

Audit Rapport

Stage 2

Audit dato	2026-08-18
Audit Lokation(er)	Hovedsæde
Audit Standard(er)	ISO/IEC 27001:2022
Lead auditor	Kurt Søndergaard
Report ID	401
Certificeringsorgan	Compliance Group Int. ApS Emil Aarestrups Gade 3-5 4990 Sakskøbing Danmark
CVR.	5331261
Danak Akkreditering nr.	5023
Kunde Navn	Software Fabric ApS
Kunde Adresse	Reberbanevej 8 8900 Randers C.
Kunde Kontakt	Dennis Sørensen
Kontakt e-mail	ds@planner4you.dk
Kunde CVR (ID)	30276981

Indholdsfortegnelse

Virksomhedens omfang (scope):	3
Resumé.....	3
Konklusion af audit	3
Tidspunkt for indsendelse af rettelser (CAP)	3
Audit mål, omfang og kriterier	4
Remote / Hybrid Audit.....	4
Audit deltagere	5
Audit Team.....	6
Management review, internal audit, SOA	7
Findings fra denne audit.....	7
Afviigelser, observationer og forbedringsforslag	12
Observationer	17
Forbedringsforslag	18
Næste skridt.....	21
NCR lukningsproces	21
Næste besøgs mål, omfang og kriterier	21
Plan for næste besøg	22
Certificeringsstruktur og løbende auditprogram.....	23
Scope for certificering	23
Auditerede lokation(er)	23
3-årigt certificeringsprogram	23
Definitioner af findings:.....	25
Note:	25
Overholdelse af lovgivningen.....	26

Virksomhedens omfang (scope):

Denne audit vedrører virksomhedens omfang gengivet herunder

Udvikling, salg, drift, hosting og kundesupport af SaaS-plattformen Planner4You til planlægning, journalisering og medicinhåndtering, jf. statement of applicability version 1. August 2026 Rev. 1 August 2026

Resumé

Auditten viser, at organisationen har etableret et godt fundament for ISMS med tydeligt ledelsesengagement og relevante politikker og processer. Risikostyring, leverandørstyring, kompetencestyring og awareness er generelt godt etableret og dokumenteret. ISMS'et er dog fortsat i en modningsfase, hvor implementeringen af SoA-kontroller endnu ikke er fuldt integreret i den daglige drift. Organisationens kontekst og informationsklassifikation bør styrkes og dokumenteres yderligere. Informationssikkerhedsmål og performance-målinger bør udvikles med tydeligere og mere målbare KPI'er. Roller og ansvar bør vurderes yderligere, særligt hvor CEO-, CISO- og ejerroller er samlet. Intern audit, management review og incident management er etableret, men der er fortsat begrænset praktisk erfaring. På den tekniske side er kontrollerne generelt godt implementeret og effektive. Samlet set er ISMS'et godt etableret, men kræver yderligere modning, herunder en mere formaliseret proces for løbende forbedringer. Asset register skal forbedres og have de nødvendige data og ejerskaber integreret.

Konklusion af audit

Den auditerede organisation kan anbefales til certificering / fortsat certificering, baseret på accept af en tilfredsstillende korrigerende handlingsplan for alle 'Minor' findings som vist i denne rapport. Effektiv implementering af korrigerende handlinger vil blive gennemgået under den næste overvågningsrevision. Korrigerende handlingsplan er således påkrævet ('Minor' findings).

