NorthGRC
CONNECTED COMPLIANCE

WHITE PAPER

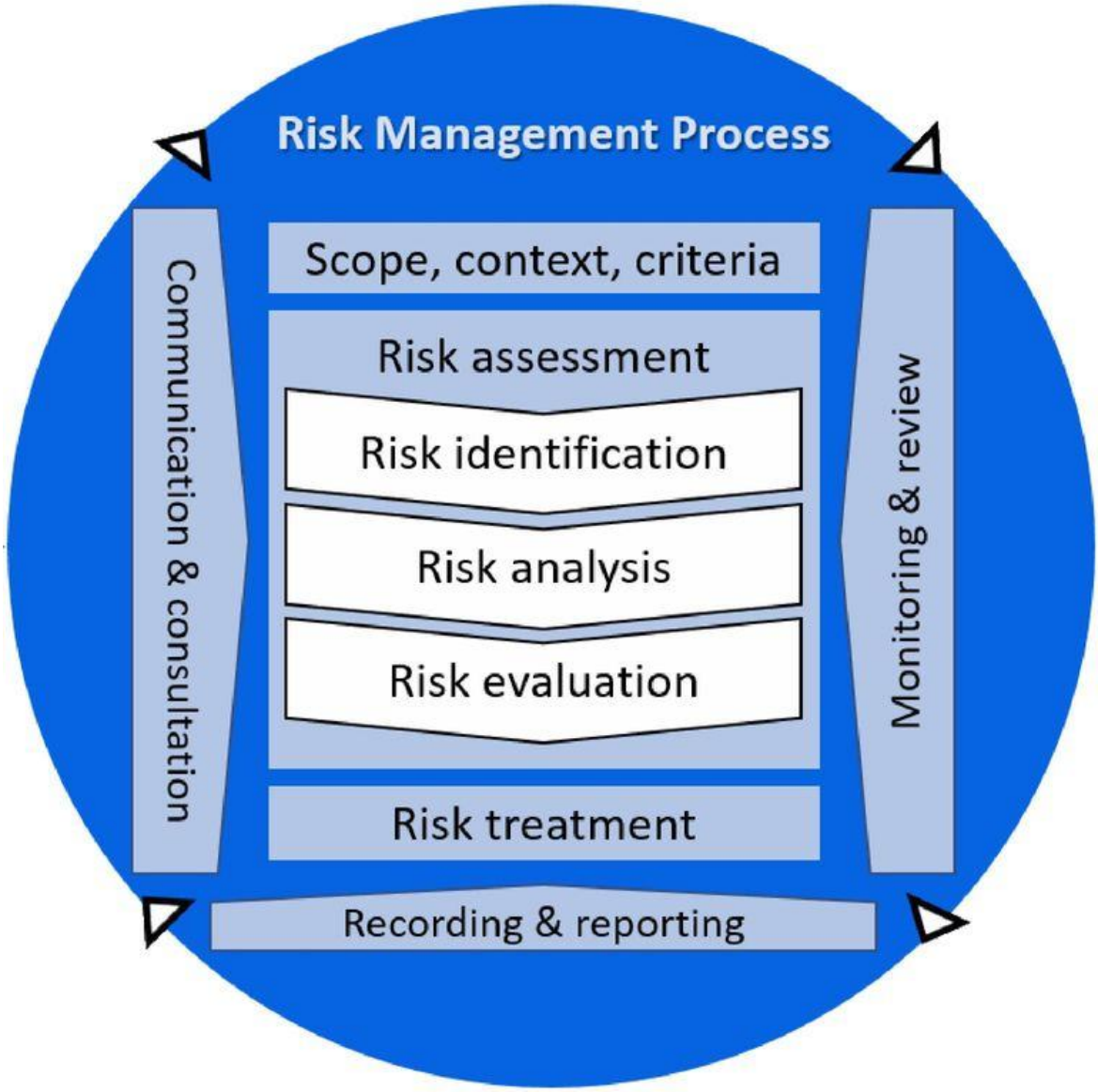
Vejledning i risikostyring med ISO 27005

Jakob Holm Hansen
CEO, NorthGRC

INDLEDNING

Et af de styrende elementer i ISO 27001 er kravet om, at informationssikkerheden baseres på de reelle risici, organisationer er udsat for. Samlet set kaldes denne aktivitet for risikostyring. De centrale dele af risikostyringen er risikovurderingen, dvs. identifikation og analyse af risici og risikohåndteringen – altså iværksættelse af tiltag til imødegåelse af risici.

