning i forhold til de elementer (organisatoriske og tekniske), der normalt indgår i informationssikkerhedsstyringssystem (ISMS), er der for hvert sikkerhedsområde defineret 1-2 målepunkter i en eller flere af følgende kategorier (i alt 4-6 målepunkter pr. sikkerhedsområde):

- Mennesker (medarbejdere, kunder, samarbejdspartnere mv.)
- Processer
- Teknologi

Målepunkter i *Mennesker*-kategorien skal sige noget om effektiviteten af de sikringsforanstaltninger, hvor målingen er afhængig af:

- Aktiviteter, der kræver en menneskelig indsats
- En bestemt menneskelig adfærd
- Bestemte menneskers/medarbejderes holdning eller opfattelse
- Virksomhedens kultur

Målepunkter i *Processer*-kategorien skal sige noget om effektiviteten af de sikringsforanstaltninger, der er afhængige af, at bestemte retningslinjer, procedurer eller instrukser beskrives eller udføres.

Målepunkter i *Teknologi*-kategorien skal sige noget om effektiviteten af de sikringsforanstaltninger, der er afhængige af en form for teknologisk understøttelse.

Alle 3 kategorier er ikke nødvendigvis relevante indenfor alle sikkerhedsområder. F.eks. kunne teknologi-målepunkter indenfor et område som *Politik og Strategi*, som stort set kun indeholder organisatoriske sikringsforanstaltninger, hurtigt forekomme lidt "søgte" inden for *Teknologi*-kategorien.

4.1 Ledelsesforankring og ressourcer

Som alle andre dele af informationssikkerhedsarbejdet skal et måleprogram ledelsesforankres. Det betyder, at ledelsen aktivt skal godkende de forretningsmæssige målsætninger for måleprogrammet samt sikre finansieringen af det. Et måleprogram har endvidere den egenskab, at en væsentlig del af resultaterne er velegnet til at indgå i ledelsesrapportering. En god indikator på ledelsesforankringen er derfor, om rapporteringen løbende efterspørges og giver anledning til korrigerende handlinger.

Det kræver ressourcer i form af kompetencer og tid at opretholde et målepunktsprogram. Hvor mange ressourcer afhænger dels af antallet af målepunkter, virksomheden vælger at implementere, dels af graden af automatisering af registrering, udtræk og behandling af måledata.

Det er ikke usandsynligt, at der i mange tilfælde vil være en egentlig businesscase i at etablere et målepunktsprogram. Opfølgningen på måleprogrammet kan betragtes som forebyggende sikkerhedsarbejde,
og målingerne er et middel til at effektivisere dette arbejde, som alligevel skulle være udført. Der vil derfor være arbejdstid at spare i det daglige arbejde og potentielt lavere ekstraomkostninger til oprydning, når hændelsen rammer.

4.2 Betydningen af virksomhedens modenhed

Nogle målepunkter har størst værdi, når virksomheden er på et bestemt styringsmæssigt modenhedsniveau. Det gælder mere generelt de målepunkter, som siger noget om procesforbedrende og modenhedsopbyggende indsatser. F.eks. kan man i forskellige sammenhænge måle på det antal af korrigerende handlingsplaner, en given måling giver anledning til. Men efterhånden som den arbejdsproces, der ligger bag målepunktet bliver mere og mere velfungerende, vil den også give anledning til færre behov for at justere. Og så vil målepunktet gradvist miste sin betydning. Modsat kan man pege på målinger, der siger noget om intensiteten af eksterne trusler, f.eks. udtræk fra IDS-systemet vedrørende forekomsten af malware-anslag mod netværket. De vil som hovedregel være lige relevante uanset modenhed.

En tommelfingerregel i den sammenhæng kunne være:

- Der vil være flere relevante målepunkter i *Teknologi*-kategorien, jo mere moden virksomheden er.
- Målepunkter i *Processer- og Mennesker*-kategorien vil have størst værdi for virksomheden, jo mindre moden den er.
- Jo højere modenhed desto flere målepunkter, der vedrører opfølgning og forbedring af informationssikkerhedsstyringen
- Jo lavere modenhed desto flere målepunkter, der vedrører planlægning og implementering af informationssikkerhedsaktiviteter.

Det er derfor vigtigt at revurdere virksomhedens portefølje af målepunkter med jævne mellemrum i forhold til den styringsmæssige modenhed, som virksomheden har opnået. Denne vurdering bør give anledning til en løbende udskiftning af målepunkter, så de matcher den aktuelle udfordring (opbygning af ledelsessystem vs. detaljeret opfølgning på tekniske indikatorer).

5. Skabelon for beskrivelse af målepunkter

Til at beskrive målepunkterne er valgt en fast skabelon, der er en lettere modificeret udgave af ”Measurement Construct Identification”-skabelonen i ISO/IEC27004 (Informationsteknologi – Effektivitetsmålinger).
Den er forenklet i forhold til udgaven i ISO/IEC27004 for at gøre anvendelsen af målepunkterne mere operationel og mindre omstændelig, men det står den enkelte virksomhed frit at udbygge beskrivelsen af de foreslåede målepunkter med attributter fra den fulde model, såfremt der er behov herfor.

Målepunktsdefinition

Betegnelse for målepunkt	Kort beskrivelse af målepunktet
Roller og ansvar for målepunkt	For hvert målepunkt virksomheden vælger at anvende, bør det fastlægges, "hvem der gør hvad" i forhold til målingen. Dette kan f.eks. angives i et RACI-paradigme (alternativt I-D-O, Informed, Decision, Ownership). (R)esponsible har ansvar for målepunktsbeskrivelsen, herunder fastsættelse af aflæsnings- og rapporteringsfrekvens samt tærskelværdier. R har endvidere det udførende ansvar i forhold til, at målingen udføres. (A)ccountable er sponsor, som skal allokere ressourcer, til at målingen kan udføres, og for at der følges op med korrigerende handlinger, hvis målingen falder uden for tærskelværdierne. Det vil ofte være CIO/it-chef. (C)onsulted er alle de involverede medarbejdere, der bidrager til datagrundlaget for målingen. (I)nformed er alle de medarbejdere, der modtager rapportering omkring målingen. I defineringen af de 22 indikatorer er I som eksempel både tildelt bestemte rolleindehavere (f.eks. CEO) og organisatoriske strukturer (f.eks. "it-sikkerhedsudvalget"). Den enkelte virksomhed skal overveje dette på baggrund af sin organisatoriske opbygning.
Type måling	• Objektiv måling - baseret direkte på en observeret værdi (målbar). • Subjektiv måling - udtryk for en menneskelig (subjektiv) vurdering af observationens betydning.
COBIT-proces som målepunktet vedrører	Henvisning til relevant COBIT-proces.
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Henvisning til relevant sikkerhedsområde fra ISO/IEC 27002:2005.
Anbefalet modenhed	Her anføres den modenhed af informationssikkerhedsstyringen, som anbefales som forudsætning for at kunne gennemføre målingen. Skala: Høj – Middel – Lav. Høj modenhed er

	kendetegnet ved, at virksomheden har et veludbygget kontrolmiljø, hvor sikringsforanstaltningerne har en høj operationel effektivitet og i høj grad er automatiserede. Middel modenhed er kendetegnet ved en god beskrivelse af sikringsforanstaltningerne, men der forekommer afvigelser i udførelsen af kontrolaktiviteterne. Foranstaltningerne er i højere grad manuelt baserede. Lav modenhed kendetegner en virksomhed, der har de basale elementer af ISMS'et på plads men stadig er i en opbygningsfase i forhold til kontrolmiljøet.
Forudsætninger	Her anføres andre forudsætninger end modenheden, der skal være til stede for at kunne udføre målingen: tilstødende processer, dokumentation, it-administrative værktøjer m.v.

