Samlet risiko	Område	Måling	Risiko
-32%	Cyberhygiejne-score	2	-25%
	Grundlæggende it-sikkerhed	0	-33%
	Organisatorisk it-sikkerhed	0	-33%
	Systemiske ressourcer	0	-33%
	Resourcetildeling	0	-33%
	Unikke tiltag / krav	0	-33%

Bemærkninger (35 spørgsmål)

Helt og fuldt	0	0%
Næsten dækkende	1	100%
Delvist	0	0%
Slet/start set ikke	0	0%

Start herunder…

Riskoområde	Svar	Spørgsmål
Cyberhygiejne-spørgsmål [8 spg]	2. Ja, næsten dækkende	Undersøges netværket aktivt og regelmæssigt for uønskede devices, som fjernes rettidigt, når de opdages?
		Undersøges netværket aktivt og regelmæssigt for uønsket software og software-versioner, som fjernes rettidigt, når de opdages?
		Er alle OS og software-versioner, som er End Of Life (EOL) og Out Of Maintenance (OOM) fjernet eller effektivt isoleret fra netværket?
		Undersøges netværket kontinuerligt med en sårbarhedsscanner, og mitigeres sårbarheder aktivt på basis af risiko?
		Undersøges eksterne IP-adresser og webapplikationer kontinuerligt med en sårbarhedsscanner, og mitigeres sårbarheder aktivt og rettidigt på basis af ri
		Har alle brugere fået fjernet lokale administratorrettigheder, når de logger på et endpoint med deres arbejdskonto?
		Anvendes sikre udgaver og opsætninger af OS, applikationer og hardware/systemer baseret på Benchmarks (Fx CIS Benchmarks)?
		Opsamles og analyseres logge fra alle relevante systemer centralt med en opbevaringstid på mindst 6 måneder?
Grundlæggende it-sikkerhed [13 spg]		Anvendes der kun sikre godkendte browsere, og går internettrafik igennem et filter både i og uden for netværket?
		Anvendes der kun sikre og godkendte e-mail-klienter, og bliver alle ind- og udgående e-mail filteret effektivt for spam og phishing?
		Anvendes der et "bedst i klasse" adfærdsbaseret anti-malwaresystem på alle klienter og servere, og er der regelmæssige kontroller for dækning og effek
		Er der en effektiv applikations-/antimalware-baseret firewall mellem netværket og internettet?
		Er der en aktiv firewall på alle klienter og servere kombineret med fravær af lokale administratorrettigheder?
		Er netværket segmenteret effektivt i grupper baseret på data og systemer, så malware ikke kan spredes fra en gruppe til en anden?
		Er wireless-adgang til det interne netværk beskyttet med 2FA og/eller certifikater, så kun autoriserede endpoints kan få kontrolleret adgang?
		Foretages der en effektiv regelmæssig backup - som også testes regelmæssigt - af alle relevante systemer?
		Er der foretaget en ledelsesgodkendt Business Impact Analysis (BIA)?
		Er der en offline backupkopi, som ikke er sårbar overfor ransomware?
		Findes der effektive mekanismer i netværket, som alarmerer ved bestemte/relevante typer af tegn på sikkerhedsbrud (IOC)?
		Forhindres brugen af uautoriserede og ukrypterede USB sticks overalt, hvor det er muligt og relevant?
		Anvendes der i udstrakt grad MFA/2FA overalt, hvor det er muligt og relevant - særligt med fokus på VPN og alle cloud-systemer (Fx O365)?
Organisatorisk it-sikkerhed [8 spg]		Anvendes der livscyklushåndtering for alle typer af konti (bruger-, service-, admin- og eksterne konti)?
		Bliver brugerne uddannet regelmæssigt og målbart efter bedste praksis i cybersikkerhedsemner baseret på en risikoanalyse (Awareness-træning)?
		Gennemføres regelmæssige phishing-øvelser med efterfølgende træning, hvor det er relevant (fx månedligt)?
		Uddannes ledelsen og relevante stabsfunktioner regelmæssigt og målbart i at opdage og undgå direktørsvindel?
		Findes der effektive, målbare og afprøvede mekanismer til at opdage intern svindel overalt, hvor det er muligt og relevant?
		Findes der en veldokumenteret og regelmæssigt efterprøvet cybersikkerhedshændelsesplan eller en tilsvarende outsourcet funktion?
		Findes der en veldokumenteret og regelmæssigt efterprøvet beredskabsplan eller en tilsvarende outsourcet funktion?
		Foretages der regelmæssige pen-test med efterfølgende rettidig mitigering af fundne sårbarheder?
Systemiske tiltag og ressourcer [5 spg]		Er it-sikkerhed helt og fuldt forankret hos ledelsen, og tildeler ledelsen tilstrækkelige ressourcer og fokus til it-sikkerheden?
		Er niveauet af it-sikkerhed målt (fx efter CIS20), og er der en kontinuerlig plan for at forbedre it-sikkerheden til et tilstrækkeligt niveau (Den accepterede r
		Anvendes der i udstrakt grad et ledelsesgodkendt praktisk it-sikkerhedsrammeværk som fx CIS eller NIST CSF som målestok for it-sikkerhed i virksomh
		Er der implementeret et målbart og regelmæssigt program for "Clear Desk Policy"?
		Uddannes brugerne regelmæssigt og målbart i organisationens it-sikkerhedspolitik?
		Bruges der aktivt og regelmæssigt et rammeværk til at måle effektiviteten af it-sikkerhedstiltagene (Kontroller som fx CIS Measures and Metrics)?
Ressourcetildeling [2 spg]		Er det et it-sikkerhedsbudget på mindst 7% af det samlede it-driftsbudget?
		Er der mindst 1 fuldtids it-sikkerhedsansvarlig medarbejder og derefter en fuldtids it-sikkerhedsmedarbejder for hver 500 medarbejdere?
Unikke tiltag		Unikke spørgsmål 1 (Tilrettes her)

