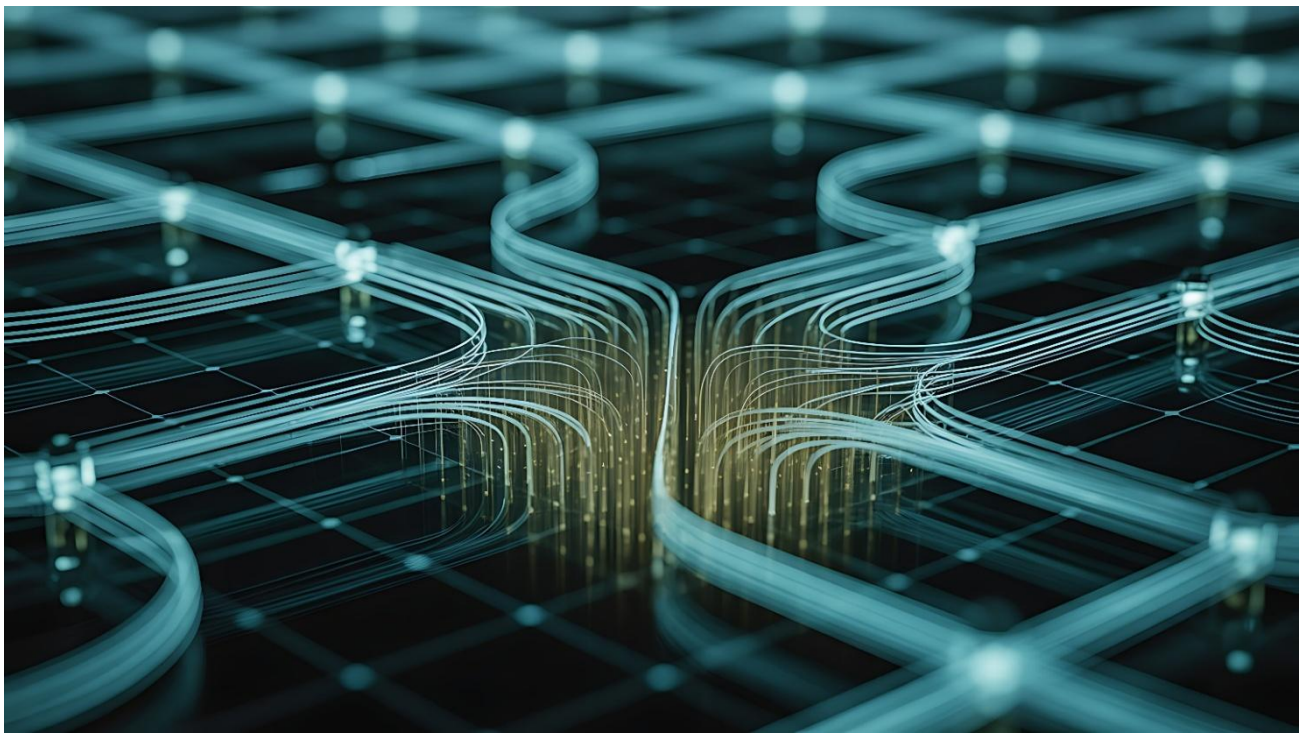
VEIKART FOR EN KVANTESIKKER FINANSNÆRING



Finans Norge

2026

Forord

Utviklingen innen kvanteteknologi representerer både nye muligheter og nye risikodimensjoner for finansnæringen. Dette veikartet er utarbeidet som en del av en arbeidsstrøm som sprang ut av prosjektet *«Fra uro til innsikt»,* etablert i mars 2026. Prosjektet har hatt som mål å bidra til økt forståelse av hvordan geopolitiske utviklingstrekk, teknologiske skifter og fremvoksende risikoer påvirker finansnæringens samlede motstandskraft. I dette arbeidet har ny teknologi, som kvanteteknologi, blitt analysert ikke bare som en mulighet, men også som en kilde til langsiktig og strukturell risiko.

Arbeidet med veikartet kan sees som en gradvis kunnskapsreise. I den innledende fasen, og underveis, har vi hatt godt faglig utbytte av samtaler med personer med kompetanse fra Universitet i Oslo, NTNU, Simula/UiB, NSM, NHO, NFCERT, BITS og medlemsbedrifter. Her vil vi spesielt trekke frem DNB, Sparebank 1, Nordea, Gjensidige, KLP og Storebrand.