Register/database/fortegnelse/person hvorfra målingen skal aflæses	Her angives kilden(erne), som indeholder datagrundlaget til at generere målepunktet. Datagrundlaget kan være genereret løbende, men kan også være resultatet fra punktvise aktiviteter (f.eks. resultat fra awareness-kampagne).
Værdi/attribut, der skal trækkes fra systemerne og eventuel beregningsmetodik	En mere præcis angivelse af, hvilke specifikke data, der skal trækkes fra systemerne samt eventuelt en angivelse af, hvorledes data skal behandles for at nå frem til den endelige måling. Følgende nøgleord illustrerer forskellen mellem de *rå data* og et *brugbart målepunkt*: 
Frekvens for aflæsning	Her angives aflæsningsfrekvens for data.
Ønsket tendens	Her angives, om målingen bør være stigende, faldende eller stabil over tid. Hvis der er en target-værdi (mål), angives denne også.
Tærskelværdier	Angivelse af tærskler over eller under hvilke, der bør iværksættes korrigerende handlinger.
Frekvens for rapportering	Data er ikke nødvendigvis sammenfaldende med aflæsningsfrekvens. Det angives, hvem der rapporteres til i henhold til RACI.

6. Målingsprocessen: Hvem og Hvordan?

6.1 Gennemførelse af en måling

Selve målingsprocessen har 3 centrale stadier, der skal udføres eller være til stede for, at måleindsatsen får den ønskede effekt.

Klarlæg forudsætninger for målingen

En af de mest centrale forudsætninger vil i de fleste tilfælde være, at datagrundlaget (input til målingen) er til stede. Om det er tilfældet kan afhænge af, at andre kontroller, der ikke har direkte forbindelse til målingen er effektive (f.eks. vil alle målinger, hvor ServiceDesk-værktøjet er kilde til datagrundlaget, være afhængige af en velfungerende Incident Management-proces). En anden forudsætning kan være, at en bestemt teknologi, der skal understøtte dataindsamlingen er implementeret og konfigureret (f.eks. et IDS-værktøj).

Foretag udtræk

På dette tidspunkt er det væsentligt kun at udtrække de data fra kilden, som er nødvendige for målingen. Endvidere skal eventuelle beregninger, som data skal udsættes for være definerede og muliggjorte (eventuelt med regneark, BI-værktøj eller lignende). I visse tilfælde vil kilden til data ikke være elektroniske registre. I så fald kan det være nødvendigt at planlægge interviews eller ”field trips” med henblik på at foretage de nødvendige observationer. Oplysninger om datakilder m.v. bør være dokumenteret som en del af målepunktsdefinitionen, jf. afsnit 4.

Rapportering

Sidste hovedaktivitet er rapporteringen. For at målingerne skal kunne resultere i eventuelle korrigerende handlinger, er det vigtigt, at de rapporteres til de personer i organisationen, der har mandat og ressourcer til at træffe beslutninger om handlingsplaner. Det konkrete rapporteringspunkt samt rapporteringsfrekvens bør være defineret som en del af målepunktsdefinitionen, jf. afsnit 4. Flere målepunkter kan med fordel rapporteres samlet til samme modtager. Rapporteringsfrekvens og -form kan med fordel følge det, som er anvist i den overordnede informationssikkerhedspolitik for virksomheden.

Det er vigtigt, at rapporteringen anvender de visuelle og andre formmæssige virkemidler, som normalt anvendes i virksomheden (”trafiklys”, diagrammer, mv.), således der ikke ”opfindes” noget specielt til dette formål.

7. Målepunkter

7.1 Generiske målepunkter

Et antal målepunkter, der kan henføres til *Mennesker*-kategorien er generiske i den forstand, at målepunkterne er relevante for alle sikkerhedsområderne:

1. Andel af overskredne tærskelværdier, der resulterer i korrigerende handlinger. Hvis en konkret måling overskrider de tærskelværdier, der i forvejen er besluttet, bør det resultere i en indsats for at styrke sikkerheden på det målte område. Det generiske målepunkt siger noget om viljen til at allokere ressourcer til at agere på afvigelser. Dette målepunkt bør have en stigende tendens mod 100 %.
2. Procent målinger, der gennemføres og rapporteres rettidigt og korrekt. Målepunktet siger noget om måleprogrammets effektivitet i relation til at få målinger udført med den rigtige frekvens og rapporteret korrekt. Dette målepunkt bør have en stigende tendens mod 100 %.
3. Antal nye retningslinjer, der udarbejdes inden for de sikkerhedsområder, som virksomheden ønsker at efterleve. Målepunktet siger noget om det aspekt i informationssikkerhedsstyringen og opbygningen af ISMS'et, der har at gøre med at *beskrive* relevante retningslinjer for sikringsforanstaltninger (designfasen). Dette målepunkt bør have en stigende tendens i opbygningsfasen af ISMS'et.

7.2 22 målepunkter

De følgende 22 målepunkter er eksempler på indikatorer, som virksomheder kan tage udgangspunkt i, når de ønsker at implementere et måleprogram for informationssikkerhed.

Målepunkterne er udvalgt fra en liste på ca. 90 målepunkter fra forskellige kilder, som er gengivet i bilag 1.

De 22 målepunkter er udvalgt indenfor samtlige 13 sikkerhedsområder, jf. afsnit 2, og er udvalgt ud fra, at de:

- Skal være realistiske at sætte i værk, såfremt forudsætningerne er til stede. Bemærk, at netop forudsætningerne kan indebære krav til en vis modenhed i virksomhedens informationssikkerhedsstyring.
- I videst muligt omfang skal være direkte indikatorer for sikkerhedsniveauet.

