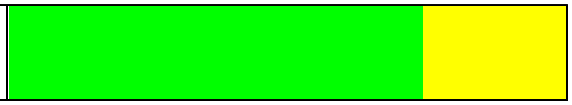
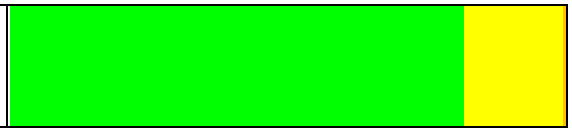
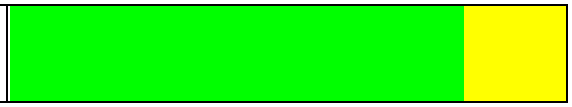
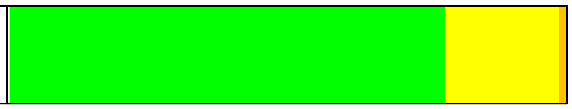
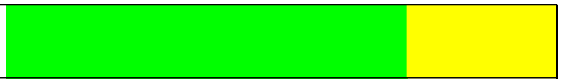
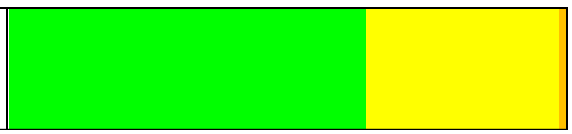
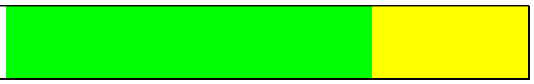
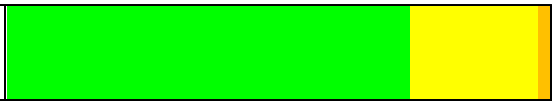
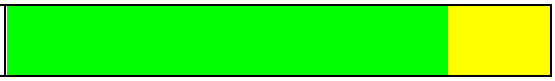
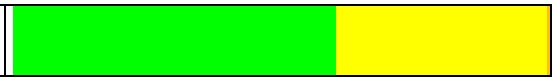
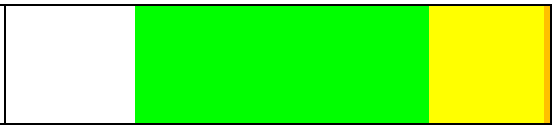
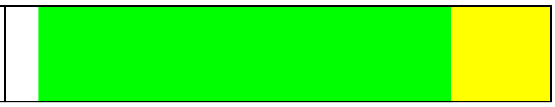
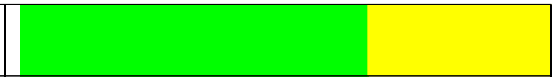
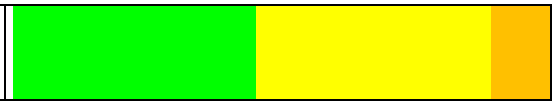
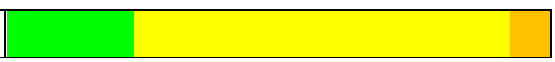
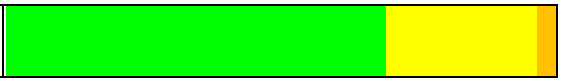
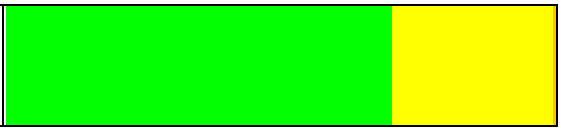
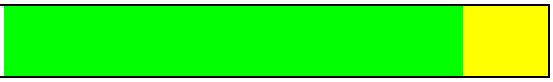
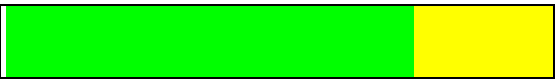
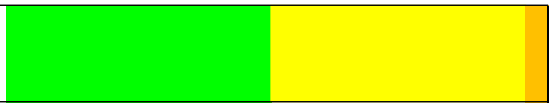
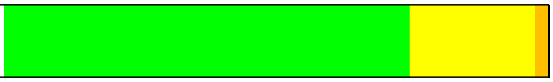
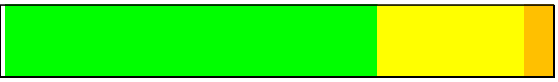
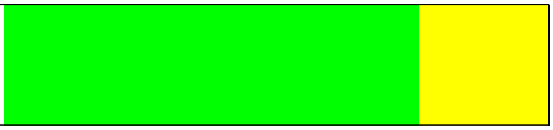
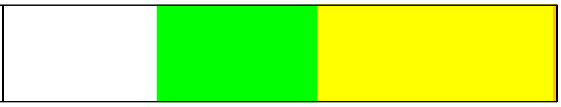
Blank=I/A, grønn=lav risiko, gult=middels risiko, orange=høy risiko, rødt=svært høy risiko Trend