Tidspunkt for indsendelse af rettelser (CAP)

Indsendelse af plan for korrigerende handlinger skal være indsendt senest den 2026-09-18

Audit mål, omfang og kriterier

ISO 27001:2022 's dokumentation af ledelsessystem til informationssikkerhed

Remote / Hybrid Audit

Er audit gennemført helt eller delvist remote? Nej

Audit deltagere

NAVN	FUNKTION	AUDITERET	ÅBNINGSMØDE	LUKKEMØDE
Dennis Bilici Sørensen	CEO	X	X	X
Nikolaj Sørensen	Konsulent	X	X	X
Dennis Mogensen	CTO	X	X	X
Jeniith Jeyanthisivam	Supporter	X		
Louis Bilici	Projektleder	X		

Audit Team

CG Audit team:

Kurt Søndergaard, Lead auditor

Chris Nielsen, Team member

Management review, internal audit, SOA

Mandatory områder for rapportering

Management review: Planlagt og gennemført Evt dato for udførsel:

Intern audit: Planlagt og gennemført Evt dato for udførsel:

SOA: Rev. 1 August 2026

Brug af Logo: Brug af mærker er ok

Findings fra denne audit

Organisationens kontekst

16 medarbejdere nu
Virksomheden har udviklet sig og på vej mod et større segment
DOC097 Værditekst 26062026 omkring virksomhedens værdier PRO001 - Scope/omfang
Kontekst er gennemgået og fundet for tynd undtagen på hjemmesiden
Interessentanalysen PRO012 Rev. 1, 26062026 gennemgået
Lovkrav er defineret i DOC028 Rev. 1, 26062026, Lovmæssige, vedtægtsmæssige, regulatoriske og kontraktlige krav
NIS2 er diskuteret og i fokus men endnu ikke et vist krav
Ledelsessystemet er MasterQMS, der er beregnet på at styre ISMS dokumenter

Området er generelt veldefineret og på plads, med undtagelse af det nævnte kontekst dokument

Ledelse og ISMS-styring, Dokumentation

Organisationsdiagram Ver. 2.0 August 2026 vist. en ny version undervejs
Konsulent som intern auditor i virksomheden. Den foretages årligt
Intern audit og rapportering styres i MasterQMS
Intern audit udføres af ekstern konsulent
Besøgslog er i MasterQMS
Afvigelser og incidents er i Planner4You
DOC095 Roller, ansvar og beføjelser, Rev. 1.0, 15062026
IS organisationen er bestående primært af de 3 ledere

D.v.s. CEO, CTO og en stedfortræder
CEO og CISO er samme person
Dette er samtidig ejergruppen
dette kan give et paradoks i forhold til A5.1 til A5.4
AMO er undervejs til etablering i firmaet
POL008 Informationssikkerhedspolitik Rev 3. 18082026
Der udvises generelt et godt lederskab ud fra de beskrevne handlinger.
Det underbygges af virksomhedens værdier i DOC097

Der er meget fokus på at uddelegere til de der har faglighed og kompetence inden for de enkelte områder

Politikken er gennemgået og denne er blevet godt opdateret fra stage 1
Den er kommunikeret ud til alle medarbejdere ved en ren gennemgang med dem
Adressees en gang i kvartalet
Dokumentet ligger også i Planner4you, som bruges af alle
Intern audit udføres af ekstern konsulent
DOC013 Klassifikation af information Rev.1, 12062026 går kun på GDPR data
Klassifikation er implicit og ikke dokumenteret for dokumenter

Området er generelt veldefineret og compliant med standarden

Risikovurdering og behandling, Gennemgang af SOA

Risiko metodik udgår fra en standard metode med sansynlighed og konsekvens, med en skala på 1-5

4 Prioritetskategorier for behandling med accepter, Overvåg/planlæg, Behandl snarest og akut (Skaleres til ledelse)

Omkring kontrol af risici, er der opbevaret logs i 5 år

Der er p.t. ca. 30 punkter i risikovurderingen, disse er ikke nødvendigvis alle, men de mest sandsynlige ud fra virksomhedens syn på dette

Statement of applicability er etableret, men ikke alle kontroller er fuldt i drift.

De er implementeret, men det er ikke blevet en naturlig del af hverdagen

Implementeringen af SOA er ikke helt på plads, mindre afvigelse lavet.