Veikartet bygger på anerkjente internasjonale standarder og rammeverk, og er utformet for å være konsistent med gjeldende og fremvoksende krav til digital operasjonell robusthet. Finans Norge følger utviklingen tett, og det vil komme felles oppfølgingsaktiviteter i kjølvannet av dette veikartet.

Formålet med veikartet er å gi norsk finansnæring et felles, strukturert og risikobasert utgangspunkt for arbeidet med overgang til kvantesikkerhet. Det er ment som et veiledende styrings- og modenhetsverktøy, ikke som en teknisk spesifikasjon eller et bindende kravdokument. Ambisjonen er å støtte tidlig handling, fremme samhandling i økosystemet og bidra til å bygge varig kryptografisk smidighet i næringen.

Avslutningsvis vil Finans Norge rette en stor takk til alle som har bidratt med kunnskap, refleksjoner og innspill underveis i prosessen. Deres bidrag har vært avgjørende for å utvikle et veikart som er faglig forankret, praktisk anvendbart og relevant for finansnæringens langsiktige arbeid med digital robusthet.

Pål Christian Waag

Finans Norge, fagdirektør cybersikkerhet

24.03.2026

Innhold

Sammendrag

Utviklingen innen kvanteteknologi representerer både betydelige muligheter og en alvorlig, langsiktig risiko for finansnæringen. Når kvantedatamaskiner blir tilstrekkelig kraftige, vil de kunne svekke eller bryte kryptografiske mekanismer som i dag beskytter finansiell kommunikasjon, identitet, transaksjoner og lagrede data. Internasjonale fagmiljøer og myndigheter er samstemte. Overgangen til kvantesikker kryptografi må planlegges og igangsettes tidlig, fordi den er kompleks, tidkrevende og berører hele den digitale verdikjeden.

Selv om det fortsatt er usikkert når kvantedatamaskiner vil være kryptografisk relevante, er risikoen allerede til stede gjennom harvest now, decrypt later-scenarier (HNDL). I slike scenarioer kan angripere samle inn krypterte data i dag, for senere å dekryptere dem når teknologien tillater det. Trusselen er derfor ikke primært knyttet til tidspunktet for et teknologisk gjennombrudd, men til dataens levetid. For finansnæringen, der mye informasjon må forbli konfidensiell i tiår eller permanent, innebærer dette at risikoen bygges opp nå.

Den mest praktiske og skalerbare måten å møte denne risikoen på i dag er overgang til post-kvante-kryptografi (PQC). PQC omfatter kryptografiske algoritmer som er utviklet for å være robuste mot både klassiske og kvantebaserte angrep, og kan implementeres på eksisterende infrastruktur. Overgangen til PQC er imidlertid ikke et enkelt algoritmebytte, men en flerårig transformasjon som krever helhetlig styring, prioritering og koordinering på tvers av virksomheter, infrastrukturer og leverandører.

Dette veikartet er utarbeidet for å gi norsk finansnæring et felles, strukturert og standardbasert rammeverk for denne overgangen. Det bygger på internasjonalt anerkjente rammeverk og anbefalinger, og legger særlig vekt på tre gjennomgående prinsipper: tidlig handling basert på risikovurdering, utvikling av kryptografisk smidighet som en varig organisatorisk evne, og tett samhandling i økosystemet mellom finansforetak, felles infrastrukturer, leverandører og myndigheter.

Veikartet er ment som et styrings- og modenhetsverktøy, ikke som en teknisk standard og ikke som et bindende krav. Samtidig er det utformet slik at det støtter opp under gjeldende rammer for digital operasjonell motstandskraft i finanssektoren, herunder forordningen om digital operasjonell robusthet (DORA). DORA etablerer et felles rammeverk for håndtering av IKT-risiko. Kvantesikkerhet og overgang til PQC faller naturlig inn i dette helhetlige styringsbildet, som en del av arbeidet med å sikre langsiktig digital robusthet.

Veikartet gir en felles retning for hvordan norsk finansnæring kan starte arbeidet tidlig, prioritere der risikoen er størst, og bygge evne til kontrollert og smidig overgang over tid. Målet er ikke å gjøre alt på én gang, men å etablere oversikt, struktur og gjennomføringskraft.