Styring og kontroll	Gjennomganger vi gjør viser at IKT-systemene gir et godt grunnlag for bl.a. - styring av virksomheten, - kontroll med kundeengasjement, og - intern rapportering og rapportering til myndigheter.		→
Styring og kontroll	Vi har dokumenterte mål når det gjelder IKT-sikkerhet og vi har dokumenterte sikkerhetsprosedyrer. Mål og prosedyrer er godkjent av ledelsen og gjennomgås regelmessig.		↘
Styring og kontroll	Vi etterlever prinsippet om de tre forsvarslinjer, eller alternativt en intern modell for risikostyring og kontroll innenfor IKT-området.		↘
Styring og kontroll	Vi benytter anerkjente standarder innenfor IKT-sikkerhet.		→
Styring og kontroll	Vi har retningslinjer som sikrer at kontrollopplegget for IKT- og sikkerhetsrisiko (ICT Risk Management Framework) a) gjennomås årlig og ved alvorlig hendelser, og b) kontrolleres regelmessig av uavhengige og kvalifiserte personer		↘
Styring og kontroll	Vi har ikke etterslep når det gjelder retting av funn som er gjort ved gjennomganger av IKT-virksomheten.		↘
Styring og kontroll	Vi har en godt innarbeidet prosess for risikoanalyse. Ansatte er kjent med prosessen og bidrar aktivt og løpende inn i den.		↘
Styring og kontroll	Informasjon som grunnlag for å vurdere risiko samler vi inn systematisk og løpende. Informasjonen kan være analyser av avvik og hendelser, informasjon fra eksterne kilder, resultat av penetrasjonstesting, observasjoner fra kunder og ansatte.		→
Styring og kontroll	IKT-ledelsen rapporterer årlig resultatene fra risikovurderingen , inkludert identifiserte funn og anbefalte tiltak, til ledelsen.		↘
Styring og kontroll	Vi har oversikt over virksomhetskritisk IKT-utstyr og programvare, inklusive lisenser. Vi har oversikt over gyldig konfigurasjon av tekniske løsninger.		↘
Styring og kontroll	Vi har en prosess for utvikling og forbedring av a) rutinene for IKT-virksomheten, og b) kontrollmekanismene som skal sikre at rutinene etterleves.		↘
Styring og kontroll	IKT-tjenesteavtalene som støtter kritiske eller viktige funksjoner sikrer rett til innsyn, revisjon og tilsyn av alle forhold som gjelder leveransen.		↘
Styring og kontroll	Vi har god bestillerkompetanse, juridisk, teknisk og faglig.		↘
Styring og kontroll	Vi følger opp våre leverandører og leveransene løpende med hensyn på leveransekvalitet (KPI), feilretting og avtalte forbedringer.		↘
Styring og kontroll	Vi har en oversikt som viser kontroller som utøves av hhv. førstelinje, risikostyring og etterlevelsesfunksjonen, og internrevisjonen (evt. annen organisering), brutt ned på kontroller som bidrar til å sikre integritet, konfidensialitet og tilgjengelighet når det gjelder systemer og data. Oversikten viser hvem som er ansvarlig for å gjennomføre kontrollene.		↘
Styring og kontroll	Vi gjør detaljert risikovurdering av betalingstjenestevirksomheten. Vi har på plass tiltak for å beskytte brukerne av betalingstjenestene mot risikoene som er identifisert, inkludert svindel og ulovlig bruk av sensitive data og personopplysninger.		→
Styring og kontroll	Vi vedlikeholder kontaktinformasjon for brukerne av tjenesten vår, og kan raskt kontakte disse ved mistanke om feil, eller dersom vi har mistanke om svindel.		→
Styring og kontroll	Ansatte har stillingsbeskrivelser. Stillingsbeskrivelsene definerer tydelig roller, ansvar og kompetansekrav.		↘
Styring og kontroll	Vi har et godt program for regelmessig bevisstgjøring og opplæring av medarbeidere når det gjelder sikkerhet.		→

Blank=I/A, grønn=lav risiko, gult=middels risiko, orange=høy risiko, rødt=svært høy risiko