Dette dokument beskriver den metodik, NorthGRC anbefaler organisationer at anvende til risikostyring. Metodikken er udarbejdet med udgangspunkt i standarden for Risk Management; ISO 31000. Overordnet set kan metodikken beskrives som et Plan-Do-Check-Act forløb, som indeholder en række aktiviteter:



I DE FØLGENDE AFSNIT VIL SAMTLIGE AKTIVITETER BLIVE GENNEMGÅET

1. Etablering af omfang og kontekst
Inden arbejdet med selve risikostyringen påbegyndes, er det nødvendigt at fastlægge de rammer, som arbejdet skal udføres under, såvel internt som eksternt. Det drejer sig blandt andet om at fastlægge:

- Basale risikokriterier som f.eks.
  - Risikovurderingskriterier – f.eks. hvornår skal der foretages risikovurdering
  - Vurdering af konsekvenser – f.eks. hvordan konsekvenser vurderes
  - Risikoacceptkriterier – f.eks. hvilke risici, organisationen vil acceptere
- Omfang og afgrænsninger
- Organisation og styring

2. Risikovurdering
Metoden for risikovurdering indeholder vurderinger af de forretningsmæssige konsekvenser af brud på sikkerheden. For at sikre, at relevante forretningsmæssige aspekter behandles under konsekvensvurderingen, er det organisationens afdelinger, som foretager denne vurdering.

Herudover indeholder metoden også vurderinger af sandsynligheden for, at sikkerhedshændelser vil ind-træffe. Dette gøres gennem vurderinger af modenheden af it-rutiner og sikkerhedstiltag, samt vurderinger af truslerne mod it-systemerne. Risikovurderingen vil ud over vurderingerne også indeholde anbefalinger til, hvordan de identificerede risici håndteres.

2.1. Fremgangsmåde
Risikovurderingen består af flere delaktiviteter, som gennemføres via workshops og interviews. Første aktivitet har til formål at fastlægge hvilke forretningsprocesser, risikovurderingen skal fokusere på. Dette overblik anvendes til at identificere hvilke it-platforme (it-systemer mv.), som disse processer er afhængige af. For hver af disse platforme foretages en forretningsorienteret konsekvensvurdering, og herefter foretages en mere detaljeret, teknisk vurdering af eventuelle trusler og sårbarheder mod disse it-platforme.

Fremgangsmåden for gennemførelse af de enkelte aktiviteter beskrives i det følgende.

2.1.1. Forretningsprocesser
Formålet med denne aktivitet er at afklare, hvilke forretningsprocesser, der skal fokuseres på i risikovurderingen. Umiddelbart skal de første risikovurderinger, man foretager, fokusere på organisationens primære forretningsprocesser. Efterfølgende risikovurderinger kan fokusere på øvrige forretningsprocesser og på organisationens støtteprocesser. Hvilke processer, der skal arbejdes med i de enkelte risikovurderinger, afklares fra gang til gang med organisationens ledelse.

2.1.2. Konsekvensvurdering

Der gennemføres workshops med de ansvarlige for de identificerede forretningsprocesser, hvor de bliver guidet gennem en vurdering af konsekvenserne af brud på sikkerheden for de it-systemer, som processen er afhængig af. Vurderingerne foretages i forhold til brud på:

- Fortrolighed – information, der kommer uvedkommende i hænde
- Integritet – korrektheden af data
- Tilgængelighed – muligheden for at arbejde med systemerne.

Vurderingerne tager udgangspunkt i en række forretningsmæssige kriterier, som er defineret sammen med organisationen. Der benyttes fem niveauer for vurdering af forretningsmæssige konsekvenser:

- Meget lille
- Lille
- Medium
- Stor
- Meget stor

Som støtte til vurderingen anvendes et begrebsskema, som definerer og beskriver de fem niveauer, der anvendes ved vurdering af forretningsmæssige konsekvenser ved brud på sikkerheden. Se appendix side 12; Forretningskonsekvens – Begrebsskema. Konsekvenserne vurderes for hvert it-system eller for en gruppe af logisk sammenhængende it-systemer.