1 Formål, mandat og avgrensning

1.1 Formål

Formålet med veikartet er å støtte norsk finansnæring i å forstå, planlegge og gjennomføre overgangen til kvantesikkerhet på en koordinert og risikobasert måte. Veikartet skal bidra til at finansnæringen kan etablere en felles situasjonsforståelse av kvantetrusselens betydning. Det skal også bidra som hjelp til å prioritere tiltak basert på kritikalitet, data-beskyttelseshorisont og økosystemavhengigheter. Avslutningsvis vi det også kunne være en rettesnor for å utvikle varig kryptografisk smidighet (agilitet), slik at kryptografi kan oppdateres og byttes ut uten uforholdsmessige kostnader og driftsforstyrrelser.

1.2 Mandat og målgruppe

Veikartet er utformet som et veiledende dokument for:

- finansforetak
- finansielle markedsinfrastrukturer
- leverandører av kritiske IKT tjenester til finanssektoren
- samt relevante myndigheter og tilsyn dersom det sees som relevant

Det fastsetter ikke bindende krav og erstatter ikke gjeldende regelverk, standarder eller tilsynspraksis. Det gir et felles utgangspunkt for planlegging, dialog og koordinering.

1.3 Forholdet til regulering og DORA

Veikartet er utformet for å være konsistent med rammer for digital operasjonell motstandskraft i finanssektoren. DORA etablerer et felles rammeverk for digital operasjonell robusthet, og omfatter blant annet krav knyttet til IKT risikostyring, hendelseshåndtering og rapportering, operasjonell testing, styring av IKT tredjepartsrisiko og informasjonsdeling.
Veikartet posisjonerer kvantesikkerhet som en sentral del av dette arbeidet. Overgangen til post kvante kryptografi er i praksis en langsiktig transformasjon av kritiske sikkerhetsmekanismer som understøtter finanssektorens IKT tjenester og forretningsprosesser. Det faller derfor naturlig inn i det helhetlige styringsbildet for IKT risiko og operasjonell robusthet.

1.3.1 Quantum Key Distribution (QKD)

I et perspektiv for å beskytte informasjon og data mot kvanteteknologien dukker også QKD opp som konsept. Quantum Key Distribution (QKD) er en teknologi for nøkkeldistribusjon og ikke for krypteringen i seg selv. QKD benytter kvantemekaniske egenskaper ved lys for å etablere en delt og hemmelig symmetrisk nøkkel mellom to endepunkter. Den sentrale egenskapen ved dette er at en eventuell avlytting vil kunne detekteres og sikkerheten er uavhengig av angriperens regnekraft. Det innebærer at sikkerheten hviler på fysikkens lover og ikke på matematiske antakelser.

Men QKD erstatter på ingen måte autentisering, digitale signaturer, sertifikater eller protokoller som TLS[1]. QKD leverer kun nøkler, og derfor må resten av sikkerhetsarkitekturen fortsatt fungere. Man kan gjerne si at PQC dekker hele spekteret av kryptografiske behov, mens QKD kun adresserer en avgrenset del av kryptokjeden. Forskning og pilotprosjekter viser også at QKD kan være krevende og drifte og gir liten fleksibilitet, mens PQC kan implementeres fasevis og kombineres med dagens kryptografi.

Både NIS[2], NSA[3], ENISA[4] og europeiske tilsynsmyndigheter peker på at PQC bør være primærstrategi, ikke QKD. BIS[5] har laget denne fremstillingen for å vise fordeler og ulemper med QKD og PQC:

PQC - Post Quantum Cryptography	**QKD – Quantum Key Distribution**
Fordeler	Fordeler
- Etablerte standarder - Kompatibel med dagens infrastruktur - Skalerbar - Flere alternativer	- Sikkerhet basert på kvantemekanikk - Motstandsdyktig mot kryptoanalyse - Langsiktig
Ulemper	Ulemper
- Krever utstrakt testing - Potensielt sårbar for kvanteangrep - Ytelseshensyn må tas	- Umoden teknologi - Kostbart - Krever fiberteknologi - Utfordringen med integreringer - Kan ikke erstatte autentisering

Basert på denne sammenligningen, europeiske tilsynsmyndigheter og autorative råd vil dette veikartet basere seg på PQC i den videre anbefalingen.