A8.30 outsourced development er fravalgt, da der ikke bruges eksterne udviklere

Området er generelt veldefineret og compliant med standarden

Mål og planlægning:

Disse er i informationssikkerhedspolitikken

Der er et begrænset antal, med begrænset målbarhed

En observation er rejst

Evt. er der en medarbejder, der kunne være med til dette

Planlægning er ændringer i informationssikkerheds systemet

Den eksisterende procedure er beskrevet

Dokumentation - onsdag

Beskrives som forespørgsel hos jurist, derefter møde med medarbejdere og udkast udarbejdes

Området er generelt veldefineret og compliant med standarden

Støtteprocesser / ressourcer/dokumentation:

Kompetencer er registrerede i MasterQMS i et internt regneark, der ser på alle ansatte

Har givet fokus på kompetencer og interviews

Bruger løbende samtaler som medarbejderinterviews og dokumenteres i kompetenceskemaer

Proceduren omkring det står i personalehåndbog DOC002 Rev. 2, 26062026

PRO017 Planlægning af ændringer af ledelsessystem 10062026 gennemgået og helt efter bogen

Her er også hvordan awareness træning foretages

Awareness procedure PRO002 Rev. 0, 26062026

Årshjul er etableret omkring træning

Awarenes log er fremvist, næste træning den 2/9

PRO016 - Styring af dokumenteret information Rev. 0, 18082026 er fuldt dækkende

Intellectual property gennemgået med rettigheder om dette.

Dokumentstyring er gennemgået (7.5.3)

Klassifikation gennemgået og der er kun en dokumentation omkring GDPR data

Der er rejst en afvigelse

Området er generelt veldefineret og compliant med standarden

Human Resources:

De fleste HR dele ligger i personalehåndbogen Rev. 2.1

Minor NC i revisionsstyring

Meget fokus på livssyn og menneskesyn

Meget høj personaleloyalitet

INS001 Screening Rev. 1. 26082026

Denne indeholder krav om straffeattest, men kun børneattest hvis der er borgerkontakt

6 måneders prøveperiode for alle

Kontrakt template indeholder de nødvendige forhold om tavshed og intellectual property

Tavshedserklæring indeholder forkert firmanavn

PRO014 procedure for awareness træning, Rev. 0, 26062026

Vilkår for udlån af udstyr

Disciplinær proces er ifølge funktionærlovgivning

Denne er lavet som implicit men ej nedskrevet

Området er generelt ok og compliant med standarden

Operationel planlægning og kontrol

Disse omhandler de primære tekniske processer og er auditeret af den tekniske auditor
DOC041 Dokumenterede driftsprocedurer Rev. 3, 17082026 gennemgået

Leverandørstyring

DOC098 Leverandøroversigt Rev. 0, 26062026
DOC017 Informationssikkerhed i leverandørforhold Rev.4, 12062026
DOC043 Håndtering af informationssikkerhed i leverandøraftaler 12062026
DOC019 Overvågning, gennemgang og ændringshåndtering af leverandøraftaler
Alle 3 er veldokumenterede og gennemgribende. Der er god grundlæggende kontrol
Forhold omkring open source er ikke fuldt dokumenteret
Dette gælder også procedure for valg, test og brug
Generelt vel dokumenteret og gennemført

Monitorering, Intern audit, Evaluering af resultater, Management review

PRO013 intern audit plan Rev. 2, 26062026 gennemgået
Denne gennemgår ISO, men mangler medarbejderinterviews som er indføjet
Årshjul er etableret og implementeret
Intern audit gennemføres kvartalsvis
Intern audit 1-13082026-1 gennemgået
Denne bærer præg af at det er tidligt i forløbet
Det er dog et godt udgangspunkt
Der manglede interview delen, men denne er blevet implementeret

Performance målinger er primært på de tekniske dele og styres af CTO vil monitoreres der
De er ikke veldokumenterede og der er ligeledes
DOC067 Kapacitetsstyring og DOC077 Overvågningsaktiviteter
Der tales her om Social engineering som målesystem
Målinger er ikke fuldt på plads i hele organisationen
Der tales meget om KPA for adfærd som målinger i den "bløde" del af virksomheden og
administration

Området er generelt ok og compliant med standarden, dog med for få mål og målsætninger

Management review (ledelsesevaluering)

Ledelsesevaluering 17082026
Evalueringen er 1 gang årligt officielt, men gennemføres i praksis kvartalsvis
Afvigelser og incidents er der endnu ikke noget særligt input.
Kun en omkring en reel testperson fra sundhedsdatanettet

Området er generelt ok og compliant med standarden idet den følger den i standarden angivne agenda.