Målepunkt	Kategori
1. Organisatorisk niveau for godkendelse af informationssikkerhedspolitik og – strategi.	Mennesker
2. Antal godkendte dispensationer fra informationssikkerhedspolitikken.	Proces
3. Andel af planlagt ledelsesrapportering, som er gennemført.	Proces
4. Andel af kravspecifikationer i udviklingsprojekter med godkendte informationssikkerhedskrav (ikke-funktionelle krav).	Proces
5. Andel af prioritet 1-risici (høj konsekvens og høj sandsynlighed) i forhold til det totale antal kendte og dokumenterede risici.	Mennesker
6. Andel af informationsaktiver, der har fået tildelt en ejer.	Proces
7. Antal forekomster af ikke-godkendt udstyr på netværket.	Teknologi
8. Antal informationssikkerhedsrelevante uddannelsestimer pr. medarbejder i den samlede medarbejderstab.	Mennesker
9. Andel af ansættelser i virksomheden, hvor der foretages forudgående screening.	Mennesker
10. Andel af fysisk adgang til interne områder, der sker uden om adgangskontrollen.	Teknologi
11. Andel af systemer, som følger den fastsatte sikkerhedsbaseline.	Teknologi
12. Antal firewallregler, som ikke er godkendt.	Teknologi
13. Antal sikkerhedshændelser, der er opstået som følge af gennemførsel af ændringer i driftsmiljøet.	Proces

14. Procentdel af adgangsrettigheder i forretningsapplikationer, der korrigeres som følge af periodisk revurdering.	Proces
15. Grad af teknisk håndhævelse af krav til password-kvalitet.	Teknologi
16. Procentdel af teknisk infrastruktur og software, som indgår i patch management processen.	Proces
17. Antal ukendte sårbarheder, som identificeres ved hjælp af teknisk sårbarhedsscanning.	Teknologi
18. Andel af indrapporterede sikkerhedshændelser, der løses inden for tidsrammen.	Proces
19. Antal opfølgningspunkter, som seneste test af beredskabsplanen har givet anledning til.	Proces
20. Andel af kritiske systemer fra risikoanalysen, der er dækket af beredskabsplanen.	Proces
21. Antal anmærkninger fra intern (it) revision, myndigheder og tilsyn pr. løbende år, som kræver opfølgning.	Mennesker
22. Andel af medarbejdere med ikke-arbejdsbetinget adgang til personfølsomme oplysninger.	Proces

8. Målepunktsdefinitioner

8.1 Målepunkt: Organisatorisk niveau for godkendelse af informationssikkerhedspolitik og -strategi

Målepunktsdefinition	
Betegnelse for målepunkt	**Organisatorisk niveau for godkendelse af informationssikkerhedspolitik og -strategi (COBIT)**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = CFO (CIO) C = CEO, Bestyrelsen I = CEO, Systemejere
Type måling	Objektiv
Vedrører COBIT proces	AP002 (Manage Strategy)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 1: Politik og Strategi
Modenhed	Lav
Forudsætninger	Der udarbejdes en informationssikkerhedspolitik/-strategi, der er underlagt en ledelsesmæssig godkendelse.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Underskriftsblad og/eller referat fra møde, hvor godkendelse er sket.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Organisatorisk placering af den medarbejder, der har foretaget endelig godkendelse af dokumenterne.
Frekvens for aflæsning	1 x årligt.
Ønsket tendens	Godkendelse bør være forankret højest muligt i det organisatoriske hierarki; CFO eller Bestyrelse (evt. CIO, men der vil i så fald være risiko for interessekonflikter, som bør overvejes).
Tærskelværdier	Hvis godkendelse er forankret lavere end C-level, bør godkendelseskravene revurderes.
Frekvens for rapportering	Rapporteres til CEO årligt.

8.2 Målepunkt: Antal godkendte dispensationer fra informationssikkerhedspolitikken

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal godkendte dispensationer fra informationssikkerhedspolitikken (COBIT)**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = CFO (CIO) C = CEO I = CEO, Systemejere
Type måling	Objektiv
Vedrører COBIT proces	AP003 (Manage Enterprise Architecture)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 1: Politik og Strategi
Modenhed	Høj
Forudsætninger	Der er implementeret retningslinjer, som kræver, at der dispenseres for afvigelser fra it-sikkerhedspolitikken (det kan f.eks. være dispensation fra krav om miljøadskillelse). Afvigelser fra retningslinjer, der er udstedt i medfør af it-sikkerhedspolitikken, skal i denne sammenhæng betragtes som afvigelser fra it-sikkerhedspolitikken. Dispensationer skal dokumenteres. Det udgør en risiko for målepunktets validitet, såfremt der i virksomheden er en for udbredt praksis med at tillade mundtlige eller på anden hvis udokumenterede dispensationer.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Register over dispensationer fra informationssikkerheds-politikken.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Samlet antal dispensationer.
Frekvens for aflæsning	Kvartalsvist.
Ønsket tendens	Faldende mod 0.
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CEO årligt.

8.3 Målepunkt: Andel af planlagt ledelsesrapportering, som er gennemført

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af planlagt ledelsesrapportering, som er gennemført (COBIT)**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = CFO (CIO) C = CEO, Bestyrelsen I = CEO, Systemejere
Type måling	Objektiv
Vedrører COBIT proces	EDM05 (Ensure Stakeholder Transparency)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 2: Styring og organisering
Modenhed	Middel
Forudsætninger	Der er implementeret retningslinjer for, hvad, hvornår og til hvem, der skal rapporteres om informationssikkerhedsmæssige forhold. Der anvendes et dokumenthåndteringssystem (ESDH), der indeholder stamdata om, hvornår givne dokumenter er forelagt til review/godkendelse.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Dokumenthåndteringssystemet.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Dato for oversendelse af rapporteringsdokumenter eller dato for referater af møder, hvor der er sket rapportering, holdes op imod deadline i henhold til retningslinjerne. Antal overskridelser af deadlines pr. løbende år tælles op. Det kan overvejes at supplere beregningen med en faktor, der tager højde for størrelsen af overskridelsen (antal dage), således at mindre overskridelser får en mindre vægt.
Frekvens for aflæsning	Årligt
Ønsket tendens	Faldende mod ingen overskridelser af deadlines.
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CEO årligt.

8.4 Målepunkt: Andel af kravspecifikationer i udviklingsprojekter med godkendte informationssikkerhedskrav (ikke-funktionelle krav)

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af kravspecifikationer i udviklingsprojekter med godkendte informationssikkerhedskrav (ikke-funktionelle krav) (COBIT)**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = CIO C = It-projektledere, it-programledere, porteføl-ge-managers I = CEO
Type måling	Objektiviseret
Vedrører COBIT proces	AP005 (Manage Portfolio), BAI01 (Manage Programs and Projects)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 2: Styring og organisering
Modenhed	Middel
Forudsætninger	Der udarbejdes kravspecifikationer på alle udviklingsopgaver, der overstiger rammerne for anvendelse af RfC'er. Hvis styringen af udviklingsprojekter ikke er centraliseret i et projektkontor eller lign., kan det være nødvendigt at indsamle oplysninger ved at kontakte de steder i virksomheden, hvor udviklingsprojekter kunne være forankret.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Fortegnelse over virksomhedens (it) udviklingsprojekter.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Kravspecifikationer for alle projekter gennemgås, og det konstateres, om disse indeholder tilfredsstillinde informationssikkerhedskrav (delvist subjektiv vurdering). Målingen udtrykkes i procent kravspecifikationer, der lever op til kravene.
Frekvens for aflæsning	Årligt
Ønsket tendens	Stigende mod 100%.
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CEO årligt.