			Trend
Integritet	Vi benytter så langt som mulig kontroller som bidrar til at systemene våre ikke blir utsatt for uautoriserte endringer og at tjenestene våre fungerer slik de skal. Kontrollene kan være versjonsstyring, signering av kode, arbeidsdeling ("fire øyne-prinsippet"), sjekksummer, sekvenskontroller mv.		↘
Integritet	Vi har kontroller som sikrer data under transport og data som lagres. Kontrollene kan være sjekksummer, kryptering, signering, tilgangskontroller, rutiner for gjenskaping (inkrementell backup).		→
Integritet	Logger er beskyttet mot endring og sletting. Det er knyttet et tidspunkt til alt som registreres i loggen. Alle klokker som brukes for å registrere tidspunkter er synkronisert.		→
Integritet	Vi opplever ikke feil i applikasjoner og data som påvirker dataenes integritet (eks. doble posteringer, overskriving av data om kunden).		↘
Integritet	Vi samler inn informasjon om drift, transaksjoner og svindel, og benytter informasjonen til å gjøre tjenestene sikrere og mer stabil.		→
Integritet	Vi vurderer fortløpende tiltak for å beskytte kunden, som for eksempel 1) mulighet for å slå av funksjoner i betalingstjenesten (f.eks. regionsperre, internettsperre), 2) varsling (SMS, e-post) når det skjer bevegelser på konto eller kort, samt ved avviste tilgangsforsøk 3) kontinuerlig antisvindel-overvåking og 4) enkel og god tilgang til kundestøtte.		→
Integritet	Når nye løsninger skal utvikles, tar vi i betraktning behovene til alle forretningsområdene. Dette for å unngå utfordringer med "silo-løsninger", som omfattende vedlikehold av programmer, komplisert drift og utfordringer med synkronisering av data.		→
Integritet	Vi tillater ikke at ansatte på forretningssiden eller som arbeider med rapportering, utvikler egne applikasjoner (eksempler: Excel, MS Access, Pyton) som benyttes i våre tjenester eller i vår rapportering til myndigheter.		→
Endrings-håndtering	Vi har gode rutiner for endringshåndtering og etterlevelse av rutinene.		↘
Endrings-håndtering	Vi har ikke gjort endringer der gjeldende endringsrutinener ikke er blitt fulgt.		↘
Endrings-håndtering	Vi har få endringer som fører til uønskede hendelser.		↘
Endrings-håndtering	Test-systemene er "produksjonslike", dvs. at testdata (anonymiserte), applikasjoner, programvare, styresystemer og maskinvare er de samme i test som i produksjon.		→
Endringshåndtering	Vi gjør endringer i infrastrukturen ("ikke-funksjonelle" endringer) når det er lite kundeaktivitet, og kan reversere endringene og rulle tilbake på kort tid om nødvendig.		→
Endrings-håndtering	Før produksjonssetting utføres det sikkerhetstesting. Testingen gjøres av personer som ikke har vært involvert i utviklingen av tjenesten som testes.		↘
Endringshåndtering	Før produksjonssetting gjennomføres det uavhengig gjennomgang av koden.		↘
Endrings-håndtering	Prinsippet om arbeidsdeling opprettholdes under hele endringsprosessen, dvs. at forskjellige personer er ansvarlig for utvikling, test, godkjenning og produksjonssetting.		↘
Endrings-håndtering	Det er lav grad av kompleksitet i IKT-systemene. Det er etablert klare ansvarsområder som gir god oversikt. Endringer håndteres på en måte som sikrer kontroll og forutsigbarhet, slik at eventuelle konsekvenser for andre systemer blir vurdert og ivaretatt.		↘
Endrings-håndtering	Endringer i IKT-sikkerhetskontroller (Eks.: brannmurregler) blir godkjent av IKT-sikkerhet før endringen iverksettes.		→
Endrings-håndtering	Nye regulatoriske krav gjør at vi stadig må endre systemene våre.		↗

Blank=I/A, grønn=lav risiko, gult=middels risiko, orange=høy risiko, rødt=svært høy risiko Trend