2.1.3. Sandsynlighedsvurdering

Sandsynligheden for sikkerhedshændelser kan enten vurderes i forhold til, hvor ofte hændelser erfaringsmæssigt indtræffer, eller i forhold til modenheden af de tiltag, der skal forhindre hændelser.

Den første metode vil typisk finde anvendelse for de systemer, hvor driften er outsourcet og den anden metode vil typisk finde anvendelse, hvor organisationen selv er ansvarlig for i hvert fald en del af håndteringen af systemerne.

I begge tilfælde arbejdes som udgangspunkt med et trusselskatalog, som omfatter:

- Brugerfejl
- Drifts- eller vedligeholdelsesfejl
- Angreb med skadelig kode
- Cyber-terror angreb
- Kapacitets-fejl
- Softwarefejl
- Informationstyveri
- Forsætligt misbrug
- Bevidst afsløring af information
- Informationslækage
- Tyveri af aktiver

2.1.3.1. Hændelsesorienteret sandsynlighedsvurdering

Når der skal foretages hændelsesorienteret sandsynlighedsvurdering gennemføres dette sammen med de ansvarlige for de relevante forretningsprocesser. Vurderingerne foretages for de systemer, som forretningsprocesserne er afhængige af. Dette kan med fordel foretages på de samme workshops, hvor der foretages forretningsmæssige konsekvensvurderinger. I denne vurdering af sandsynlighed anvendes fem niveauer for sandsynligheden for, at en given hændelse vil indtræffe:

Sandsynlighed		Definition
20	Sjældent	Der kan gå år imellem sikkerhedshændelser forekommer
40	Indimellem	Sikkerhedshændelser forekommer gennemsnitligt en enkelt eller et par gange årligt
60	Regelmæssigt	Sikkerhedshændelser forekommer gennemsnitligt en gang om måneden
80	Ofte	Sikkerhedshændelser forekommer gennemsnitligt en gang om ugen
100	Konstant	Sikkerhedshændelser forekommer dagligt

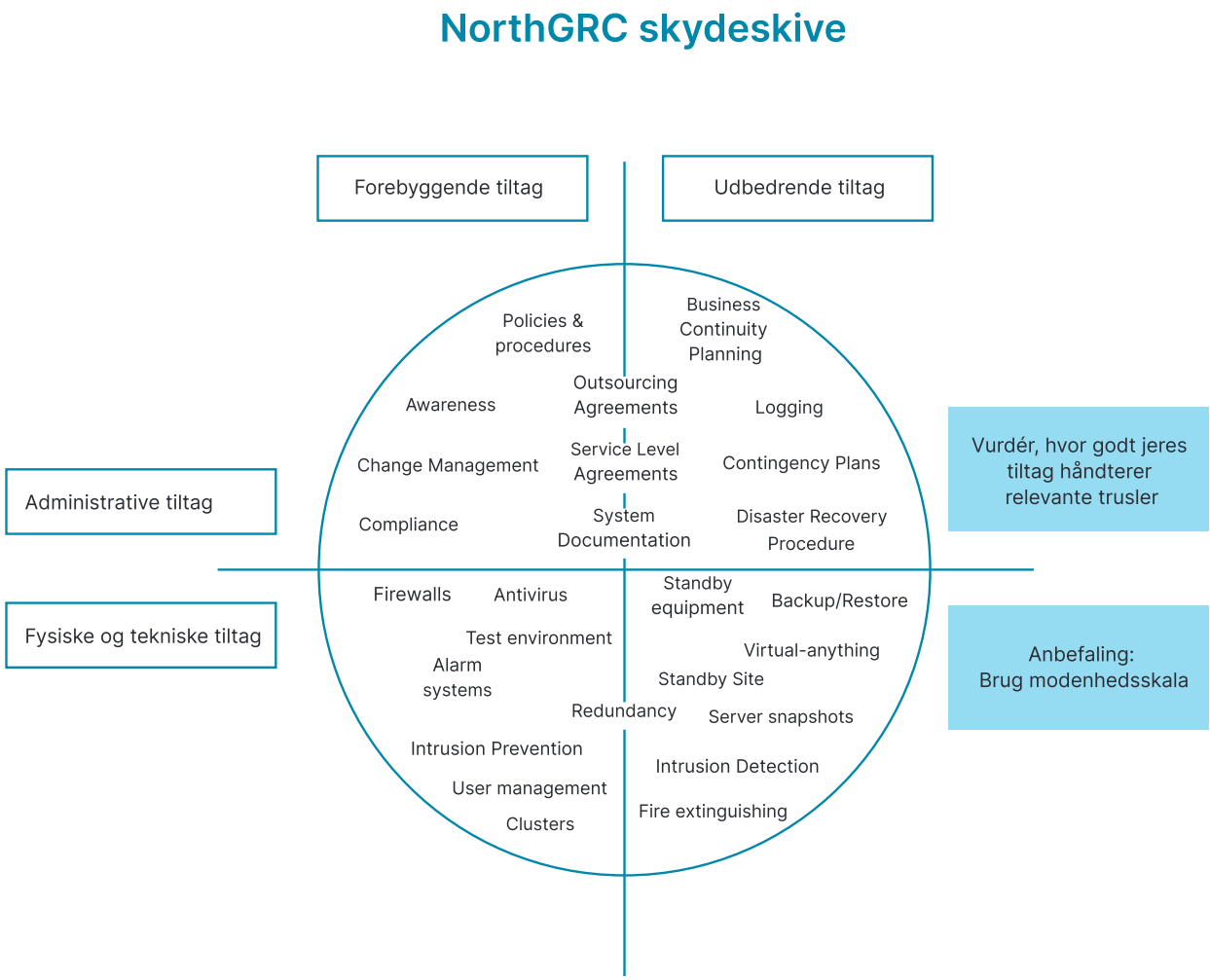
2.1.3.2. Modenhedsorienteret sandsynlighedsvurdering