8.5 Målepunkt: Andel af prioritet 1-risici (høj konsekvens og høj sandsynlighed) i forhold til det totale antal kendte og dokumenterede risici.

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af prioritet 1-risici (høj konsekvens og høj sandsynlighed) i forhold til det totale antal kendte og dokumenterede risici.**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = CIO C = It-projektledere, it-programledere, porteføl-ge-managers I = CEO, Bestyrelsen
Type måling	Subjektiv
Vedrører COBIT proces	AP012 (Manage Risk)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 3: Risikostyring
Modenhed	Middel
Forudsætninger	Der udarbejdes periodiske it-risikoanalyser på det forretningsmæssige/strategiske plan, hvor risikoen for tab af Fortrolighed, Integritet og Tilgængelighed til virksomhedens informationsaktiver vurderes i et forretningsmæssigt perspektiv og kvantificeres (konsekvens x sandsynlighed) således, at de kan rangordnes indbyrdes og kategoriseres efter alvorlighed.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Seneste risikoanalyserapport eller datagrundlag for denne.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Antal risici i den mest alvorlige kategori (”Uacceptabelt”) sættes i forhold til det samlede antal risici (alle kategorier).
Frekvens for aflæsning	Årligt
Ønsket tendens	Faldende mod 0%.
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CEO årligt.

8.6 Målepunkt: Andel af informationsaktiver, der har fået tildelt en ejer

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af informationsaktiver, der har fået tildelt en ejer (COBIT)**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = CIO C = Systemejere I = CIO
Type måling	Objektiv
Vedrører COBIT proces	BAI09 (Manage Assets)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 4: Styring af aktiver
Modenhed	Lav/Middel
Forudsætninger	At systemejere i forretningen accepterer rollen og de opgaver, der følger med. Det anbefales at bruge en bred definition af begrebet *informationsaktiver,* som også inkluderer enkelt-komponenter, men det kræver dog en relativt højere modenhed.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	CMDB eller lignende værktøj. Fortegnelse over informationsaktiver.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Hvorvidt aktiver har ”flag” sat ved ”Ejer tildelt”. Målepunktet er procent aktiver, hvor ejerskab er tildelt.
Frekvens for aflæsning	2 x årligt
Ønsket tendens	Stigende mod 100%.
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CIO årligt.

8.7 Målepunkt: Antal forekomster af ikke-godkendt udstyr på netværket

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal forekomster af ikke-godkendt udstyr på netværket (COBIT)**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = CIO C = Afdelingsledere eller ledere af forretningsenheder I = CIO
Type måling	Objektiv
Vedrører COBIT proces	BAI09 (Manage Assets)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 4: Styring af aktiver
Modenhed	Høj
Forudsætninger	Målepunktet forudsætter, at det er teknisk muligt at afsløre uautoriseret tilkoblet udstyr. En måde at gøre dette på er anvendelse af 802.1X autentificering af udstyr..
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Opfølgningslog fra det driftsadministrative værkstøj, der anvendes til overvågning af netværkstilslutninger (faste og trådløse)
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Antal afviste tilslutningsforsøg.
Frekvens for aflæsning	Kvartalsvist
Ønsket tendens	Faldende mod 0.
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CIO årligt.

8.8 Målepunkt: Antal informationssikkerhedsrelevante uddannelsestimer pr. medarbejder i den samlede medarbejderstab

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal informationssikkerhedsrelevante uddannelsestimer pr. medarbejder i den samlede medarbejderstab (COBIT)**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = HR C = Afdelingsledere eller ledere af forretningsenheder I = CIO
Type måling	Objektiv
Vedrører COBIT proces	AP007 (Manage Human Ressources)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 5: Medarbejdersikkerhed
Modenhed	Lav
Forudsætninger	N/A
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	HR-system eller lign, hvor medarbejdernes uddannelsesforløb står registreret.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Antal uddannelsestimer, der kan henføres til temaer inden for informationssikkerhed. Målepunktet kan evt. differencernes mellem den samlede medarbejderstab og medarbejdere i it-sikkerhedsfunktionen.
Frekvens for aflæsning	Årligt
Ønsket tendens	Stigende mod XX (skal defineres af virksomheden).
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CIO årligt.

8.9 Målepunkt: Andel af ansættelser i virksomheden, hvor der foretages forudgående screening

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af ansættelser i virksomheden, hvor der foretages forudgående screening**
Roller og ansvar for målepunkt	R = CISO, it-sikkerhedskoordinator A = HR C = Afdelingsledere eller ledere af forretningsenheder I = CEO
Type måling	Objektiv
Vedrører COBIT proces	AP007 (Manage Human Ressources)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 5: Medarbejdersikkerhed
Modenhed	Middel
Forudsætninger	Der skal være retningslinjer i virksomheden, der opstiller krav om, at kandidater til stillinger (evt. kun stillinger på højrisikoområder) udsættes for kontrol af referencer og/eller straffeattest (screening) forinden ansættelse.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	HR-system eller lignende
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Registrering af, hvorvidt screening er foretaget.
Frekvens for aflæsning	Årligt
Ønsket tendens	Stigende mod 100%
Tærskelværdier	Skal besluttes af virksomheden i hvert enkelt tilfælde.
Frekvens for rapportering	Rapporteres til CISO årligt.