[1] TLS – Transport Layer Security – Utbredt kryptografisk protokoll som brukes for å sikre kommunikasjon over et datanettverk. Sørger for konfidensialitet, integritet og autentisitet mellom klient og en server.
[2] A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryprography (digital-strategy.ec.europa.eu)
[3] Post-Quantum Cryptography: CISA, NIST and NSA Recommend How to Prepare Now (nsa.gov)
[4] Post-Quantum Cryptography: Current state and quantum mitigation (enisa.europa.eu)
[5] Quantum-readiness for the financial system: a roadmap (bis.org)

2 Kvantetrusselen

Store deler av dagens digitale motstandskraft hviler på kryptografiske algoritmer som benyttes til å sikre konfidensialitet (kryptering av data), autentisering (digitale signaturer) og nøkkelutveksling (TLS i nettbank, betalinger og API-er[6]). Dette gjelder særlig asymmetrisk kryptografi som RSA[7]og ECC[8]. Disse algoritmene er selve grunnmuren i å sikre nettforbindelser, identitets- og tilgangsstyring, digitale sertifikater og betalinger/meldingsutvekslinger i finanssektoren.

Algoritmene er sikre fordi de bygger på matematiske problemer som er uløselige med klassiske datamaskiner, innenfor rimelig tid. Men med kvantedatamaskiner vil dette endre seg. Kvantedatamaskiner utnytter egenskaper fra kvantefysikken som superposisjon. Dette gjør at bestemte typer problemer kan løses langt mer effektivt enn klassiske datamaskiner er i stand til. Shors algoritme[9] og Grovers algoritme[10] løser logaritmiske problemer mer effektivt og konsekvensen er at asymmetrisk kryptografi i praksis står ovenfor et strukturelt sammenbrudd. Det handler ikke om dårlig implementering, men at de matematiske forutsetningene er endret. Kvantedatamaskiner som er i stand til å bryte RSA og ECC er imidlertid ikke operasjonelle enda.

Det er viktig å merke seg at trusselen ikke knyttet til tidspunktet for gjennombruddet, men til dataens beskyttelseshorisont.

Mye informasjon og data i finanssektoren har lang beskyttelseshorisont og vil være konfidensiell i 10-30 år, eller i praksis permanent. Dermed må slik informasjon beskyttes i dag, slik at den ikke kan utnyttes innenfor det tidsrommet. Med dette perspektivet oppstår trusselen om Harvest Now – Decrypt Later (HNDL[11]). Angriperen er muligens ikke i stand til å dekryptere dataene i dag, men de er i stand til å samle den for å kunne dekryptere den og utnytte den på et senere tidspunkt. Med andre ord flytter den reelle verdien seg inn i fremtiden. Eksempelvis vil vi kunne oppleve en fremtidig forfalskning av signaturer, kompromittering av identiteter og tillitskjeder i det finansielle systemene. Det kan være vanskelig å oppdage slike datatyveri fordi det ikke oppstår noen umiddelbar skade. En angriper kan også utnytte faktoren tid til sin fordel slik at sporbarheten blir minimal.

Relevante aktører i dette landskapet er statlige etterretningstjenester og nasjonale sikkerhetsorganisasjoner som har langsiktige og strategiske mål, kapasitet til å samle og lagre enorme datamengder og analysekapasitet. Men det kan også være statssponsede organiserte kriminelle som jobber på vegne av stat og industri. Ved å lese rapportene fra norske EOS-tjenestene er det naturlig å

[6] API – (Application Programming Interface) Programmeringsgrensesnitt)
[7] RSA er en asymmetrisk krypteringsmetode, oppkalt etter Rivest, Shamir og Adleman
[8] Elliptiske kurver
[9] Shors algoritme: Kvantealgoritme som kan brukes for å faktorisere store tall (quantum.cloud.ibm.com)
[10] Grovers algoritme: kvantealgoritme som akselererer søk i en usortert datamengde ved å forsterke sannsynligheten for den riktige løsningen (quantum.cloud.ibm.com)
[11] Quantum computing and the financial system: opportunities and risks (bis.org)

tenke seg hvem som er aktørene i slike scenarioer. Det finnes også dokumenterte tilfeller av omdirigering og tapping av internettrafikk på et nasjonalt nivå.

Akademiske studier og myndighetsanalyser peker på at følgende data er særlig utsatt og må beskyttes:

- Finansielle transaksjoner[12]
- Identitetsdata og autentiseringslogger[13]
- Juridiske avtaler og kontrakter[14]
- Sensitive meldinger mellom finansinstitusjoner[15]
- Regulatorisk rapportering og tilsynsdokumentasjon[16]

Slik informasjon er relevant fordi den kan ha en strategisk og etterretningsmessig verdi og kan brukes til økonomisk press, påvirkning eller innsikt på et senere tidspunkt.