?	Forsikringsdækning - Sikkerhedsforholdsregler							
		Punkt 1	Punkt 2	Punkt 3	Punkt 4	Punkt 5	Punkt 6	Samlet vurdering
Krav:	Krav tekst:	Der er udpeget en ansvarlig for opfyldelse af kravet	Kravet opfyldes målrettet	Forelagt forsikrings-selskab	Godkendt af forsikrings-selskab	Link til dokument/ Godkendelse	Er kravet under Change Management kontrol	Sansynlighed for at kravet er overholdt
#1: Rutiner for sikkerhedskopiering/backup	Der skal tages sikkerhedskopi/backup af virksomhedskritisk og anden relevant data som minimum hver 5. dag. Hvis sikrede selv tager backup på lokale medier, skal data opbevares forsvarligt f.eks. i særskilt lokale eller aflåst databrandskab. Foretages backup via en online-udbyder, skal forbindelsen mellem sikrede og udbyder krypteres.	2. Delvist	3. Ja	3. Ja	3. Ja	3. Ja	1. Nej	75%
#2: Firewall og antivirusprogram	At sikrede beskytter systemer og netværk med selvstændig firewall og antivirusprogram af professionel standard, egnet for erhvervsmæssigt brug. Firewall og antivirusprogram skal opdateres regelmæssigt (fx i forbindelse med sikkerhedsopdateringer, software patches m.v.).	3. Ja	3. Ja	3. Ja	3. Ja	3. Ja	3. Ja	100%
#3: Kryptering af mobile enheder	Mobile enheder, som bruges i sikredes virksomhed eller håndterer sikredes information, f.eks. mobiltelefoner, bærbare computers, tablets, memory sticks, harddiske eller lignende, skal være hardwarekrypteret.	2. Delvist	1. Nej	3. Ja	1. Nej	1. Nej	1. Nej	25%
#4: Efterlevelse af PCI-DSS	Hvis den sikrede tilbyder betaling via konto- eller kreditkort skal den sikrede opfylde krav som foreskrives den sikrede i kontrakt som regulerer håndtering af kreditkortsoplysninger, PCI-DSS (Payment Card Industry – Data Security Standard).	1. Nej	1. Nej	1. Nej	1. Nej	1. Nej	1. Nej	0%
Samlet forventning til opfyldelse af Cyber Forsikrigs krav (sikkerhedsforholdsregler) er opfyldt:								50%

Se eksempel herunder **Se eksempel på Tryg CY16 betingelser**	Hvad er kravene til din cyberforsikring? https://tryg.dk/erhverv/cyberforsikring

Vigtige kontroller som børe være på plads for at kunne demonstrere efterlevelse af ovenstående CIS 20 kontroller