Når der foretages modenhedsorienteret sandsynlighedsvurdering afholdes møder med de it-driftsansvarlige for de pågældende systemer. På disse møder afdækkes afhængigheder mellem de forskellige systemer og systemernes sårbarhed vurderes.

Systemernes sårbarhed vurderes, i forhold til hvad der er gjort for at sikre systemerne jævnfør fire typer af tiltag:

- Forebyggende administrative tiltag
- Forebyggende tekniske tiltag
- Udbedrende administrative tiltag
- Udbedrende tekniske tiltag

TYPISKE EKSEMPLER PÅ DE FORSKELLIGE TILTAG ER VIST I NEDENSTÅENDE FIGUR



Figur 1
Summary of measures

Figure 1: Summary of measures

De administrative tiltag vurderes efter følgende skala:

Administrative tiltag		Definition
20	Optimeret	Der foretages løbende tilpasninger af definerede administrative tiltag rettet mod truslen eller dens konsekvenser, og af disses implementering gennem rettidig opfølgning på metrikker og etablering af handlingsplaner
40	Styret	Der foretages målinger af implementeringen af definerede administrative tiltag rettet mod truslen eller dens konsekvenser gennem løbende vurderinger af risiko, efterlevelse og sikkerhedsbevidsthed og gennem anvendelse af metrikker, der anskueliggør sikkerhedsniveauet
60	Defineret	Administrative tiltag rettet mod truslen eller dens konsekvenser er baseret på en formel ansvarsdelegering og konsistent dokumenteret gennem formelle politikker, regler, planer og procedurer
80	Gentagelig	Administrative tiltag rettet mod truslen eller dens konsekvenser er baseret på en uformel, men fastlagt ansvarsdelegering og en erfaringsbaseret, indarbejdet praksis
100	Ad Hoc	Administrative tiltag rettet mod truslen eller dens konsekvenser er ikke systematiseret

De tekniske tiltag vurderes efter følgende skala:

Tekniske tiltag		Definition
20	Megte effektive	Der er foretaget systematiske tekniske/fysiske implementeringer i flere lag (i tilfælde af svigt af primære sikringsforanstaltninger) for at beskytte mod truslen eller dens konsekvenser, og til-tagene er baseret på anerkendt best practice og professionelt vurderet eller testet som særdeles effektive
40	Effektive	Der er foretaget systematiske tekniske/fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser, og tiltagene er baseret på anerkendt best practice og professionelt vurderet eller testet som effektive
60	Implementerede	Der er foretaget systematiske tekniske/fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser
80	Delvist implementerede	Der er foretaget sporadiske tekniske/fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser
100	Fraværende	Der er ikke foretaget tekniske/fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser

2.1.4. Rapportering

Efter at der er skabt overblik over såvel konsekvenser som sandsynligheder, sammenholdes og konsolideres disse, således at man får et overordnet risikobillede for organisationen. For hvert af de vurderede systemer beregnes en risikofaktor for hver af sikkerhedsdimensionerne:

- Fortrolighed
- Integritet
- Tilgængelighed

Risikofaktoren beregnes ved at multiplicere konsekvensfaktoren med sandsynlighedsfaktoren. Herved beregnes en værdi mellem 0 og 100, hvor 100 er den største risiko.