[12] Quantum-readiness for the financial system: a roadmap (bis.org)
[13] NIST Releases Post-Quantum Encryption Standards (quantum.gov)
[14] "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privact RIsks for Distributed Ledger Networks (feredalreserve.gov)
[15] Quantum-readiness for the financial system: a roadmap (bis.org)
[16] Cryptographic Products Market Analysis (enisa.europa.eu)

3 Overordnede prinsipper

Internasjonale rammeverk peker på at kvantesikkerhet må bygges på tydelige, anvendelige prinsipper som kan skaleres og brukes på tvers av aktører. Følgende prinsipper legges til grunn i dette veikartet:

3.1 Tidlig handling og langsiktig perspektiv

Overgangen til post-kvantesikker kryptografi (PQC) handler ikke om å reagere på et akutt teknologisk gjennombrudd, men om å håndtere en langsiktig og strukturell endring i forutsetningene for digital sikkerhet. Nettopp derfor er det avgjørende å komme i gang tidlig. Tiltakene må forankres i et perspektiv som strekker seg langt utover dagens systemer og teknologivalg.

En sentral forskjell mellom kvantetrusselen og tidligere teknologiske skifter er at konsekvensene av å vente kan være irreversible. Data som krypteres i dag, men samles inn av en motstander, kan dekrypteres i fremtiden dersom beskyttelsen bygger på kryptografi som senere viser seg å være sårbar. Når dette først skjer, finnes det ingen tekniske tiltak i ettertid som kan gjenopprette konfidensialiteten. Risikoen etableres altså nå, men materialiserer seg senere. Dette gjør at tidlig overgang til PQC først og fremst handler om å bryte denne tidsforskyvningen i angriperens favør. Ved å ta i bruk kvantesikre algoritmer i nøkkelutveksling og autentisering reduseres verdien av data som eventuelt samles inn i dag. Dataene kan fortsatt bli stjålet, men de mister sin fremtidige strategiske verdi.

Det er viktig å erkjenne at PQC ikke er en "engangsoppgradering". Det vil ta tid å bytte kryptografiske mekanismer berører derfor hele den digitale grunnmuren i organisasjonen. Dette er grunnen til at et langsiktig perspektiv er like viktig som tidlig oppstart. En forhastet eller fragmentert innføring av PQC kan i verste fall gi falsk trygghet eller nye sårbarheter. Overgangen må derfor skje gradvis, kontrollert og med tydelig arkitekturforankring.

Et langsiktig perspektiv handler også om å erkjenne at PQC i seg selv ikke er slutten på utviklingen. Nye kryptografiske metoder vil komme, og noen vil bli forlatt. Derfor er et av de viktigste målene med å starte tidlig ikke bare å bytte algoritmer, men å bygge kryptografisk smidighet.

Vi må komme i gang tidlig med PQC for å redusere en risiko som allerede bygges opp i dag, særlig knyttet til data med lang beskyttelseshorisont og høy verdi. Samtidig må vi tenke langsiktig, fordi overgangen berører fundamentale deler av den digitale infrastrukturen og må gjennomføres på en måte som er robust, styrbar og bærekraftig over tid. Overgangen til PQC innebærer betydelig kompleksitet og det krever derfor en tydelig prioritering, koordinering og systematisk gjennomføring.

3.2 Risikobasert og proposjonal tilnærming

Ikke all informasjon, ikke alle systemer og ikke alle forbindelser har samme verdi, samme trusselbilde eller samme konsekvens ved kompromittering. Å behandle dem likt vil enten føre til overbeskyttelse, med unødvendig kostnad og kompleksitet, eller manglende beskyttelse der risikoen faktisk er størst. I en kvantesikker kontekst betyr dette først og fremst å forstå hvilken informasjon som må forbli konfidensiell over lang tid, og hvilke systemer som er avhengige av kryptografi som senere kan bli sårbar.

En proporsjonal tilnærming innebærer å rette de mest omfattende og krevende tiltakene dit risikoen faktisk er høyest, og ikke der det er enklest å gjennomføre dem.

Dette perspektivet er særlig viktig fordi overgangen til PQC ikke bare handler om sikkerhet, men også om ytelse, stabilitet og kompleksitet. Kvantesikre algoritmer har andre egenskaper enn dagens løsninger, noe det må tas høyde for ved en migrasjon.

En risikobasert tilnærming er også avgjørende for å sikre god styring over tid. Kvantetrusselen utvikler seg gradvis, og kunnskapen om både teknologi og trusselaktører vil endre seg. For finanssektoren, som har en stor grad av kompleksitet og avhengigheter, har proporsjonalitet også en viktig systemdimensjon. Overdrevne eller ukoordinerte tiltak i én del av økosystemet kan få utilsiktede konsekvenser andre steder.