Drift	Vi har i løpet av siste 12 måneder gjort risikoanalyse, identifisert områder med høy risiko for nedetid (for eksempel Single Point of Failure), og satt i verk tiltak for å sikre kontinuerlig drift.		↘
Drift	Vi har oversikt over forretningsprossene og IKT-systemene som støtter hver forretningsprosess. Vi vurderer konsekvensene for forretningsprosessen (BIA) som følge av avvik eller stopp i IKT-systemene. På bakgrunn av oversikten setter vi mål for maksimal tid for reetablering av normal drift (RTO) og maksimalt datatap (RPO).		↘
Drift	Vi gjennomgår regelmessig planer, prosesser og prosedyrer for kontinuitet og reetablering av IKT-systemer som støtter kritiske og viktige tjenester.		↘
Drift	Vi anvender anerkjente retningslinjer når det gjelder bruk av leverandører av IKT-tjenester, som for eksempel EBA Guidelines on outsourcing arrangements.		→
Drift	Våre retningslinjer for bruk av leverandører av IKT-tjenester definerer roller og ansvar, så vel som kompetanse som kreves for å overvåke og håndtere risiko forbundet med de utkontrakterte tjenestene.		↘
Drift	Samarbeidsrutinene og ansvarsforholdet mellom oss og leverandører av IKT-tjenester er detaljerte og presise.		↘
Drift	Vi holder informasjonsregisteret (RoI) oppdatert (se (EU) 2024/2956) og har oppdaterte risikovurderinger av IKT-tjenestekjøp. Andre og tredje forsvarslinje har tilstrekkelig kompetanse og ressurser, og følger opp IKT-tjenesteavtalene og leverandørene regelmessig.		↘
Drift	Kontraktene med leverandører av IKT-tjenester som støtter kritiske eller viktige funksjoner regulerer støtten leverandøren skal gi i en situasjon der vi ønsker å bytte leverandør eller gå over til å benytte egne systemer.		↘
Drift	Vi har gode tiltak for å avdekke avvik (unormal belastning, unormal bruk av porter / protokoller, avvikende svarstider, sikkerhetshendelser) i datatrafikken og ta aksjon før skade inntreffer.		↘
Drift	Vi har oppdaterte rutiner for å håndtere hendelser, herunder cyberhendelser. Rutinene inkluderer regler for eskalering og rapportering.		↘
Drift	Vi tester kontinuitetsplanene og gjenoprettingsplanene for IKT for alle systemer årlig, og ved betydelig endringer i IKT-systemer som støtter kritiske eller viktige funksjoner.		↘
Drift	Vi overvåker "tikkende bomber", dvs. komponenter som gradvis slites, og verdier som gradvis når nivåer som krever inngrep, for eksempel minnelekkasje, sertifikater som går ut på dato, elektroniske komponenter som slites, energiforsyning som slites (batterier, brennstoff til nødstrøm-aggregat), CPU-utnyttelse, RAM, disk.		↘
Drift	Vi har lite "teknisk gjeld", noe som reduserer risikoen når det gjelder utvikling og drift.		↘
Drift	Nedetid i IKT-systemene som påvirker forretningsdriften negativt opplever vi mindre og mindre av.		↘
Drift	Rettigheter til å administrere systemer og data ("admin-rettigheter") tildeles der det er tjenestlig behov.		↘
Drift	Grensesnittene som tredjeparter benytter for å få tilgang til betalingskontoer er testet og godkjent i samarbeid med tredjepartene. Feil som oppstår i grensesnittene rettes med samme prioritet som feil i våre egne løsninger.		→
Drift	Grensesnittene som tredjeparter benytter er sikret i samsvar med regelverket.		→

Blank=I/A, grønn=lav risiko, gult=middels risiko, orange=høy risiko, rødt=svært høy risiko

