Dashboard (Samet score)	
Risikovurdering og sårbarheder	38%
Risikoappetit og strategi	75%
Planer, processer og beredskab	0%
Rapportering og kontrol	0%
Kultur og mennesker	13%
Kompetencer og organisering	0%

Nuværende score	Målsat score	Delta	Individuel Perf
21%	100%	79%	8%

Relevans	Risikovurdering og sårbarheder	38%
1. Ja	Delvist	Er det vurderet og mitigeret hvad det betyder for forretningen, hvis vigtige værdier ændres, stjæles, lækkes eller hvis kritiske systemer eller andre it-services er utilgængelige i kortere eller længere tid?
1. Ja	Ja	Er det vurderet og mitigeret hvem er de sandsynlige angribere, hvad er deres mål, og hvilke redskaber/teknikker bruger de til at opnå disse mål?
1. Ja	Nej	Er det vurderet og mitigeret på hvilke områder virksomheden er mest sårbar overfor angreb (teknologi, personale, processer), og hvor sandsynligt er angreb indenfor disse områder?
1. Ja	Nej	Er det vurderet og mitigeret hvad virksomhedens plan for risikohåndtering er, inkl. investeringer?

Relevans	Risikoappetit og strategi	75%
1. Ja	Ja	Er budgettet for cyber- og informationssikkerhed tilstrækkeligt?
1. Ja	Ja	Er det vurderet hvor virksomhedens sikkerhedsniveau- og budget ligger sammenlignet med andre forretningsområder? Med andre virksomheder?
1. Ja	Delvist	Er det vurderet hvad de potentielle omkostninger forbundet med at investere i en opgradering af sikkerhedsniveauet er?
1. Ja	Delvist	Baseret herpå, er det vurderet hvad virksomhedens tolerance for at påtage sig cyberrisici er?

Relevans	Planer, processer og beredskab	0%
1. Ja		Har virksomheden nedskrevne it-sikkerhedspolitikker, som direktionen aktivt støtter, og som medarbejderne er trænet i?
1. Ja		Foreligger der beredskabs- og kommunikationsplaner – både elektronisk og på papir – til at håndtere sikkerhedshændelser?
1. Ja		Beskriver planerne hvordan forretningen kan fortsætte i tilfælde af manglende adgang til de vigtigste it-systemer og it-services, hvem der skal involveres i en krisesituation, og hvordan der sker reetablering af it-systemer og it-services?
1. Ja		Angiver planerne en handlingsplan for de første 24 timer efter en sikkerhedshændelse, herunder hvem der har ansvaret for at føre minutrapport?
1. Ja		Bliver planerne øvet og testet regelmæssigt?
1. Ja		Hvad er resultatet af seneste test, og har det ført til ændringer?
1. Ja		Bliver planerne justeret i lyset af angreb, der har ramt andre virksomheder?
1. Ja		Er der indgået aftale med eksterne, som kan tilkaldes for at støtte interne teams?

Relevans	Rapportering og kontrol	0%
1. Ja		Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed (risici, status, investeringer, anbefalinger mv.) fra direktionen?
1. Ja		Er cyber- og informationssikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
1. Ja		Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?

Relevans	Kultur og mennesker	13%
1. Ja		Er der et trænings- og uddannelsesprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
1. Ja		Foregår der et samarbejde på tværs af organisationen, hvor der deles viden?
1. Ja	Delvist	Opfordrer virksomheden sine tekniske specialister til at udveksle viden og erfaringer med medarbejdere fra lignende organisationer?
1. Ja		Går bestyrelsen forrest i at understøtte en stærk og bevidst cybersikkerhedskultur, f.eks. ved selv at anvende VPN, password managers og flerfaktor godkendelse?

Relevans	Kompetencer og organisering	0%
1. Ja		Har mindst ét bestyrelsesmedlem kompetencer og erfaring indenfor cyber- og informationssikkerhed? Hvis ikke, får bestyrelsen intern eller ekstern rådgivning og/eller sparring på området? F.eks. fra rådgivere eller en komité?
1. Ja		Deltager bestyrelsen aktivt i diskussioner om cyber- og informationssikkerhed?
1. Ja		Er bestyrelsen opmærksom på, at dens medlemmer selv kan være et oplagt mål for cyberangreb?
1. Ja		Hvor i organisationen (person/funktion) ligger ansvaret for cyber- og informationssikkerhed?
1. Ja		Rapporterer denne sikkerhedsfunktion direkte til de rigtige på ledelsesniveau?
1. Ja		Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
1. Ja		Har virksomheden de rette tekniske kompetencer inhouse, eller er der behov for ekstern hjælp?

Relevans	Personlig cybersikkerhed	8%
1. Ja	Nej	Kender og overholder virksomhedens itsikkerhedspolitik
1. Ja	Delvist	Skaber/Har overblik over data og systemadgange
1. Ja	Ja	Bruger en dedikeret e-mailkonti til virksomhedskommunikation
0. Nej		Arbejder ikke som lokal administrator på computeren. Heller ikke på en privat computer hvorpå der arbejdes
1. Ja		Bruger stærke adgangskoder og genbruger ikke passwords
1. Ja		Benytter to-faktorautentificering
1. Ja		Kontrollerer om du har været med i et læk af adgangskoder
1. Ja		Tænker over hvad du deler på sociale medier
1. Ja		Bruger ikke fremmede USB-enheder eller opladere
1. Ja		Benytter et privacy-filter til din computer og tablet
1. Ja		Låser altid dine enheder. Når du forlader dem mere end kort tid logger du helt af
1. Ja		Krypterer dit indhold
1. Ja		Benytter sikkerhedsprodukter med antivirus og firewall
1. Ja		Opdaterer dit operativsystem og programmer regelmæssigt
1. Ja		Beskytter dig med VPN på usikre netværk
1. Ja		Har en sund skepsis og opmærksomhed relateret til cybersikkerhed
1. Ja		Er opmærksom på atypiske hændelser på din computer eller mobiltelefon
1. Ja		Underretter virksomhedens it-afdeling hurtigst muligt ved mistanke om cybersikkerhedshændelser
1. Ja		Har en plan klar til når uheldet er ude
1. Ja		Tager sikkerhedskopier – både online og offline