En risikobasert og proporsjonal tilnærming er derfor avgjørende i arbeidet med å skape en kvantesikker finansnæring.

3.3 Kryptografisk smidighet (agilitet) som kjernekapasitet

I en verden der kryptografiske forutsetninger endrer seg raskt, er kryptografi en grunnleggende forutsetning for sikker drift, tillit og regulatorisk etterlevelse av sektoren. Når kryptografiske algoritmer svekkes som følge av nye sårbarheter, regulatoriske krav eller teknologiske gjennombrudd som kvantedatamaskiner, må organisasjonen/virksomheten kunne reagere raskt uten å sette drift, tillit eller etterlevelse i fare. Uten kryptografisk smidighet kan nødvendige endringer bli langsomme, kostbare og forstyrrende for kjernevirksomheten. Virksomheter risikerer at kritiske systemer blir låst til foreldet kryptografi, som igjen kan føre til langvarige driftsavbrudd, forhastede nødløsninger og økt operasjonell risiko.

Modellen for kryptografisk smidighet gir et rammeverk for å håndtere denne risikoen[17]. Ved å etablere full oversikt over kryptografiske avhengigheter, planlegge endringer på forhånd og

[17] Building Cryptographic Agility In The Financial Sector (fsisac.com)

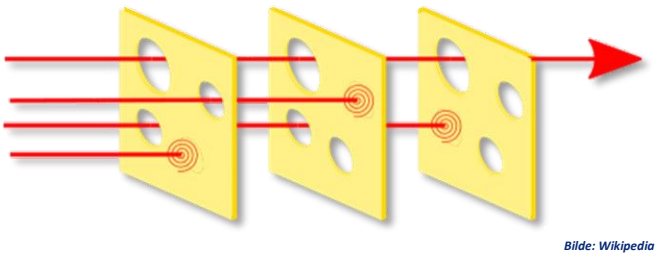
teste nye løsninger før de tas i bruk, kan organisasjonen gjennomføre nødvendige utskiftinger kontrollert og med minimal påvirkning på kjernevirksomheten. Dette gjør det mulig å opprettholde forretningskontinuitet selv når eksisterende kryptografi raskt må fases ut. Denne prosessen er ikke et engangsinitiativ, men illustrerer en varig organisatorisk evne til å tilpasse seg de raske kryptografiske endringene.

Når utskifting og verifikasjon av kryptografi er en innarbeidet prosess, reduseres avhengigheten av enkeltpersoner, spesialløsninger og krisehåndtering. Kryptografi blir i stedet en styrt, vedlikeholdt del av normal drift, på linje med andre kritiske infrastrukturtjenester. På den måten bidrar kryptografisk smidighet til operasjonell robusthet.
Gjennom kontinuerlig vedlikehold og regelmessig revurdering av kryptografiske valg kan virksomheten forbli motstandsdyktig over tid, også i møte med teknologiske skifter. Dette gjør kryptografisk smidighet til et strategisk virkemiddel for langsiktig sikker, stabil og effektiv drift.

3.4 Forsvar i dybden, pragmatisk overgang og kryptografisk smidighet

Overgangen til kvantesikker kryptografi skjer i møte med et trusselbilde preget av høy usikkerhet, lang tidshorisont og betydelig teknologisk kompleksitet. I en slik situasjon er det verken realistisk eller ønskelig å basere sikkerheten på én enkelt løsning, ett teknologisk sprang eller én antatt fremtid. Tvert imot gjør dette forsvar i dybden og en pragmatisk overgang til helt sentrale prinsipper.

Forsvar i dybden bygger på erkjennelsen av at ingen enkeltmekanisme gir full beskyttelse over tid. Kryptografiske algoritmer kan vise seg å ha svakheter, implementasjoner kan feile, og trusselaktører kan finne omveier rundt tekniske kontrolltiltak. Når konsekvensene er alvorlige, må sikkerheten derfor være sammensatt av flere, delvis overlappende lag, slik at svikt i ett ledd ikke umiddelbart fører til tap av kontroll.