		Trend
Sikkerhet	Vi har på plass tiltak for å sikre oss mot angrep (advanced persistence threat, trojanere, ransomware, DDoS, e-post-angrep). Eksempler på tiltak: Intrusion Detection og Intrusion Prevention, brannmur, antivirus, kontroll av web-trafikk, sikring av e-post, sikkerhetsoppdatering, sandboxing.	→
Sikkerhet	Vi har etablert program for testing av vår digitale motstandsdyktighet. For systemer og applikasjoner som støtter kritiske eller viktige funskjoner, tester vi den digitale motstandsdyktigheten minimum årlig.	↘
Sikkerhet	Vi gjør sårbarhetsscanning av IKT-sytstemer som støtter kritiske og viktig funksjoner ukentlig.	↘
Sikkerhet	Vi sjekker at sikkerhetskontrollene er hensiktsmessige og fungerer slik de skal - årlig for kritiske systemer og minst hvert 3. år for ikke-kritiske systemer.	→
Sikkerhet	Vi har gode rutiner når det gjelder sikkerhetsoppdateringer.	↘
Sikkerhet	Vi har kontroll på: - hvem som har tilgang til våre data og systemer (både internt og hos leverandører) - hvilke data og systemer brukeren har tilgang til - hvorfor brukeren har tilgang - dato for fornyet vurdering og identitetskontroll av brukeren.	↘
Sikkerhet	Personell har personlig logon-ID. Det er ingen "fellesbrukere".	→
Sikkerhet	Innlogging som programmerte prosesser gjør mot systemer og data er låst til prosessen slik at personell ikke kan bruke innloggingsdetaljene for å logge seg inn.	↘
Sikkerhet	Vi har god tilgang til IKT-sikkerhetskompetanse, herunder kompetanse til å stille krav til leverandører og følge opp leveransen.	→
Sikkerhet	Vi følger anerkjente standarder som kan bidra til kvalitet og sikkerhet i programkoden (for eksempel OWASP).	↘
Sikkerhet	Vi fjerner løpende programvare som vi ikke lenger bruker, og programvare som ikke lenger støttes av leverandøren.	↘
Sikkerhet	All fjernaksess til våre systemer skjer ved bruk av VPN og tofaktorautentisering.	→
Beskyttelse av data	Vi har gode retningslinjer for klassifisering og beskyttelse av både strukturert (databaser) og ustrukturert (Word, e-post, personlige filområder) informasjon.	↘
Beskyttelse av data	Vi har gode rutiner for tildeling, vedlikehold og kontroll av rettigheter som ansatte, leverandører, konsulenter og applikasjoner har i systemene våre.	→
Beskyttelse av data	Vi logger tilgang til data og systemer. Dersom det forkommer uautorisert tilgang eller forsøk på tilgang, går det et varsel som umiddelbart blir fulgt opp. Vi har kontroller som vil varsle dersom loggingen ikke lenger virker.	→
Beskyttelse av data	Vi har inndelt nettverket i sikkerhetssoner basert på en sikkerhetsgradering av data og systemer. Graderingen bestemmer nivået når det gjelder fysisk og logisk (tilgangskontroller, kryptering mv.) sikring av data og funksjoner i sonen. Sone for lagring av sikkerhetskopier inngår i vurderingene.	↘
Beskyttelse av data	Vi krypterer all data på bærbart utstyr.	→
Beskyttelse av data	Ved terminering av avtaler om datalagring må leverandøren dokumentere at data er fullstendig slettet.	→
Beskyttelse av data	Vi har rutiner for sikker lagring og overvåking av sensitiv betalingsinformasjon (informasjon som kan misbrukes til å begå svindel, for eksempel kortdetaljer og påloggingsinformasjon), samt kontroller når det gjelder lagring og tilgang til denne informasjonen.	→

Blank=I/A, grønn=lav risiko, gult=middels risiko, orange=høy risiko, rødt=svært høy risiko

		Trend
ID-tyveri	Vi har gode tiltak for å forhindre at en angriper tar over en bruker-ID og misbruker denne.	→
ID-tyveri	Vi har gode tiltak for å forhindre at en angriper tar over en kunde-ID og misbruker denne.	↘
ID-tyveri	Vi krever sterk kundeautentisering i forbindelse med betalinger for handel på internett.	↗
ID-tyveri	Vi har god kontroll når det gjelder utlevering, bruk og sletting av autentiseringskjennetegn til kunder.	→
ID-tyveri	Vi benytter kontroller som forhindrer "skimming" og "Card not present"-svindel.	→
Interne misligheter	Vi har gjort en detaljert risikovurdering og definert mislighetsscenarioer.	→
Interne misligheter	Vi har etablert særskilt logging og varsling for situasjoner der risikovurderingen indikerer har det er høy sannsynlighet for misligheter. Dette kan for eksempel være tilbakevalutering, bevegelser på interne kontoer, bevegelse på passive kontoer, overføring fra kunde til ansatt og tilbake, ikke-tjenestlige oppslag på kundedata eller ansatte som er i en presset økonomisk situasjon.	↘
Interne misligheter	Vi benytter tjenestedeling ("fire øyne-prinsippet") så langt som mulig.	↘
Interne misligheter	Vi overvåker ansattes egenhandel.	→
IKT støtte AML/CTF	Våre IKT-systemer gir et samlet bilde av kunde, kunderelasjonen og kundeadferden.	↘
IKT støtte AML/CTF	Vi har elektronisk overvåking av transaksjoner og transaksjonsmønstre.	↘
IKT støtte AML/CTF	Vi har en stadig bedre presisjon når det gjelder flagging av mistenkelig forhold.	↘
IKT støtte AML/CTF	Transaksjonsovervåkingssystemet fanger opp alle mistenkelig betalingstransaksjoner.	↘
IKT støtte AML/CTF	AML-systemene benytter i utstrakt grad data fra øvrige systemer.	↘
IKT støtte AML/CTF	Med tiden «lærer» AML-systemene våre gradvis å gjenkjenne mistenkelige pengebevegelser.	↘
IKT støtte AML/CTF	Sanksjonscreeningsystemet har høy presisjon i treff av listeførte personer og foretak.	↘