Der udarbejdes en oversigt over hvilke systemer, der har de største risici, årsagen til de højeste risici beskrives og der skitseres forslag til hvordan de største risici håndteres.

3. Udarbejde risikohåndteringsplan

Risikohåndtering (også kaldet risikobehandling eller "risk treatment") er en central del af det overordnede begreb risikostyring. Med udgangspunkt i det udarbejdede risikobillede fra risikovurderingen besluttes det, hvordan de identificerede risici håndteres. Beslutningerne tages ud fra overvejelser om de økonomiske konsekvenser af de identificerede risici i forhold til omkostningerne ved at implementere eventuelle tiltag. Mulighederne for risikohåndtering falder typisk i én af følgende kategorier

- Reducér – indfør tekniske eller administrative tiltag
- Acceptér – det vurderes ikke, at det er rentabelt at iværksætte tiltag
- Undgå – ophøre med risikobetonede aktiviteter (f.eks. forbud mod at medarbejderne kobler eget udstyr (f.eks. smartphone) til organisationens systemer
- Del – forsikring eller leverandørkontrakter (bod eller lignende økonomiske kompensationer)

Hvilken form for risikohåndtering der vælges, vil afhænge af, hvor store risici organisationen er villig til at acceptere – organisationens "risikoappetit."

Reducér betyder, at man etablerer tiltag, der mindsker sandsynligheden for en hændelse eller mindsker konsekvensen, når en hændelse sker. Disse tiltag kan være af såvel teknisk som administrativ karakter. Tiltag, der mindsker sandsynligheden for sikkerhedshændelser, benævnes forebyggende tiltag. Tiltag, som mindsker konsekvenserne af sikkerhedshændelser, benævnes udbedrende tiltag. Ovenstående Figur 1. Oversigt over tiltag illustrerer de fire typer tiltag.

Acceptér betyder, at organisationen vælger at leve med en risiko. Denne måde at håndtere risici på, er en naturlig følge af, at 100% sikkerhed ikke findes

Undgå. Denne mulighed indebærer typisk, at organisationen ophører med en aktivitet, som giver anledning til en given risiko. Det kan f.eks. være et usikkert system, man holder op med at bruge. Denne risiko-behandlingsform bruges kun sjældent i praksis.

Del betyder, at organisationen håndterer risikoen ved at dele den med andre. For eksempel gennem forsikring eller gennem leverandørkontrakter, hvor der betales et forsikringsselskab eller en leverandør for at have en del af risikoen. I den gamle udgave (2008) af ISO 27005-standarden hed dette punkt "overfør". Det skal bemærkes, at det overordnede ansvar for enhver risiko altid vil ligge hos organisationen.

3.1. Dokumentation af risikohåndteringsplan (handlingsplan)

Beslutningerne om hvordan de identificerede risici håndteres dokumenteres i en risikohåndteringsplan (handlingsplan). Risikohåndteringsplanen kan i praksis benyttes som en anbefaling/indstilling fra den informationssikkerhedsansvarlige til organisationens ledelse. Her anføres det, hvilke tiltag som bør indføres, og hvilke risici som bør accepteres med udgangspunkt i de fastsatte kriterier for risikotolerance.

Planen udarbejdes efter sædvanlig standard for projektplaner. Dvs. at for hver aktivitet/tiltag beskrives:

- Formål
- Ansvarlig (risikoejer)
- Ressourceindsats
- Øvrige omkostninger
- Tidsplan

4. Risikoaccept
Når risikohåndteringsplanen er udarbejdet, skal den forelægges for virksomhedens ledelse. Ledelsen skal godkende de tiltag, der iværksættes, herunder den ressourceindsats og øvrige omkostninger, der er nødvendige for at gennemføre tiltagene. Ledelsen skal endvidere acceptere de risici, der ikke iværksættes tiltag mod.