#1: Rutiner for sikkerhedskopiering/backup (CIS CSC #10)								
10	10,1	Data	Beskyt	Vær sikker på at der tages regelmæssige	Vær sikker på at alle systemer bliver	1	1	1
10	10,2	Data	Beskyt	Gennemfør komplet system backup	Vær sikker på at alle organisationens	1	1	1
10	10,3	Data	Beskyt	Test backup på backup medier	Deloittes kommentar: Det er af afgørende		1	1
10	10,4	Data	Beskyt	Beskyt backups	Vær sikker på at alle sikkerhedkopier er beskyttede via	1	1	1
10	10,5	Data	Beskyt	Vær sikker på at alle backups har mindst en off-line kopi	Vær sikker på at alle sikkerhedskopier har mindst en off	1	1	1
#2: Antivirusprogram & Firewall (CIS CSC #8 & #12)								
8	8,1	Enheder	Beskyt	Brug en centralt administreret anti-malware løsning	Brug et centralt administreret anti-malware system til		1	1
8	8,2	Enheder	Beskyt	Vær sikker på at anti-malware software og signaturer er	Vær sikker på at organisationens anti-malware software	1	1	1
8	8,3	Enheder	Beskyt	Slå OS malware beskyttelsesmekanismer/funktioner til og udnyt	Slå operativ systemets indbyggede forsvarsmekanismer til som fx		1	1
8	8,4	Enheder	Opdag	Konfigurer anti-malware scanning af USB/disk	Konfigurer enheder så de automatisk gennemfører anti	1	1	1
8	8,5	Enheder	Beskyt	Slå auto-run fra	Konfigurer enheder til IKKE at køre auto-run fra flytbare medier	1	1	1
8	8,6	Enheder	Opdag	Centraliser anti-malware logning	Send alle malware hændelser til det centrale anti-malware system og til organisationens centrale log system så de kan analyseres og der kan alarmeres hvor det er relevant		1	1
8	8,7	Netværk	Opdag	Slå DNS forespørgsel logs til	Sørg for at Domain Name System (DNS)		1	1
8	8,8	Enheder	Opdag	Slå kommando linje logning til	Sørg for at slå kommando linje logs til for		1	1
12	12,1	Netværk	Identificer	Vedligehold en inventarliste med alle	Vedligehold en opdateret inventarliste med	1	1	1
12	12,2	Netværk	Opdag	Scan for uautoriseret kommunikation på tværs af	Gennemfør regelmæssige scanninger fra ydersiden mod		1	1
12	12,3	Netværk	Beskyt	Stop/forhindr kommunikation med alle kendte malware IP	Stop kommunikationen med kendte malware eller		1	1
12	12,4	Netværk	Beskyt	Stop/forhindre kommunikation på alle	Stop kommunikationen over	1	1	1
12	12,5	Netværk	Opdag	Implementer et overvågningssystem som kan	Konfigurer overvågningssystemer til at		1	1
12	12,6	Netværk	Opdag	Implementer IDS scannere i netværket	Udrul netværksbaserede Intrusion Detection		1	1
12	12,7	Netværk	Beskyt	Udrul IPS systemer i netværket	Udrul netværksbaserede Intrusion Prevention			1
12	12,8	Netværk	Opdag	Deploy NetFlow Collection on Networking	Aktiver modtagelsen af NetFlow og log		1	1
12	12,9	Netværk	Opdag	Udrul en proxy server til filtrering af applikationstrafik	Vær sikker på at al netværkstrafik til og fra internettet			1
12	12,10	Netværk	Opdag	Dekrypter netværkstrafik som paserer Proxy Serveren	Dekrypter alt krypteret netværkstrafik ved perimeter			1
12	12,11	Brugere	Beskyt	Gennemtving MFA på remote login til	Kræv at al fjern login til organisationens		1	1
12	12,12	Enheder	Beskyt	Alle enheder der kan logger remote ind på	Scan alle enheder der bruges til fjern			1
#3: Kryptering af mobile enheder (CIS CSC #13) og Mobile Device Companion: https://www.cisecurity.org/white-papers/cis-controls-mobile-companion								
13	13,1	Data	Identificer	Vedligehold en inventarliste med alle	Vedligehold en inventarliste af alle sensitive	1	1	1

