REVISJONSRAPPORT

Virksomhet:

FarPay ApS

Wildersgade 14, KØBENHAVN K, Denmark

Navn på virksomhetens kontaktperson:

Claus Thomsen, cth@farpay.dk

Revisjonstype:	**Revisjonslag:**	
Sertifiseringsrevisjon ISO 27001 **Sertifiseringsrevisjon ISO 27701**	Revisjonsleder Fageksper t Systemrevisor	Lars Farinha

Tidsrom for revisjonen :

2023-09-04/ 2023-09-07

Referansekrav i henhold til:

ISO/IEC 27001:2013
ISO/IEC 27701:2021

Sertifikatets virksomhetsområde og lokaliteter:

Sertifikatets virksomhetsområde og lokaliteter ved sertifisering:

Omfanget bestemt av virksomheten er datert: 2023-09-05

Engelsk sertifikattekst i samsvar med virksomhetens dokumenterte informasjon:

Development, sales and integration of The FarPay solution, a SaaS solution facilitating integration between different payment gateways and the customer's accounting solution, covering the functionalities Automatic payment, Automatic accounting, Automatic reminders, Intelligent invoice delivery, Payment link and Dashboards.

Lokaliteter omfattet av sertifiseringen:

Se revisjonsprogrammet for detaljer.

Vedlagt:

Revisjonsprogram – sertifiseringsperioden:

program-farpay-aps
-iso27001-27701.doc

REVISJONSRAPPORT

Oppsummering av revisjonen

Lokaliteter som ble revidert:	Tidsrom:
Se revisjonsprogram	2023-09-04/ 2023-09-07

Sammendrag og konklusjon fra revisjonen:

Revisjonen ble gjennomført i samsvar med vedlagte gjennomføringsplan og er basert på stikkprøver fra tilgjengelig informasjon.

Sammendrag

FarPay ApS er en IT-virksomhet som optimerer betaling og regnskap med sine alt-i-én SaaS IT-løsninger.

Styringssystemet for ISMS (inkludert 27701) er implementert i Confluence og oppfølging av saker/hendelser med bruk av Jira/HubSpot. Det er etablert en meget god struktur med bruk Confluence, som gir brukerne fin oversikt å finne fram i tilhørende policyer, prosedyrer og arbeidsinstrukser. Prosedyrer har egne flytskjemaer. Drift av FarPay ApS sine SaaS B2B løsninger utføres i Microsoft Azure. Det er ingen lokale servere i FarPay ApS sine lokaler.
Dokumentasjon blir lagret i Confluence. Årshjul er etablert, og vil være del av systemet å følge opp ISMS'en, samt det også er lagt inn automatiske due dates for å sikre gjennomgåelse av kontrollene i SoA i faste intervaller. Eier av sikringstiltak er dokumentert i gitte prosedyrebeskrivelser.
Årshjulet brukes også som et planverk for interne revisjoner.

Klassifisering av dokumenter var mangelfullt dokumentert i Confluence. Ble oppdatert under revisjonen.

On- og offboarding step blir dokumentert i Jira Kanban board.
Jump Cloud håndterer asset.

Opplæring/bevisstgjøring/bruk av ISMS Confluence har blitt utført digitalt (teams) og med bruk av diverse online-opplæringsmoduler. De som har blitt intervjuet har bra kjennskap til sine prosesser, og hvor de finnes i ISMS'et.

Baseline for risikoanalyse er etablert. Støre risikoer blir flyttet opp i Jira for videre oppfølging i Security Board.

Innkommende saker (Ticket) fra kunder blir håndtert i HubSpot. Avdeling Support er 1ste.linje service, mer komplekse saker flyttes over til Operation. Innkommende Ticket blir kategorisert, som igjen gir diskusjonsgrunnlag for videre forbedringer. Bra!

Sikringstiltak A.12 driftssikkerhet og A.14 utvikling/vedlikehold av systemer ble gjennomgått veldig grundig under revisjonen. Stikkprøver av de forskjellige sikringstiltakene viste de er i samsvar med standarden sine krav.
PIMS Anneks A ble gjennomgått. Det er tilrettelagt med utfyllende info på hjemmesidene hvordan persondata blir håndtert. Databehandleravtale er inngått med samarbeidspartnere.