8.10 Målepunkt: Andel af fysisk adgang til interne områder, der sker uden om adgangskontrollen

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af fysisk adgang til interne områder, der sker uden om adgangskontrollen.**
Roller og ansvar for målepunkt	R = Leder af fysisk sikkerhedsafdeling A = CEO C = CISO I = Sikkerhedsudvalg
Type måling	Objektiv
Vedrører COBIT-proces	DSS05 (Manage Security Services)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 6: Fysisk sikkerhed
Modenhed	Middel
Forudsætninger	Det forudsættes, at der anvendes et automatisk adgangskontrolsystem (ADK), men at der ikke er implementeret sluser/man traps.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Der udvælges et adgangspunkt, hvor der fra eksterne områder kan opnås adgang til interne kontorlokaler.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Der foretages en stikprøve ved observation af adgangspunktet, og det noteres, hvor mange procent af adgange, der foregår uden brug af ADK-systemet (dvs. i form af piggybacking).
Frekvens for aflæsning	2 x årligt
Ønsket tendens	Faldende eller stabil under 5 %.
Tærskelværdier	Hvis målepunktet overstiger 5 %, bør der iværksættes korrigerende handlinger. F.eks. i form af informationskampagner eller implementering af sluser/man traps, øget overvågning eller tilsvarende.
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.11 Målepunkt: Andel af systemer, som følger den fastsatte sikkerhedsbaseline

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af systemer, som følger den fastsatte sikkerheds-baseline.**
Roller og ansvar for målepunkt	R = Driftschef A = CIO C = Systemejere I = CISO, Sikkerhedsudvalg
Type måling	Objektiv
Vedrører COBIT-proces	DSS01 (Manage Operations)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 7: Styring af netværk og drift
Modenhed	Høj
Forudsætninger	Det forudsættes, at der anvendes et monitoreringsværktøj, hvormed det er muligt at verificere, hvor mange systemer, der har implementeret de sikkerhedspolitikker, som er fastsat for det enkelte område. Ved lavere modenhed kan man nøjes med at gennemføre stikprøver.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Et eller flere monitoreringsværktøjer, som kontrollerer en eller flere grupper af systemer, f.eks. et domæne.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Ved hjælp af monitoreringsværktøjet foretages et udtræk over antallet af systemer, som efterlever den fastsatte sikkerheds-baseline. Systemer omfatter udstyr, OS, databaser, applikationer m.v. F.eks. hvor mange servere i et domæne, som efterlever den fastsatte domæne-politik.
Frekvens for aflæsning	12 x årligt
Ønsket tendens	Faldende eller stabil under 1 %.
Tærskelværdier	Hvis målepunktet overstiger 0 %, bør der iværksættes en undersøgelse af årsagen hertil.
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.12 Målepunkt: Antal firewallregler, som ikke er godkendt

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal firewallregler, som ikke er godkendt**
Roller og ansvar for målepunkt	R = Driftschef A = CIO C = Ansvarlige for udvikling, test og drift I = CISO, Sikkerhedsudvalg
Type måling	Objektiv
Vedrører COBIT-proces	BAI07 Manage Change Acceptance and Transitioning
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 7: Styring af netværk og drift
Modenhed	Høj
Forudsætninger	Der er krav om funktionsadskillelse (godkender-proces) og dokumentation af regelændringer på firewall. Virksomheden råder over værktøj, der kan analysere regelsættet og generere en ændringsrapport.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Automatisk genereret ændringsrapport over firewall-regelsættet samt ændringsanmodninger.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Ændringsrapporten sammenholdes med ændringsanmodningerne, og udokumenterede ændringer registreres.
Frekvens for aflæsning	4 x årligt
Ønsket tendens	Faldende eller stabil under 1.
Tærskelværdier	Hvis målepunktet overstiger 0, bør der iværksættes en undersøgelse af årsagen hertil.
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.13 Målepunkt: Antal sikkerhedshændelser, der er opstået som følge af gennemførsel af ændringer i driftsmiljøet

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal sikkerhedshændelser, der er opstået som følge af gennemførsel af ændringer i driftsmiljøet (COBIT).**
Roller og ansvar for målepunkt	R = Driftschef A = CIO C = Change Manager I = CISO, Sikkerhedsudvalg
Type måling	Objektiv
Vedrører COBIT-proces	BAI06 (Manage Changes)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 7: Styring af netværk og drift
Modenhed	Høj
Forudsætninger	Det er en forudsætning, at relevante hændelser kategoriseres som sikkerhedshændelser, og at der sker opfølgning på resultatet af gennemførte RfC'er (ændringsønsker).
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Helpdesk-værktøj. (Ændringsstyringsværktøj).
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Antal sikkerhedshændelser, der har direkte forbindelse til gennemførelsen af en RfC (ændringsønske) tælles op.
Frekvens for aflæsning	2 x årligt
Ønsket tendens	Faldende mod 0.
Tærskelværdier	Hvis målepunktet overstiger X, bør der iværksættes en undersøgelse af årsagen hertil, herunder af kvaliteten af de operationelle risikovurderinger, såfremt sådanne foretages i forbindelse med RfC-anmodninger (ændringsønsker).
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.14 Målepunkt: Procentdel af adgangsrettigheder i forretningsapplikationer, der korrigeres som følge af periodisk revurdering

Målepunktsdefinition	
Betegnelse for målepunkt	**Procentdel af adgangsrettigheder i forretningsapplikationer, der korrigeres som følge af periodisk revurdering.**
Roller og ansvar for målepunkt	R = Systemejere, autorisationsansvarlige A = CIO C = CISO I = Sikkerhedsudvalg
Type måling	Objektiv
Vedrører COBIT-proces	DSS05 (Manage Security Services)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 8: Adgangsstyring
Modenhed	Middel
Forudsætninger	Det forudsættes, at der foretages periodisk revurdering af adgangsrettigheder i forretningsapplikationer. Det udgør en risiko for målingens validitet, hvis vurderingen af adgangsrettigheder har proforma-karakter. Systemejere bør trænes i opgaven omkring periodisk revurdering.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Resultatet fra den seneste revurdering af adgangsrettigheder.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Med udgangspunkt i antallet af ændrede adgangsrettigheder og det samlede antal revurderede adgangsrettigheder beregnes, hvor mange procent af rettighederne, som er blevet korrigeret.
Frekvens for aflæsning	2 x årligt
Ønsket tendens	Faldende eller stabil under 5 %.
Tærskelværdier	Hvis målepunktet overstiger 5 %, bør der iværksættes en undersøgelse af årsagen hertil.
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.15 Målepunkt: Grad af teknisk håndhævelse af krav til passwordkvalitet

Målepunktsdefinition	
Betegnelse for målepunkt	**Grad af teknisk håndhævelse af krav til passwordkvalitet**
Roller og ansvar for målepunkt	R = Driftschef A = CIO C = Systemejere I = CISO, Sikkerhedsudvalg
Type måling	Subjektiv
Vedrører COBIT-proces	DSS05 (Manage Security Services)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 8: Adgangsstyring
Modenhed	Lav
Forudsætninger	Det forudsættes, at der er fastsat en politik for kvaliteten (kompleksiteten) af passwords.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Domænepolitikker og systemopsætninger.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Sikkerhedspolitikkens krav til passwordkvalitet sammenholdes med de implementerede tekniske kontroller, og der foretages en kvalitativ vurdering af, i hvor høj grad den tekniske opsætning sikrer håndhævelse af politikkens krav. Vurderingen kan foretages på en 1-5 skala, hvor 1 er meget lav, og 5 er meget høj.
Frekvens for aflæsning	2 x årligt
Ønsket tendens	Stigende eller stabil på et højt niveau.
Tærskelværdier	Hvis målepunktet ikke er på et højt niveau, bør der iværksættes en undersøgelse af årsagen hertil.
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.16 Målepunkt: Procentdel af teknisk infrastruktur og software, som indgår i patch management processen