5. Gennemføre risikohåndteringsplan
Når ledelsen har godkendt risikohåndteringsplanen og accepteret de risici, hvor der ikke iværksættes tiltag, skal risikohåndteringsplanen gennemføres.

På samme måde, som planen bør være udarbejdet efter etablerede metoder for projektplaner, bør de sikkerhedsprojekter, som iværksættes, også ledes af en erfaren projektleder. Afhængigt af projektledelseserfaringen hos de medarbejdere i organisationen, der har ansvaret for informationssikkerhed, kunne projektlederen være en af disse personer.

I forlængelse af gennemførelsen af risikohåndteringsplanen opdateres SoA-dokumentet. SoA-dokumentet indeholder bl.a. en beskrivelse af de sikringsforanstaltninger, som organisationen har valgt at implementere. SoA-dokumentet skal derfor altid opdateres, når der er gennemført en risikovurdering og taget beslutning om at ændre på sikringsforanstaltningerne.

6. Overvågning og revurdering af risici
Der bør løbende foretages opfølgning på risici. Dels bør det sikres, at de sikringsforanstaltninger og tiltag, der indføres som en del af risikohåndteringen, rent faktisk også bliver implementeret og fungerer efter hensigten. Dels bør der løbende følges op på de forudsætninger, som ligger til grund for risikovurderingen. Aktiver, trusler, sårbarheder og konsekvenser kan hurtigt ændres - og medfører tilsvarende ændringer i risikobilledet. Organisationens risikostyring bør derfor sikre, at der på en struktureret måde foretages en løbende opfølgning på risici.

6.1. Kommunikation af risici
Kommunikation er en central del af risikostyringen. Risikostyring er en tværorganisatorisk proces, og der indgår mange interessenter med forskellige opgaver og ansvarsområder.

Typisk vil det være informationssikkerhedsudvalget og informationssikkerhedskoordinatoren, som har det praktiske ansvar for risikostyringen, mens linjeledelsen har ansvaret for risici inden for eget område. For at sikre en fælles opfattelse og tilgang til risikostyringen, bør kommunikationen planlægges, så der er en ensartet tilgang og fælles forståelse af processen.

7. Løbende forbedring af risikostyringen
Kvaliteten af risikostyringen bør løbende overvåges, revideres og forbedres.

Løbende overvågning og revision er nødvendig for at sikre, at rammerne, udfaldet af risikovurderingen og risikohåndteringen såvel som handlingsplaner, fortsat er relevante og passer til virksomhedens virkelighed.

Organisationen skal sikre, at risikostyringen og relaterede aktiviteter fortsat er hensigtsmæssige under de nuværende omstændigheder, og at metoden og planerne følges. Enhver aftalt forbedring af proces eller handlinger, der er nødvendige for at forbedre overholdelsen af processen, skal aftales med ledelsen. Dermed har man sikkerhed for, at ingen risiko eller risikoelement er overset og/eller undervurderet. Man har også sikkerhed for, at alle nødvendige skridt er taget og beslutninger truffet for at give en realistisk risikoforståelse og en evne til at reagere hurtigt og relevant.