Annen kommentar/info fra revisjonen:
Bra kvalitet på ledelsen gjennomgåelse. Vil bli utført 2 ganger i året.
Security Board meeting utføres hver måned. Oppfølgingssaker legger i Jira.
Farpay intranett er etablert, oversiktlig for bruker å finne fram hvor det skal registreres et avvik eller en hendelse.

Andre forhold

Forbedringer i ledelsessystemet gir økt ytelse og er relevante for interessepartene.
Alle punkter i gjennomføringsplanen som ikke er nevnt i rapporten, er funnet i orden.

I rapporten er det beskrevet forbedringsmuligheter i ledelsessystemet. Forbedringsmuligheter beskriver forhold som per nå ikke er vurdert som avvik fra kravene. Ved fremtidige revisjoner blir forbedringsmuligheter fulgt opp og revurdert opp mot sertifiseringskravene til ledelsessystemet.

REVISJONSRAPPORT

Revisjonsleders innstilling fra revisjonen:
Det er ikke funnet avvik ved denne revisjonen. Virksomheten har tilfredsstillende prosesser for internrevisjon og ledelsens gjennomgåelse. På grunnlag av relevante stikkprøver viser styringssystemet medvirkning til politikk og måloppnåelse, samt bidrag til kontinuerlige forbedringer i ytelse. Virksomhetens ledelsessystem anses å være i samsvar med standardkravene, interesseparters krav og omfanget til virksomhetens ledelsessystem. Revisjonsleder innstiller til sertifisering.
Neste revisjon:
Neste revisjon vil være en oppfølgingsrevisjon og er planlagt til: 2024-09-02/04

Revisjonens fokusområder

ISO 27001, overordnede konklusjoner sertifisering:	Samsvar iht til kravene? ->	Ja	Nei
Organisasjonen følger sine egne retningslinjer, mål og prosedyrer		X	
Toppledelsen forplikter seg til informasjonssikkerhetspolitikk og mål for informasjonssikkerhet		X	
Organisasjonen tilfredsstiller dokumentkravene oppført i standarden		X	
Informasjonssikkerhetsrelaterte risikoer og vurderinger gir konsistente, gyldige og sammenlignbare resultater hvis de gjentas		X	
Bestemmelse av kontrollmål og kontroller basert på risikovurdering av informasjonssikkerhet og risikobehandlingsprosesser		X	
Informasjonssikkerhetsprestasjoner og effektiviteten til ISMS, evaluert mot informasjonssikkerhetsmål		X	
Samsvar mellom innførte kontroller, SoA og resultatene av informasjonssikkerhets-risikovurderingene og risikobehandlingsprosessen og informasjonssikkerhets politikk og mål;		X	
Implementeringen av kontroller, med tanke på ekstern/ intern kontekst, relaterte risikoer, organisasjonens overvåking, måling og analyse av informasjonssikkerhetsprosesser og kontroller; Kontrollene er implementert og effektive og oppfyller målene for informasjonssikkerhet		X	
Funksjonaliteten til prosedyrer for periodisk evaluering og gjennomgang av etterlevelse av relevant lovgivning og forskrifter om informasjonssikkerhet		X	

Merk at konklusjonene baserer seg på stikkprøver.

Revisjonsleders overordnede konklusjoner ved sertifiseringen:	Samsvar iht til kravene? ->	Ja	Nei
Samsvar iht krav i standard		X	
Resultatoppfølging, måling, rapportering og gjennomgåelse opp mot mål		X	
Ledelsessystemets evne og ytelse til å møte myndighetskrav og kontraktsmessige krav		X	
Eventuelt åpne avvik fra offentlige myndigheter. Sett X i kolonnen "Ja", for samsvar med standard, ingen åpne avvik overfor offentlige myndigheter Sett X i kolonnen "Nei", for ikke samsvar med standard, det er åpne avvik overfor offentlige myndigheter		X	
Driftskontroll og styring i prosesser		X	
Internrevisjon og ledelsens gjennomgåelse		X	
Ledelsens ansvar for policy		X	

Merk at konklusjonene baserer seg på stikkprøver.