Målepunktsdefinition	
Betegnelse for målepunkt	**Procentdel af teknisk infrastruktur og software, som indgår i patch management processen.**
Roller og ansvar for målepunkt	R = Driftschef A = CIO C = Systemejere I = CISO, Sikkerhedsudvalg
Type måling	Objektiv
Vedrører COBIT-proces	DSS05 (Manage Security Services)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 9: Styring af udviklingsprocesser
Modenhed	Middel
Forudsætninger	Det forudsættes, at der er overblik over infrastruktur og software, som reelt anvendes i organisationen, f.eks. ved brug af et værktøj, som automatisk registrerer dette. Det er desuden en forudsætning, at der er etableret en patch management proces.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Liste eller værktøj, som indeholder alle anvendte over infrastruktur og software samt liste over dem, som indgår i patch management processen.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Der foretages en sammenligning, og det noteres, hvor mange af de anvendte over infrastruktur komponenter og software, som ikke indgår i patch management processen.
Frekvens for aflæsning	2 x årligt
Ønsket tendens	Faldende eller stabil under X.
Tærskelværdier	Hvis målepunktet overstiger X, bør der iværksættes en undersøgelse af årsagen hertil.
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.17 Målepunkt: Antal ukendte sårbarheder, som identificeres ved hjælp af teknisk sårbarhedsscanning

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal ukendte sårbarheder, som identificeres ved hjælp af teknisk sårbarhedsscanning.**
Roller og ansvar for målepunkt	R = Driftschef A = CIO C = Systemejere I = CISO, Sikkerhedsudvalg
Type måling	Objektiv
Vedrører COBIT-proces	MEA02 (Monitor, Evaluate and Assess the System of Internal Control)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 9: Styring af udviklingsprocesser
Modenhed	Middel
Forudsætninger	Det forudsættes, at der foretages periodiske sårbarhedsscanninger eller sikkerhedstest.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Resultatet fra seneste scanning.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Antallet af identificerede ukendte sårbarheder.
Frekvens for aflæsning	1 x årligt
Ønsket tendens	Faldende eller stabil under X.
Tærskelværdier	Hvis målepunktet overstiger X, bør der iværksættes en undersøgelse af årsagen hertil.
Frekvens for rapportering	Rapporteres ved hver aflæsning.

8.18 Målepunkt: Andel af indrapporterede sikkerhedshændelser, der løses inden for tidsrammen

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af indrapporterede sikkerhedshændelser, der løses inden for tidsrammen**
Roller og ansvar for målepunkt	R = Sikkerhedskoordinator A = CIO C = Helpdesk, systemejere, leverandører I = CEO, Systemejere
Type måling	Objektiv
Målepunktet kan relateres til følgende punkt fra COBIT	DSS02 (Manage Service Requests and Incidents)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 10: Hændelsesstyring
Modenhed	Middel
Forudsætninger	Begrebet *sikkerhedshændelse* skal være defineret. Alle sikkerhedshændelser indrapporteres, og tidspunktet for opdagelse af hændelsen registreres såvel som tidspunktet for, hvornår hændelsen er løst. Det er desuden en forudsætning, at den aftalte tidsramme for, hvornår en hændelse skal være løst, er angivet.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Sikkerhedskoordinatoren
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Der foretages et udtræk af antal registrerede sikkerhedshændelser indenfor de sidste 6 måneder. Dette antal sættes i forhold til det antal sikkerhedshændelser, der er løst inden for tidsrammen.
Frekvens for aflæsning	2 x årligt, f.eks. 31/1, 31/7.
Ønsket tendens	Målepunktet bør være stigende mod 100 %.
Tærskelværdier	Hvis målepunktet er under 80 % ved 2 på hindanden følgende målinger, bør der iværksættes undersøgelser for, hvilken del af hændelsesstyringen, der sænker processen, eller alternativt om tidsrammen er urealistisk lav.

Frekvens for rapportering	Rapporteres til CIO ved hver aflæsning.

8.19 Målepunkt: Antal opfølgningspunkter, som seneste test af beredskabsplanen har givet anledning til

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal opfølgningspunkter, som seneste test af beredskabsplanen har givet anledning til.**
Roller og ansvar for målepunkt	R = Beredskabskoordinatoren A = CIO C = Systemejere, Sikkerhedskoordinatoren I = CEO, Dataejere
Type måling	Objektiv
Målepunktet kan relateres til følgende punkt fra COBIT	DSS04 (Manage Continuity)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 11: Beredskabsstyring
Modenhed	Middel
Forudsætninger	Beredskabsplanen testes regelmæssigt, og opfølgningspunkter afledt heraf registreres. Det udgør en risiko for målingens validitet, hvis de anvendte testscenarier ikke er fuldt dækkende i forhold til beredskabsplanens operationelle del.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Beredskabskoordinatoren
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	De opfølgningspunkter, som forrige test af beredskabsplanen gav anledning til sammenlignes med de fra den seneste test. Antallet af ens opfølgningspunkter noteres som værdi for målepunktet.
Frekvens for aflæsning	2 x årligt, f.eks. 31/1, 31/7.
Ønsket tendens	Målepunktet bør være faldende mod 0.
Tærskelværdier	Hvis målepunktet overstiger 0, indikerer det, at der ikke er fulgt effektivt op på sidste beredskabstest, og der skal udarbejdes handlingsplaner, som sikrer løsninger på de relevante problemer.
Frekvens for rapportering	Rapporteres til CIO ved hver aflæsning.

8.20 Målepunkt: Andel af kritiske systemer fra risikoanalysen, der er dækket af beredskabsplanen

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af kritiske systemer fra risikoanalysen, der er dækket af beredskabsplanen.**
Roller og ansvar for målepunkt	R = Beredskabskoordinatoren A = CIO C = Systemejere, Sikkerhedskoordinatoren I = CEO, Dataejere
Type måling	Objektiv
Målepunktet kan relateres til følgende punkt fra COBIT	DSS04 (Manage Continuity)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 11: Beredskabsstyring
Modenhed	Lav
Forudsætninger	Virksomheden/organisationen har en regelmæssigt opdateret risikoanalyse og beredskabsplan.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Aktiv-fortegnelsen i risikoanalysen, Sikkerhedskoordinatoren.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	De systemer, der fremgår af risikoanalysen som kritiske sammenlignes med de systemer, der er dækket af beredskabsplanen.
Frekvens for aflæsning	2 x årligt, f.eks. 31/1, 31/7.
Ønsket tendens	Målepunktet bør være stigende mod 100 procent.
Tærskelværdier	Hvis målepunktet er under 100 % på 2 af hinanden følgende målinger, bør de manglende kritiske systemer tilføjes til beredskabsplanen, med mindre der er væsentlige hensyn, der taler for det modsatte.
Frekvens for rapportering	Rapporteres til CIO ved hver aflæsning.