Actions / Non-Conformity / Incidents / Complaints, Improvement

Afvigelseshåndtering er implementeret i virksomhedens primære platform og der rapporteres direkte i denne for afvigelser på ISO, B2B (kunder) og leverandører

Der er indtil videre kun 1 incident registreret, Denne er omtalt i ledelsesevalueringen

PRO002 Procedure for afvigelser Rev. 2, 17042026

DOC021 Planlægning og forberedelse af håndtering af incidents Rev. 2, 2, 12062026

PRO009 DR plan Rev.3, 25062026 gennemgået

DR recovery plan er endnu ikke testet da platformen er helt nyinstalleret

Test har været foretaget på den tidligere platform

DOC024 Læring af informationssikkerhedshændelser Rev. 2, 12062026

Drejer sig om læring og er det nærmeste der er omkring en forbedringsproces

Der mangler en decideret proces for løbende forbedringer

og det er nævnt herudover

Området er generelt svagt, men compliant med standarden bortset fra de nævnte mangler

Adgangsstyring

Der er implementeret procedurer for håndtering af adgangsstyring, styring af identitet og autentificering samt procedurer for håndtering af privilegerede adgange.

Vi har ved inspektion af brugeradgange i systemer og udviklingsmiljø, konstateret at adgangene var passende jf. gældende procedurebeskrivelser.

Kommunikationssikkerhed

Der er designet og implementeret procedurer for overførsel af information, sikker overførsel, brug af kryptografi samt web filtrering.

Der er implementeret tekniske foranstaltninger for at understøtte brugen af kryptografi ved overførsel af informationer, både intern i organisationen samt med eksterne kunder mv.

Aftaler med kritiske underleverandører er gennemgået.

Der er implementeret logisk segmentering af netværk i organisationen.

Cybersikkerhed

Der er designet og implementeret procedurer for beskyttelse mod malware, håndtering af tekniske sårbarheder samt forebyggelse af dataleakage.

Awareness træning for medarbejdere inkluderer punkter vedr. malware og tekniske sårbarheder.

Informationsopbevaring

Der er designet og implementeret procedurer for beskyttelse af optegnelser, håndtering af lagringsmedier, sikker bortskaffelse eller genbrug af udstyr & lagringsmedier, sletning af information, håndtering af backup af information.

Der er passende reference til gældende lovgivning og kundekrav i procedure for sletning af information og håndtering af backup af information.

Ved stikprøve inspektion af databehandleraftale med én tilfældig udvalgt kunde fandt vi ingen afvigelse fra organisationens egne procedure.

Fysiske foranstaltninger

Der er passende kontorområder. Indgangsområde er overvåget af fast personale. Andre indgange er aflåst fast.

Der er designet og implementeret procedurer for fysisk perimetersikring, sikre arbejdsområder, overvågning af arbejdsområder, clear screen clear desk samt beskyttelse mod fysiske og miljømæssige trusler.

Vi har ved fysisk inspektion af kommunikations- og serverrum kunnet konstatere at organisationen følger egen procedure for sikring af informationsfaciliteter.

Vi har gennemgået revisionserklæring om kontroller hos kritisk underleverandør til organisationens kundevendte drift, og ikke fundet afvigelser.