Forbedringsmuligheter i ledelsessystemet

Forbedringsmulighet 1 av 7: Rapport fra interne revisjoner

Med dagens dokumentasjon fra interne revisjoner hvor det ikke er funnet noen avvik, er dette kommentert med OK.
Ettersom interne revisjoner er basert på årshjulet i visse intervaller, bør det hvis mulig om det kan lages en slutt kommentar hvordan revisor opplevde revisjonen for dette intervallet. Det bør også vurderes på de områdene det kan oppstå en konflikt med habilitet at dette blir dokumentert hvordan dette ble håndtert i kommende revisjoner.

Forbedringsmulighet 2 av 7: Årshjul, interne revisjoner

Interne revisjoner er planlagt i henhold til årshjul. Det er noe mangelfullt dokumentert når revisjoner er utført i henhold til årshjulet, uten at gitte interne revisjoner er funnet fram i Confluence. Stikkprøver viste enkelte interne revisjoner som er planlagt avviker fra dato som er satt i årshjulet.

Forbedringsmulighet 3 av 7: Lokaler og innsyn

Stikkprøver viser at det ikke er diskutert hvordan innsyn utenfra/utsiden kan medføre utenforstående kan se interne dokumenter/bruk av digitale løsninger. For eksempel møterom som er i bruk har ikke egne retningslinjer å begrense innsyn ved bruk.

Forbedringsmulighet 4 av 7: Roadmap group

Roadmap group ble etablert sommeren 2023. Formålet med denne gruppen er bla bestemme prioriteringer, go/no-go på prosjekter. For sikrer utvikling av systemer bør det etablerers policyer og regler hvordan denne gruppen skal virke.

Forbedringsmulighet 5 av 7: Sertifikat utveksling Nordea

I visse intervaller utføres det sertifikat utveksling med Nordea, hvor bruk av sidemannskontroll er en del av prosedyren. Prosedyren er i dag person avhengig og ikke beskrevet i Confluence. Det bør etablerers dokumentasjon på denne prosedyren for å redusere risiko.

Forbedringsmulighet 6 av 7: A.17 Disaster recovery plan

Gjennomgang av Disaster recovery plan som er etablert i selskapet er meget generell, og noe mangelfull på enkelte scenarier den bør være mer tilpasset organisasjonen og dens interesseparter.
Det bør også komme tydeligere fram info på kontakt personer i de gitte scenariene og vurdere om maks nedetid er i samsvar med forventingene/forpliktelsene.

Forbedringsmulighet 7 av 7: A.18 Samsvar

Samsvar med juridiske og kontraktmessige krav, inkludert personvern er gjennomført på flere områder (ISMS / PIMS).
Med dagens dokumentasjon som er noe spredt i styringssystemet, bør vurderes om ovennevnte samsvarsvurdering kan settes i eget dokument, som viser når de er gjennomgått, av hvem og godkjent av CEO.

Framvist dokumentert informasjon

Dokumentert informasjon vedlagt:

Omfanget til ledelsessystemet:

FAR-Konteksten for organisationen-05092

Mål (6.2); Ledelsens gjennomgåelse (9.3):

FAR-Management review H1 2023-0509

ISO 27001:2017; siste versjon av SoA, og redegjørelse for risikovurderinger av informasjonssikkerhet

SoA versjon: 27/05/2023

SOA27701.pdf

SOA27001.pdf

Baseline for risikoanalyse er etablert. Støre risikoer blir flyttet opp i Jira for videre oppfølging i Security Board. Security Board gjennomfører møter hver mnd.

Førrevisjonsrapport; Rapport fra internrevisjon; Rapport fra ledelsens gjennomgåelse:

FAR-IA.00 Årshjul over audits og sikkerh

FAR-Interne revision-050923-132

rapport-f-rrevisjon.docx

Annen framvist dokumentert informasjon:

ISMS Confluence
Ledelsens gjennomgåelse
Diverse intern revisjoner
Riskoanalyser
Databehandleravtaler
Kontekst dokument
Microsoft Azure
HubSpot
Jira
Årshjul, inkludert intern revisjons plan
Jump Cloud
Kompetanse matrise
Farpay Scrumboard
Tickets
Disaster recovery plan

Deltakere

Navn	Tittel	Åpnings-møte	Intervju	Slutt-møte
Claus Thomsen	CISO	XL	XL	XL
Andre deltakere under revisjonen: SCAN0322.PDF				

L = Virksomhetens ledsager under revisjonen