8.21 Målepunkt: Antal anmærkninger fra myndigheder, tilsyn og intern (it) revision pr. år, som kræver opfølgning

Målepunktsdefinition	
Betegnelse for målepunkt	**Antal anmærkninger fra myndigheder, tilsyn og intern (it) revision pr. år, som kræver opfølgning.**
Roller og ansvar for målepunkt	R = Den ansvarlige for compliance A = CIO C = Intern Revision I = CEO
Type måling	Objektiv
Målepunktet kan relateres til følgende punkt fra COBIT	MEA03 (Monitor, Evaluate and Assess Compliance With External Requirements)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 12: Compliance
Modenhed	Middel
Forudsætninger	Virksomheden/organisationen registrerer de anmærkninger, der modtages fra myndigheder, tilsyn og intern (it) revision pr. år.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Den ansvarlige for compliance og efterlevelse af eksterne krav.
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Det samlede antal af anmærkninger fra myndigheder, tilsyn og intern revision pr. år, som kræver opfølgning trækkes ud og benyttes som værdi for dette målepunkt.
Frekvens for aflæsning	1x årligt, f.eks. 31/1.
Ønsket tendens	Målepunktet bør være faldende mod 0.
Tærskelværdier	Hvis målepunktet er stigende på 2 på hinanden følgende målinger, skal der udarbejdes handlingsplaner for effektivisering af arbejdet med compliance på det relevante område.
Frekvens for rapportering	Rapporteres til CIO ved hver aflæsning.

8.22 Målepunkt: Andel af medarbejdere med ikke-arbejdsbetinget adgang til personfølsomme oplysninger

Målepunktsdefinition	
Betegnelse for målepunkt	**Andel af medarbejdere med ikke-arbejdsbetinget adgang til personfølsomme oplysninger.**
Roller og ansvar for målepunkt	R = Sikkerhedskoordinator/ ansvarlig for compliance A = CIO C = Intern revision I = CEO
Type måling	Subjektiv
Målepunktet kan relateres til følgende punkt fra COBIT	MEA03 (Monitor, Evaluate and Assess the System og INternal Control)
Sikkerhedsområde fra ISO/IEC 27002:2005, som målepunktet vedrører	Område 13: Privatlivsbeskyttelse
Modenhed	Middel
Forudsætninger	Organisationen har klassificeret deres data efter graden af følsomhed og fortrolighed.
Register/database/fortegnelse/person, hvorfra målingen skal aflæses	Register over brugeradgange Register over dataklassifikation Sikkerhedskoordinator
Værdi/attribut, der skal trækkes ud og evt. beregningsmetodik	Sikkerhedskoordinatoren vurderer ud fra organisationens dataklassifikation og de brugeradgange, der er til data, hvor stor en andel i procent, der har et reelt behov for at tilgå de følsomme/fortrolige data som led i deres arbejde. Alt efter omfang og overblik laves vurderingen ud fra stikprøveundersøgelser eller en skønsmæssig betragtning fra sikkerhedskoordinatoren.
Frekvens for aflæsning	2 x årligt, f.eks. 31/1, 31/7.
Ønsket tendens	Målepunktet bør være faldende mod 0.
Tærskelværdier	Hvis målepunktet overstiger 0, skal det undersøges, hvilke muligheder, der er, for at afgrænse adgangen til de følsomme oplysninger til de personer, der har et sagligt behov for at tilgå disse.
Frekvens for rapportering	Rapporteres til CIO ved hver aflæsning.

Bilag 1

Liste af målepunkter, der kan anvendes som inspirationskatalog for yderligere målinger. Listen er ikke udtømmende og kan suppleres af organisationens egne specifikke målepunkter:

Politik og strategi		
Mennesker	**Organisatorisk niveau for godkendelse af informationssikkerhedspolitik og -strategi.**	**Antal interessenter, der konsulteres ifm. udarbejdelse og opdatering af informationssikkerhedsstrategi og -politik.**
Proces	**Grad af sammenhæng mellem forretningsmæssige mål og informations-sikkerhedsmål.**	**Forløbet periode siden sidste opdatering.**
	Grad af opfyldelse af ISMS dokumentationskrav (ISO/IEC27001).	**Frekvens af uafhængige eftersyn af informationssikkerhedsstrategi og -politik.**
	Antal godkendte dispensationer fra informationssikkerhedspolitikken.	
Teknologi		

Styring og organisering		
Mennesker	**Grad af repræsentation af sikkerhedsfunktionen i virksomhedens styrende udvalg eller i projekt-styregrupper.**	**Ledelsens grad af tilfredshed med tilrettelæggelsen af informationssikkerhedsstyringen og kvalitet af rapporteringen.**
Proces	**Størrelse af informationssikkerhedsbudget i forhold til branchegennemsnittet.**	**Realiserede informationssikkerhedsudgifter i forhold til budgetterede informationssikkerhedsudgifter.**
	Procent gennemførte informationssikkerhedstiltag vs. planlagte tiltag.	**Procent ledelsesrapportering, der gennemføres som planlagt.**
	Procent kravspecifikationer med godkendte informationssikkerhedskrav (ikke-funktionelle krav).	**Antal gennemførte leverandørvurderinger (allerede benyttede leverandører).**
	Procent leverandør-SLA'er, der indeholder målsætninger inden for	**Antal sikkerhedshændelser, der direkte skyldes forhold hos leverandører.**

	informationssikkerhed.	
Teknologi		

Risikostyring		
Mennesker	**Antal systemejere, der har henvendt sig til sikkerhedsfunktionen med forespørgsler, der relaterer sig til informationsaktivers risikoprofil.**	**Organisatorisk niveau for godkendelse af risici.**
Proces	**(Procent af implementerede sikringsforanstaltninger, der kan relateres direkte til forretningsmæssigt relevante risici for tab af fortrolighed, integritet og tilgængelighed).**	**Procent it-projekter i forbindelse med hvilke, der gennemføres en strategisk risikoanalyse.**
	Procent risici, der vurderes som uacceptable i forhold til det totale antal kendte og dokumenterede risici.	**Udvikling i antal prioritet 1 og 2-risici (i forhold til vurderede aktiver).**
	Antal af ledelsen fravalgte sikringsområder (niveau 2), hvor risikohåndtering er angivet som "accept af risiko".	
Teknologi		

Styring af aktiver		
Mennesker	**Antal hændelser, som skyldes, at den accepterede brug af virksomhedens informationsaktiver er overtrådt.**	
Proces	**Procentdel informationsaktiver, der har fået tildelt en ejer.**	**Procent informationsaktiver, der har fået tildelt en godkendt klassifikation.**
	Antal afvigelser fra konfigurations-baselines.	
Teknologi	**Grad af automatisering af fortegnelser over informationsaktiver (anvendelse af CMDB-værktøj el. lign.).**	**Antal forekomster af ikke-godkendt udstyr på netværket.**