Figur: Ostehullsteorien beskrevet av James Reason ved University of Manchester

I en kvantesikker kontekst betyr dette å erkjenne at PQC, selv om det er nødvendig og riktig, ikke alene er tilstrekkelig. Forsvar i dybden handler dermed ikke om å legge til kompleksitet for kompleksitetens skyld, men om å redusere avhengigheten av enkelttiltak enten de er teknologiske eller strategiske. Dette prinsippet henger tett sammen med behovet for en pragmatisk overgang. Kvantesikkerhet representerer ikke et klart brudd mellom “gammelt” og “nytt”, men en lang periode der ulike teknologier må sameksistere. Eksisterende systemer vil leve videre i mange år, samtidig som nye løsninger utvikles og tas i bruk. En pragmatisk tilnærming anerkjenner denne realiteten og søker å håndtere den på en kontrollert måte. Det handler også om å erkjenne at kvantesikkerhet ikke utvikler seg i et vakuum. Standarder, anbefalinger og beste praksis vil modnes over tid. Ved å gå stegvis frem, med rom for justering, reduseres risikoen for å låse seg til løsninger som senere viser seg å være suboptimale eller uegnede. Kryptografisk smidighet blir dermed også et nøkkelord i denne sammenheng.

Derfor er disse prinsippene avgjørende for at overgangen til kvantesikkerhet ikke bare skal bli teknisk korrekt, men også operasjonelt stabil, styrbar over tid og tillitsskapende for sektoren som helhet.

3.5 Samhandling og et økosystemperspektiv

Finansnæringens avhengigheter gjør at kvantesikkerhet må håndteres koordinert, både internt i det enkelte selskap og i næringen. G7 veikartet[18] er eksplisitt utformet for å støtte en harmonisert overgang på tvers av aktører, og fremhever også leverandør- og avhengighetsbildet.

Overgangen til kvantesikkerhet er ikke et isolert teknologiprosjekt som kan løses av enkeltvirksomheter hver for seg. Den berører felles digitale infrastrukturer, delte leverandørkjeder, standarder, tillitsmekanismer og regulatoriske rammer. Nettopp derfor er samhandling og et økosystemperspektiv en grunnleggende forutsetning for å lykkes.
Kryptografi er i sin natur relasjonell. Den virker i grensesnittet mellom aktører. Mellom kunde og bank, mellom banker, mellom finansnæringen og leverandører, og mellom privat og offentlig sektor. Når forutsetningene for kryptografisk sikkerhet endres, endres de derfor ikke bare for én aktør, men for hele samspillet mellom dem.

Et økosystemperspektiv tar utgangspunkt i denne gjensidige avhengigheten. Det erkjenner at sikkerheten i én virksomhet i stor grad påvirkes av modenheten i omgivelsene, både hos leverandører, samarbeidspartnere og fellesløsninger. I en kvantesikker kontekst betyr det at manglende fremdrift eller ukoordinerte valg ett sted kan skape risiko andre steder, selv om den enkelte virksomhet isolert sett gjør alt riktig.

Samhandling er derfor ikke først og fremst et spørsmål om effektivitet, men om risikoreduksjon og systemrobusthet. Dersom aktører beveger seg i ulik takt eller velger inkompatible løsninger, kan resultatet bli fragmentering, økt kompleksitet og i verste fall nye sårbarheter. En økosystemtilnærming søker i stedet å bygge retning, samspill og forutsigbarhet.

Samhandling er også avgjørende fordi kvantesikkerhet er et område preget av usikkerhet og umodenhet. Ingen enkeltaktør sitter med hele fasiten. Standarder, beste praksis og operative erfaringer utvikles nå. Samtidig er det viktig å understreke at samhandling ikke betyr ensretting. En velfungerende økosystemtilnærming gir rom for ulik modenhet, ulike forretningsmodeller og ulike risikoprofiler. Poenget er ikke at alle skal gjøre det samme til samme tid, men at utviklingen skjer innenfor felles rammer og en delt forståelse av målbildet.

3.6 Standardbasert tilnærming

Overgangen til kvantesikkerhet skjer i et landskap preget av teknologisk usikkerhet, lange tidshorisonter og komplekse avhengigheter mellom aktører, systemer og jurisdiksjoner. I en slik

[18] G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector (treasury.gov)

situasjon er det avgjørende å unngå løsninger som er skreddersydd for øyeblikket, enkeltleverandører eller særskilte teknologivalg. I stedet må overgangen forankres i en standardbasert tilnærming.