APPENDIX

FORRETNINGSKONSEKVENS – BEGREBSSKEMA

KONSEKVENS	INDVIRKNING			
	Omdømme	**Administrativ byrde**	**Lov-, regel- og kontraktbrudt**	**Indflydelse på serviceniveau**
Meget lille	Ingen eller minimal interesse fra offentligheden.	Vil ikke medføre øgede administrative byrder.	Vil ikke medføre kontraktbrud eller lovbrud.	Vil ikke have nævneværdig indflydelse på serviceniveauet.
Lille	Forbigående opmærksomhed fra interessenter eller offentlighed.	Vil medføre minimalt øgede administrative byrder, der dog kan løses inden for normal arbejdstid.	Kan betyde mindre alvorlige brud på kontrakter eller lovgivning. Vil ikke udløse sanktioner.	Vil betyde mindre nedgang i serviceniveau. Forpligtelser vil dog stadig kunne overholdes.
Medium	Længerevarende negativ opmærksomhed om organisationen. Medfører presseomtale i større medier. Vil betyde tab af image.	Vil medføre øgede administrative byrder, med behov for overarbejde af nøglepersoner.	Vil medføre brud på vigtige kontrakter eller lovgivning. Organisationen kan blive udsat for sanktioner eller erstatningskrav.	Vil medføre et markant fald i det generelle serviceniveau for organisationen. Enkelte vigtige forpligtelser kan ikke overholdes. Borgere kan ikke serviceres som forventet.
Stor	Længerevarende negativ opmærksomhed i landsdækkende presse, der vil medføre stor skade på omdømme. Vil tage lang tid at vende til positivt image.	Vil medføre markant øgede administrative byrder, med behov for omfattende overarbejde samt indkaldelse af vikarer.	Vil medføre større brud på vigtige kontrakter eller lovgivning. Organisationen vil blive udsat for større sanktioner eller krav om erstatning.	Vil medføre et større fald i serviceniveauet for organisationen. Flere vigtige forpligtelser over for borgere kan ikke overholdes og de vil opleve en væsentlig forringelse af forventet service.
Meget stor	Længerevarende negativ opmærksomhed i landsdækkende presse, der vil medføre uoprettelig skade på omdømme. Vil betyde kraftigt og længerevarende imagetab.	Vil medføre kraftigt øgede administrative byrder, der truer med at sætte afdelinger ud af spil.	Vil medføre alvorlige brud på kritiske kontrakter eller lovgivning. Organisationen vil blive udsat for alvorlige sanktioner eller erstatningskrav, og muligvis blive sat under administration.	Vil medføre et alvorligt lavt serviceniveau for organisationen. Flere vigtige forpligtelser kan ikke overholdes. Borgere modtager ingen eller meget mangelfuld service.
MAKSIMAL ACCEPTABEL NEDETID				
Meget lille	> 1 uge	Systemet er ikke tidskritisk, og kan godt være utilgængeligt i mere end 1 uge.		
Lille	1 uge	Man kan fungere uden systemet i en periode, men maksimalt i 1 uge.		
Medium	4 dage	Man kan fungere uden systemet i en kort periode, men maksimalt 4 dage.		
Stor	2 dage	Systemet er tidskritisk, og må maksimalt være utilgængeligt 2 dage.		
Meget stor	<1 dag	Systemet er meget tidskritisk, og må maksimalt være utilgængeligt 1 dag.		

Kunne du bruge denne vejledning? Tilmeld dig NorthGRC månedlige nyhedsbrev og vær sikker på at modtage vores kommende vejledninger, artikler og invitationer til webinarer og seminarer. Kun viden og inspiration om informationssikkerhed, ingen spam. Det er nemt at afmelde sig igen, hvis du fortryder

Tilmeld dig her: www.northgrc.com/da/nyhedsbrev

SECURE ISMS TIL EFFEKTIV LEDELSE AF INFORMATIONSSIKKERHED

NorthGRC har specialiseret sig i at udvikle ledelsessystemer til informationssikkerhed (Information Security Management Systems). Vores løsninger, Secure GDPR og Secure ISMS er specifikt designet til at hjælpe private og offentlige virksomheder med at overholde EU's Databeskyttelsesforordning,
standarder som ISO 27001/2/5 og ISO 22301 såvel som virksomhedernes egne regler og procedurer. Med løsningerne er det enklere at etablere de processer der skal til, for at efterleve disse krav samt sikre kontinuerlig compliance.

Læs mere og hent en gratis prøveversion på www.northgrc.dk

FÅ HJÆLP FRA ERFARNE IT-SIKKERHEDSKONSULENTER

Skal I etablere et ISMS? Hvordan udarbejdes en Statement of Applicability? Skal den årlige risikovurdering gennemføres? Skal beredskabsplanerne opdateres? Hvordan følger I op på hændelser? Har I aftalt sikkerhedsansvar med jeres it-leverandører? Beskyttes persondata tilstrækkeligt? Vil I starte med en ISO 27001 gap-analyse?

Der er mange ting man skal overveje i forhold til it-sikkerhed. Derfor stiller vi dygtige og erfarne konsulenter til rådighed. Vores viden og erfaringer bringer virksomheder, institutioner og styrelser sikkert i mål med ISO 27001-efterlevelse på kortere tid. Når I planlægger og udfører jeres ISO 27001-aktiviteter rigtigt, kan den nødvendige informationssikkerhed indføres pragmatisk og fleksibelt. Det er NorthGRC eksperter i.

VIL DU HØRE MERE?

Ring til Louise Bøttner

+45 7025 8030

NorthGRC
CONNECTED COMPLIANCE

UK240518-1