Implementeringsgruppe 1
Implementeringsgruppe 2
Implementeringsgruppe 3

13	13,2	Data	Beskyt	Fjern alle sensitive data/systemer fra organisationens netværks hvis de ikke tilgås regelmæssigt	Fjern alle sensitive data og systemer som ikke tilgås regelmæssigt af organisationen fra netværket. Disse systemer skal kun kunne bruges som isolerede systemer (Stand-Alone) som er koblet fra organisationens netværk. Alternativt skal de helt virtualiseres og slukkes indtil de	1	1	1
13	13,3	Data	Opdag	Overvåg og bloker uautoriseret netværkstrafik	Udrul et automatiseret system på organisationens perimeter som overvåger uautoriseret overførsel af sensitive informationer og blokerer denne trafik med en alarm til it-sikkerhedsafdelingen			1
13	13,4	Data	Beskyt	Giv kun adgang til autoriserede skytjenester (fx data storage)	Tillad kun adgang til autoriseret on-line lagerplads		1	1
13	13,5	Data	Opdag	Overvåg og opdage alle uautoriserede former for	Overvågt trafik som forlader organsationen for at opdage			1
13	13,6	Data	Beskyt	Krypter data fra mobile enheder	Udnyt godkendte krypteringsmetoder til at beskytte organistionens	1	1	1
13	13,7	Data	Beskyt	Administrer USB enheder	Hvis USB sticks er et krav skal organisationen begrænse		1	1
13	13,8	Data	Beskyt	Administrer systemers ekstern diske (som kan	Konfigurer systemer til ikke at kunne skrive data til eksterne			1
13	13,9	Data	Beskyt	Krypter alle data på USB sticks	Hvis USB sticks er et krav, skal alle data skrevet til disse enheder			1

#4: Efterlevelse af PCI-DSS

CIS V7.1 Controls	PCI DSS 3.2	PCI DSS 3.1	PCI DSS 3.0	Se mere på https://www.auditscripts.com/free-resources/critical-security-controls/ (MS Excel Dokument: AuditScripts-CIS-Controls-Master-Mappings-v7.1c.xlsx)
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	2,4	2,4	2,4	
Critical Security Control #2: Inventory of Authorized and Unauthorized Software	2,4	2,4	2,4	
Critical Security Control #3: Continuous Vulnerability Assessment and Remediation	6.1 6.2	6.1 6.2	6.1 6.2	
Critical Security Control #4: Controlled Use of Administrative Privileges	2.1 7.1 - 7.3	2.1 7.1 - 7.3	2.1 7.1 - 7.3	
Critical Security Control #5: Secure Configurations for Hardware and Software	2.2 2.3	2.2 2.3	2.2 2.3	
Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs	10.1 - 10.9	10.1 - 10.8	10.1 - 10.7	
Critical Security Control #7: Email and Web Browser Protections	2.2 2.3	2.2 2.3	2.2 2.3	
Critical Security Control #8: Malware Defenses	5.1 - 5.4	5.1 - 5.4	5.1 - 5.4	
Critical Security Control #9: Limitation and Control of Network Ports	1,4	1,4	1,4	
Critical Security Control #10: Data Recovery Capabilities	4.3 9.5 - 9.7	4.3 9.5 - 9.7	4.3 9.5 - 9.7	
Critical Security Control #11: Secure Configuration for Network Devices, such as Firewalls, Routers a	1.1 - 1.2 2.2	1.1 - 1.2 2.2	1.1 - 1.2 2.2	
Critical Security Control #12: Boundary Defense	1.1 - 1.3 8.3	1.1 - 1.3 8.3	1.1 - 1.3 8.3	
Critical Security Control #13: Data Protection	3.6 4.1 - 4.3	3.6 4.1 - 4.3	3.6 4.1 - 4.3	
Critical Security Control #14: Controlled Access Based on the Need to Know	1.3 - 1.4 4.3	1.3 - 1.4 4.3	1.3 - 1.4 4.3	
Critical Security Control #15: Wireless Access Control	4.3 11.1	4.3 11.1	4.3 11.1	
Critical Security Control #16: Account Monitoring and Control	7.1 - 7.3 8.7 - 8.8	7.1 - 7.3 8.7 - 8.8	7.1 - 7.3 8.7 - 8.8	
Critical Security Control #17: Implement a Security Awareness and Training Program	12,6	12,6	12,6	
Critical Security Control #18: Application Software Security	6.3 6.5 - 6.7	6.3 6.5 - 6.7	6.3 6.5 - 6.7	
Critical Security Control #19: Incident Response and Management	12.10	12.10	12.10	
Critical Security Control #20: Penetration Tests and Red Team Exercises	11,3	11,3	11,3	