Medarbejdersikkerhed		
Mennesker	**Personale-omsætningshastighed i sikkerhedsfunktionen.**	**Antal informationssikkerhedsrelevante uddannelsestimer pr. medarbejder i sikkerhedsfunktionen/den samlede medarbejderstab.**
	Andel af medarbejderstaben, der har modtaget "introduktion for nye medarbejdere" i informationssikkerhed.	**Antal kvalificerede ansøgere, der dumper kontrol af referencer og straffeattest.**
	Andel overtrædelser af informationssikkerhedspolitikken, der sanktioneres.	**Procent ansættelser, hvor der foretages forudgående screening.**
Proces	**Andel af udleveret udstyr, der er afskrevet som mistet.**	
Teknologi	**Antal brugerkonti, der ikke er lukket efter fratrædelse af medarbejdere.**	

Fysisk sikkerhed		
Mennesker	**Procentdel af medarbejderne som har kendskab til retningslinjerne for håndtering af it-udstyr uden for virksomhedens lokation.**	**Procentdel af adgange til interne områder, der sker uden om adgangskontrollen.**
Proces	**Antal dage siden sidste test af nødstrømsanlæg.**	**Procentdel af fysiske adgangsrettigheder til sikre områder, der korrigeres som følge af periodisk revurdering.**
Teknologi	**Antal autorisationer i ADK-systemet, som ikke er personhenførbare.**	**Procentvis afvigelse af miljømåling (temperatur & luftfugtighed) i datacenter i forhold til de fastsatte grænseværdier.**
	Antal gyldige adgangskort, som ikke er anvendt inden for de seneste 60 dage.	

Styring af kommunikation og drift		
Mennesker		
Proces	**Procentdel af it-systemer, som har fastsat krav til logning.**	**Antal records, der ikke kunne reetableres som forventet ved seneste test af reetablering fra sikkerhedskopi.**
	Antal changes, som afvises på bagrund af en vurdering af de sikkerhedsmæssige konsekvenser.	
Teknologi	**Antal servere/klienter, som har et antivirusprogram, hvor signaturfilerne er opdateret inden for 12 timer.**	**Procentdel af servere i domænet, som følger den fastsatte domænepolitik.**
	Procentdel af infrastruktur, hvor kapacitet overvåges automatisk vha. snmp-traps eller lignende metode.	**Antal firewallregler, som tillader udveksling af data mellem udvikling/test og produktionsmiljø.**

Adgangsstyring		
Mennesker	**Antal succesfulde "social engineering"-angreb (evt. konstateret ved kontrollerede test).**	**Grad af kendskab til informationssikkerhedspolitikkens krav om "arbejdsbetinget behov".**
Proces	**Procent forretningsapplikationer, der ikke provisioneres i henhold til retningslinjerne for bruger- og rettighedsstyring.**	**Antal individuelle rettigheder i forretningsapplikationer, der korrigeres som følge af systemejeres periodiske revurdering af adgangsrettigheder.**
Teknologi	**Antal loggede afviste adgangsforsøg.**	**Grad af teknisk håndhævelse af krav til password-kvalitet.**

Styring af udvikling		
Mennesker	**Antal medarbejdere, som både har adgang til udviklings- og produktionsmiljø.**	
Proces	**Procentdel af iværksatte it-udviklingsprojekter, hvor der er foretaget vurdering af sikkerhedsrisici og specificeret relevante sikkerhedskrav.**	**Procentdel af anvendte applikationer, som indgår i patch management processen.**

	Antal kendte SoD-overtrædelser.	
Teknologi	**Procentdel af servere/klienter, som har alle frigivne patches installeret.**	**Antal ukendte sårbarheder, som identificeres ved hjælp af teknisk sårbarhedsscanning/sikkerhedstest.**

Hændelsesstyring		
Mennesker	**Generiske**	**Generiske**
Proces	**Andel af sikkerhedshændelser, der rapporteres gennem de vedtagne rapporteringskanaler.**	**Andel af sikkerhedshændelser, som bliver løst på tilfredsstillende måde.**
	Antal hændelser, der efterfølgende omkategoriseres til sikkerhedshændelser.	**Andel af sikkerhedshændelser, der burde være opdaget af slutbrugere, men som ikke er rapporteret af disse.**
Teknologi	**Antal sikkerhedshændelser pr. år.**	**Andel af indrapporterede sikkerhedshændelser, der løses inden for tidsrammen angivet i den relevante SLA.**

Beredskabsstyring		
Mennesker	**Beredskabsorganisationens kendskab til deres respektive roller og ansvar i en beredskabssituation.**	**Antal medarbejder, der er trænet i beredskab.**
Proces	**Andel af kritiske systemer fra risikoanalysen, der er dækket af beredskabsplanen.**	**Antal dage siden sidste test af beredskabsplanen.**
	Antal it-understøttede forretningsprocesser, for hvilke der er beskrevet nødplaner.	**Antal opfølgningspunkter, som seneste test af beredskabsplanen har givet anledning til.**
	Antal hændelser, der har medført permanent datatab.	**Planens dækningsgrad i forhold til kendte scenarier.**
Teknologi	**Antal kendte Single Points Of Failure i it-infrastrukturen.**	**Antal dublerede systemer.**
	Antal sikkerhedshændelser, hvor RTO-målsætninger ikke overholdes.	**Antal sikkerhedshændelser, hvor RTO-målsætninger overholdes.**

Compliance		
Mennesker	**Antal medarbejdere, der er beskæftiget med compliance-relaterede opgaver.**	
Proces	**Ledelsens vurdering af, hvor godt deres overblik over eksterne krav (subjektiv vurdering) er.**	**Andel af relevante krav og bestemmelser, der er implementeret og dokumenteret i virksomhedens politiker og procedurer.**
	Antal anmærkninger fra intern (it) revision pr. år, som kræver opfølgning.	**Antal anmærkninger fra myndigheder og tilsyn pr. år, som kræver opfølgning.**
	Årlig bødesum i kr. som følge af compliance overtrædelser.	
Teknologi	**Overensstemmelse mellem betalte og forbrugte licenser.**	

Privatlivsbeskyttelse		
Mennesker	**Generiske**	**Generiske**
Proces	**Andel af systemer, der er klassificeret i henhold til virksomhedens retningslinjer**.	**Mængde af persondata, der opbevares i længere tid, end hvad der er nødvendigt for formålet.**
Teknologi	**Andel af systemer, der kan håndtere differentieret brugeradgang i overensstemmelse med datas klassificering.**	**Andel af medarbejdere med unødvendig adgang til personfølsomme oplysninger (subjektiv vurdering).**
	Antal systemer, der behandler persondata, hvor logning er i overensstemmelse med lovkravene.	