Systemudvikling og vedligehold

Der er designet og implementeret procedurer for adgang til kildekode, konfigurationsstyring, installation af software på driftssystemer, sikker udviklingscyklus, krav til applikationssikkerhed, sikker programmering samt brugen af test data og test miljø.

Vi har ved inspektion af to tilfældige stikprøver kunnet konstatere at procedure for sikker udviklingscyklus er blevet efterlevet. Vi gennemgik to kodegennemgange og godkendelser, som efterlevede organisationens fire-øjne princip.

Vi har ved inspektion af udviklingsmiljø og udviklingsværktøj kunne konstatere at test data og information bliver automatisk genereret og disse ikke bliver generet fra reelle produktionsdata.

Afgigelser, observationer og forbedringsforslag

Audit Finding(403)	
ID	403

Område (Agenda punkt)	Risikovurdering og SOA
Requirement (Clause)	8.2
Control	
Objective Evidence	SOA mangler de ansvarlige og er ikke helt gennemskuelig grundet implementeringen i MasterQMS.
Type of Finding	Minor Nonconformity
Cause	
Correction / Containment	
Corrective Actions	
- - - - -	
Audit Finding(404)	
ID	404
Område (Agenda punkt)	HR
Requirement (Clause)	7.5.3
Control	
Objective Evidence	Revisionsstyring er ikke konsekvent.
Type of Finding	Minor Nonconformity
Cause	
Correction / Containment	
Corrective Actions	
- - - - -	
Audit Finding(406)	
ID	406

Område (Agenda punkt)	Overvågning
Requirement (Clause)	9.1
Control	
Objective Evidence	Der er ikke udvalgt målepunkter til KPI'er. Dette er tilsyneladende på grund af skiftet til ny platform og derfor ikke kørt helt på plads.
Type of Finding	Minor Nonconformity
Cause	
Correction / Containment	
Corrective Actions	
- - - - -	
Audit Finding(408)	
ID	408
Område (Agenda punkt)	Dokument og dokument klassifikation
Requirement (Clause)	
Control	A.5.12
Objective Evidence	Der er ikke formuleret en klassifikation for information, selvom den er initieret i SOA
Type of Finding	Minor Nonconformity
Cause	
Correction / Containment	
Corrective Actions	
- - - - -	
Audit Finding(412)	
ID	412

Område (Agenda punkt)	Asset Management
Requirement (Clause)	
Control	A.5.9
Objective Evidence	Der skal udarbejdes et asset register som fyldestgørende viser alle informationsaktiver. Altså både Hardware, hvor information er lagret, men også andre typer af informationer, som for eksempel regnskabsdata, kundedata, salgsdata, HR data, mv.
Type of Finding	Minor Nonconformity
Cause	
Correction / Containment	
Corrective Actions	
- - - - -	
Audit Finding(413)	
ID	413
Område (Agenda punkt)	Beskyttelse mod fysiske og miljømæssige trusler
Requirement (Clause)	
Control	A.7.5
Objective Evidence	Der er ikke tilstrækkeligt designet procedure for beskyttelse mod fysiske og miljømæssige trusler. Som minimum skal der tilføjes til risikoregisteret: (1) at der forefindes aktive vandrør i server- og kommunikationsrum, (2) at der mangler brandslukningsudstyr i server- og kommunikationsrum, (3) at der er manglede temperaturstyring i serverrum.
Type of Finding	Minor Nonconformity
Cause	
Correction / Containment	

Corrective Actions	
- - - - -	
Audit Finding(414)	
ID	414
Område (Agenda punkt)	Information backup
Requirement (Clause)	
Control	A.8.13
Objective Evidence	Der skal anføres I proceduren scope og interval for udførelse af restore test.
Type of Finding	Minor Nonconformity
Cause	
Correction / Containment	
Corrective Actions	
- - - - -	
Audit Finding(415)	
ID	415
Område (Agenda punkt)	Sikrings af netværkstjenester
Requirement (Clause)	
Control	A.8.21
Objective Evidence	Der skal udarbejdes en SLA for kundevedte driftsystemer -- alternativt skal kundeaftaler indeholde oplysninger om opetid, kundeservice-kanaler mv.
Type of Finding	Minor Nonconformity
Cause	

