Appendiks 2. Rapportering - inspirationsliste

1 – Risikovurdering og sårbarheder / 2 – Risikoappetit og strategi
Status på virksomhedens risikobillede, herunder ***i)*** overblik over vigtigste værdier, systemer og (IT-)leverandører samt konsekvenser ved læk eller nedbrud, ***ii)*** virksomhedens vurdering af de primære sårbarheder, væsentligste cyberrisici og relevante truslers sandsynlighed og risikoindvirkning på forretningen, samt ***iii)*** udvikling/trends siden sidst og fremadrettet. Kan vises sammen med et "risk heatmap". Formålet er at give bestyrelsen et samlet billede af virksomhedens risiko indenfor cybersikkerhed for at den kan fastlægge risikoappetitten.
Anbefalinger til yderligere forbedringer og merinvesteringer forbundet hermed
Sikkerhedsbudget og sammenligning med markedet
Forsikringer og hvilke udgifter/tab de dækker ved et cyberangreb
Eventuelle fravigelser fra de af bestyrelsen fastsatte risikotolerancer
3 – Planer, processer og beredskab (identificere, beskytte, opdage, håndtere, genoprette)
Status på implementering af sikkerhedstiltag, herunder pågående programmer eller projekter for forbedringer af cybersikkerhed
Status på pågående sikkerhedshændelser og konsekvenser heraf
Virksomhedens evne til at opdage sikkerhedshændelser så tidligt som muligt (engelsk: *threat intel* / *threat hunting*) og begrænse potentiel skade (f.eks. ved sikker adgangskontrol, logning, kryptering, segmentering af netværk m.v.)
Virksomhedens evne til at håndtere og analysere cybersikkerhed hændelser, herunder loghændelser og årsagsanalyser (se f.eks. vejledning ”Logning - en del af et godt cyberforsvar” fra CFCS)

3 – Planer, processer og beredskab (forts.)
Status på virksomhedens kontinuitetsplanlægning (dvs. evne til at fortsætte forretningen, handlingstid for at vende tilbage til normaldrift, roller, ansvar og rapportering)
Forberedte cybersikkerheds scenarier med roller, ansvar samt kommunikation ved f.eks. ransomwarehændelse, virusangreb og scenarier hvor virksomheden eller virksomhedens kunder er truet i relation til integritet, tilgængelighed og fortrolighed af data (og indenfor industrien evt. også skader på personer og aktiver)
Resultater fra test af beredskabsplaner og kritiske systemer, herunder validering og beskyttelse af virksomhedens sikkerhedskopier
Resultater fra sårbarhedsanalyser af cyber sårbarheder (f.eks. relateret til opdateringsgrad af systemer og services), inkl. vurdering af leverandører, samt status på udbedringer
Forslag til forbedringer af beredskab og cyber krisehåndtering (kvalitetscyklus "plan-do-check-act")
4 – Rapportering og kontrol
Resultater fra interne og eksterne audits
Status modenhed og styring indenfor cybersikkerhed (cybersikkerheds kapaciteter baseret på f.eks. (principperne i) ISO27002-kontroller, NIST-rammeværket, eller CIS-kontrollerne)
Status på pågående forbedringer af cybersikkerhed (Cyber Security Capabilities modenhed eller certifikat fra revisionshus)
5 – Kultur og mennesker / 6 – Kompetencer og organisering
Status på cybersikkerheds træning og bevidsthed i organisationen, herunder kompetencebehov, cyber security awareness programmer, ledelsestræning m.v.