Correction / Containment	
Corrective Actions	
- - - - -	

Observationer

Audit Finding(402)	
ID	402
Område (Agenda punkt)	Organisationsnens kontekst
Requirement (Clause)	4.1
Control	
Objective Evidence	Kontekst er ikke tilstrækkeligt defineret i ISMS, men refereret til på hjemmesiden. Den bør skal fremgå af ISMS direkte som grundlæggende dokument for denne.
Type of Finding	Observation
- - - - -	
Audit Finding(405)	
ID	405
Område (Agenda punkt)	Leverandørhåndtering
Requirement (Clause)	
Control	A.5.20
Objective Evidence	Forhold omkring open source er ikke fuldt dokumenteret Dette gælder også procedure for valg, test og brug
Type of Finding	Observation
- - - - -	

Audit Finding(416)	
ID	416
Område (Agenda punkt)	Sikring af netværkstjenester
Requirement (Clause)	
Control	A.8.21
Objective Evidence	Der bør defineres en process for regelmæssig gennemgang af aftaler og SLA'er fra kritiske underleverandører.
Type of Finding	Observation
- - - - -	

Forbedringsforslag

Audit Finding(407)	
ID	407
Område (Agenda punkt)	Forbedringsforslag
Requirement (Clause)	10.2
Control	
Objective Evidence	DOC024 kan forbedres og forbedringsproces kan dokumenteres lidt bedre.
Type of Finding	Opportunity for improvement
- - - - -	

Audit Finding(417)	
ID	417
Område (Agenda punkt)	Overførsel af information
Requirement (Clause)	

Control	A.5.14
Objective Evidence	Tilføj procedure beskrivelse for brugen af sagshåndteringssystemet (tickets), ifm. kundeservice og -kommunikation. Denne process er pt. implicit.
Type of Finding	Opportunity for improvement
- - - - -	
Audit Finding(418)	
ID	418
Område (Agenda punkt)	Clear desk, Clear screen
Requirement (Clause)	
Control	A.7.7
Objective Evidence	(1) Align jeres clear screen clear desk procedure med samme afsnit i personalehåndbogen. (2) Ved stikprøvekontrol fandt vi herreløs hardware MFA token, samt dokumentation til interne systemer.
Type of Finding	Opportunity for improvement
- - - - -	
Audit Finding(419)	
ID	419
Område (Agenda punkt)	Brugerenheder
Requirement (Clause)	
Control	A.8.1
Objective Evidence	Det er tvetidigt om det er tilladt for medarbejdere at benytte egne enheder. Og regler for brugen af egne enheder er ikke defineret skriftligt.
Type of Finding	Observation
- - - - -	
Audit Finding(420)	
ID	420

Område (Agenda punkt)	Information Deletion
Requirement (Clause)	
Control	A.8.10
Objective Evidence	Der bør udarbejdes en definition på hvornår information ikke skal gemmes længere. Refer gerne generelt til gældende lovgivning, kundekrav mv.
Type of Finding	Observation
- - - - -	
Audit Finding(421)	
ID	421
Område (Agenda punkt)	Change Management
Requirement (Clause)	
Control	A.8.32
Objective Evidence	Der bør tilføjes reference til de andre klasser af informations faciliteter (bærbar mv.), til den eksisterende change management procedure.
Type of Finding	Observation
- - - - -	

Næste skridt

NCR lukningsproces

Se afsnittet Audit konklusion og anbefaling for en eventuel påkrævet indsendelse og definerede tidslinje.

Næste besøgs mål, omfang og kriterier

CAV - Målet med audit er at gennemføre en overvågningsaudit og lede efter positive beviser for at bekræfte, at elementer af certifikatscope og kravene i ledelsestandarderne effektivt håndteres af organisationens ledelsessystem; at systemet viser evnen til at understøtte opnåelsen af lovpligtige, reguleringsmæssige og kontraktlige krav samt organisationens specificerede mål i forhold til omfanget af ledelsestandarden; at bekræfte den fortsatte opnåelse og anvendelighed af den fremadskuende strategiske plan.

ISO 27001:2022

Dokumentation af ledelsessystem for informationssikkerhed

Bemærk venligst, at CG forbeholder sig ret til at opkræve et gebyr svarende til den fulde dagspris for organisationens afbestilling af besøget inden for 30 dage efter en aftalt besøgsdato. Det er en betingelse for registreringen, at der udpeges en suppleant for direktionen. Det forventes, at stedfortræderen træder i stedet, hvis ledelsesrepræsentanten ikke er til rådighed for at deltage i et aftalt besøg inden for 30 dage efter dets afførelse.

I øvrigt henvises til Compliance Groups Terms and conditions

Plan for næste besøg

Plan vil blive fremsendt 4 - 6 uger før næste audit

Certificeringsstruktur og løbende auditprogram

Scope for certificering

IS 26005 (ISO/IEC 27001:2022)

Udvikling, salg, drift, hosting og kundesupport af SaaS-plattformen Planner4You til planlægning, journalisering og medicinhåndtering, jf. statement of applicability version 1. August 2026

Auditerede lokation(er)

Hovedsæde

Lokation (site)	Hovedsæde
Audit type	
Audit dato	2026-08-18
Afvigelse fra auditplan	
Total antal ansatte	16
Scope for aktiviteterne på site	Udvikling, salg, drift, hosting og kundesupport af SaaS-plattformen Planner4You til planlægning, journalisering og medicinhåndtering, jf. statement of applicability version 1. August 2026
Audit duration	3,5

3-årigt certificeringsprogram

Det 3-årige certificerings program er certificeringsorganets grundlæggende struktur over hvilke områder, der skal gennemgås over en 3-årig cyklus.

Den herunder viste er den generelle og denne kan ændres hvis der viser sig brug for at ændre denne på grund af specifikke områder der er behov for at genbesøge grundet svage eller risikofyldte områder.

Audit area	Participants	Year 0	Year 1	Year 2	Year 3	ISO/IEC 27001 clause	ISO/IEC 27002 Controls
		08/26	06/27	06/28	06/29		

Opening meeting	All	X	X	X	X	—	—
Context of the organization	All	X	X		X	4.1 – 4.4	A.5.1, A.5.2, A.5.3
Management and ISMS management	Top management, everyone	X	X	X	X	5.1 – 5.3	A.5.4, A.5.5, A.5.7
Risk assessment and treatment	Risk, IT, all	X	X	X	X	6.1.1 – 6.1.3	A.5.9, A.5.10, A.5.11
Goals & Planning	All	X		X	X	6.2 – 6.3	A.5.6, A.5.13
Support processes	HR, Admin, Training	X	X		X	7.1 – 7.5	A.6.1 – A.6.5
Operational planning and control	Production, development, IT production	X		X	X	8.1	A.5.15, A.8.25
Control of staff	HR, Managers	X	X		X	8.1	A.6.1 – A.6.5
Physical controls	Facilities, Production	X		X	X	8.1	A.7.1 – A.7.10
Technology Controls - Part 1	IT, Development	X	X		X	8.1	A.8.1 – A.8.10
Technology Controls - Part 2	IT, DevOps, IT Production	X		X	X	8.1	A.8.11 – A.8.20
Monitoring, auditing, performance evaluation, Management review	Compliance, Internal Audit, Support	X	X	X	X	9.1 – 9.3	A.5.14, A.8.16, A.8.23
Deviations and improvement	All, Support	X	X	X	X	10.1 – 10.2	A.5.12, A.5.17
Annex A Control — SoA Verification	All	X	X	X	X	Appendix A	All implemented controls

Definitioner af findings:

Afvigelse:

Manglende opfyldelse af et krav.

Større afvigelser (Major NC):

Afvigelse, der påvirker ledelsessystemets evne til at opnå de tilsigtede resultater.

Afvisninger kan klassificeres som alvorlige under følgende omstændigheder:

- Hvis der er væsentlig tvivl om, at effektiv proceskontrol er på plads, eller at produkter eller tjenester vil opfylde specificerede krav;
- En række mindre afvigelser i forbindelse med samme krav eller problem kan påvise et systemisk svigt og dermed udgøre en væsentlig afvigelse.
- Store afvigelser kræver en indlevering af plan for løsning af denne inden 30 dage og Lukning ved genbesøg inden for 6 måneder

Mindre afvigelser (Minor NC):

Manglende overensstemmelse, der ikke påvirker ledelsessystemets evne til at opnå de tilsigtede resultater.

- Ved første gangs certificering og re-certificering skal der indleveres en plan for løsning af afvigelser inden for 30 dage. Denne skal godkendes af certificeringsorganet før udstedelse af certifikat

Mulighed for forbedring (OFI):

Det er en konstatering af de faktiske omstændigheder, der er fremsat af en bedømmer under en audit, og som underbygges af objektive beviser, og som henviser til en svaghed eller potentiel mangel i et ledelsessystem, som, hvis den ikke forbedres, kan føre til manglende overensstemmelse i fremtiden. Vi kan give generiske oplysninger om bedste praksis i industrien, men der skal ikke gives nogen specifik løsning som en del af en mulighed for forbedring.

Observation (OBS):

Det er en erklæring om de faktiske omstændigheder, som bedømmeren har fremsat, og som henviser til en svaghed eller potentiel mangel ved et ledelsessystem, som, hvis den ikke forbedres, kan føre til en manglende overensstemmelse i fremtiden.

Note:

Denne rapport og relaterede dokumenter er udarbejdet til og kun til CG's klient og ikke til andre formål. Som sådan påtager CG sig ikke noget ansvar (juridisk eller på anden måde) eller påtager sig noget ansvar for eller i forbindelse med andre formål, som rapporten kan bruges til, eller over for nogen anden person, som rapporten vises til eller i hvis hænder den måtte komme, og ingen andre personer er berettiget til at stole på rapporten. Hvis du ønsker at distribuere kopier af denne rapport uden for din organisation, skal alle sider inkluderes.

CG, dets personale og agenter skal holde alle oplysninger vedrørende din organisation fortrolige og må ikke videregive sådanne oplysninger til nogen tredjepart, undtagen dem, der er offentligt tilgængelige eller påkrævet ved lov eller relevante akkrediteringsorganer. CG's personale, agenter og

akkrediteringsorganer har underskrevet individuelle fortrolighedsforpligtelser og vil kun modtage fortrolige oplysninger på "need to know"-basis.

Denne audit blev gennemført gennem dokumentgennemgang, interviews og observation af aktiviteter. Den anvendte audit metode er baseret på stikprøver af organisationens aktiviteter, og den har til formål at evaluere opfyldelsen af de reviderede krav i den relevante ledelsessystemstandard eller andet normativt dokument og bekræfte ledelsessystemets overensstemmelse og effektivitet og dets fortsatte relevans og anvendelighed for certificeringens omfang.

Da denne audit er baseret på en stikprøver af organisationens aktiviteter, indebærer de rapporterede resultater ikke, at de omfatter alle problemer i systemet.

Overholdelse af lovgivningen

CG's kontraktbetingelser for dette besøg kræver, at CG informeres om alle relevante lovgivningsmæssige afvigelser eller hændelser, der kræver underretning til en regulerende myndighed. Kundens accept af denne rapport betyder, at alle sådanne problemer er blevet oplyst som en del af revisionsprocessen og aftale om, at enhver sådan manglende overholdelse eller hændelser, der opstår efter dette besøg, vil blive meddelt CG-kundechefen