Standarder representerer felles, fremforhandlede svar på komplekse problemstillinger. De bygger på bred faglig vurdering, åpenhet og erfaring fra mange aktører, og er nettopp utviklet for å redusere risikoen for feilslutninger, fragmentering og teknologisk innlåsing. I møte med kvantetrusselen gir standarder et nødvendig ankerfeste i et felt der mye fortsatt er i utvikling.

En standardbasert tilnærming bidrar først og fremst til forutsigbarhet og konsistens. Når kryptografiske mekanismer endres, må de fungere på tvers av systemer, virksomheter og landegrenser. Uten felles standarder risikerer man inkompatible løsninger, økt kompleksitet og svakere sikkerhet i grensesnittene. Det er i disse grensesnittene mange av de største sårbarhetene vil oppstå.

Det finnes allerede standardiserte algoritmer for PQC (nist.gov), blant annet utviklet av National Institute of Standards and Technology

For finanssektoren, der tillit og samvirke er grunnleggende forutsetninger, er dette særlig viktig. Betalingssystemer, meldingsutveksling, autentisering og rapportering er avhengige av at aktører kan stole på hverandres sikkerhetsmekanismer. Standarder gjør det mulig å etablere denne tilliten uten at hver enkelt relasjon må vurderes og forhandles særskilt.

En standardbasert tilnærming er også avgjørende for langsiktig robusthet. Kvantesikkerhet er ikke et endepunkt, men en fase i en kontinuerlig utvikling av kryptografiske metoder. Ved å knytte seg til anerkjente standarder reduseres risikoen for å låse seg til løsninger som senere viser seg å være svake, utdaterte eller vanskelige å videreutvikle. Standarder gir et rammeverk for kontrollert endring, der nye algoritmer og mekanismer kan fases inn uten å måtte bygge alt på nytt.

Standarder spiller også en viktig rolle i samspillet med leverandørmarkedet. Uten standarder risikerer man økt avhengighet av enkeltleverandører og proprietære løsninger. Med en standardbasert tilnærming kan sektoren stille tydeligere og mer konsistente krav, fremme konkurranse og redusere risikoen for innlåsing. Dette er særlig viktig i en overgangsfase der teknologien fortsatt modnes, og utviklingen er i bevegelse.

Samtidig er det viktig å understreke at en standardbasert tilnærming ikke betyr passivitet eller fravær av vurdering. Standarder må tolkes, tilpasses og anvendes med faglig skjønn. De gir retning og rammer, men fritar ikke virksomheter og sektorer fra ansvar for å forstå egen risiko og egne behov. Tvert imot gir de et felles utgangspunkt for å gjøre nettopp dette på en mer strukturert og sammenlignbar måte.

4 Roller og ansvar i en kvantesikker finansnæring

Overgangen til kvantesikkerhet er et økosystemansvar. Roller og ansvar må være tydelige for å unngå fragmentering og "hull" i verdikjeden.

4.1 Finansforetak

Finansforetak har ansvar for styring, risikobasert prioritering og oppfølging av egen eksponering, inkludert krav og forventninger til leverandører. Arbeidet med kvantesikring av systemene og infrastrukturen bør forankres i ordinær styringsstruktur for IKT risiko og operasjonell robusthet, som også harmonerer med DORA rammeverkets mål om robusthet og kontroll[19].

4.2 Finansielle markedsinfrastrukturer

Markedsinfrastrukturer har en særskilt rolle gitt kritikalitet og systemrisiko. De bør bidra til sektorvis koordinering, samspillstesting og felles modenhetsløp, i tråd med internasjonale forventninger om harmonisering og koordinert migrasjon. Dette veikartet er finansnæringens tilnærming og retningsgivende dokument for å sikre en koordinert vei mot kvantesikkerhet. Finansnæringen står imidlertid ikke alene i denne problemstillingen, og samarbeid på et tverrsektorielt nivå vil være viktig.

4.3 Leverandører og tjenestetilbydere

Leverandører må støtte standardbasert migrasjon og dokumentere veikart for kvantesikkerhet. DORA forsterker betydningen av tredjepartsstyring i finanssektoren, og legger til rette for et mer strukturert og harmonisert kravbilde mot IKT leverandører. For andre sektorer vil også NIS2[20] og Digitalsikkerhetsloven[21] forsterke denne betydningen.

4.4 Myndigheter og tilsyn

Myndigheter og tilsyn har rolle i å støtte harmonisering, tydeliggjøre forventninger og legge til rette for koordinert overgang. ESA[22] har publisert tekniske standarder under DORA som styrker harmonisering av IKT risikostyring, tredjepartsstyring og hendelses klassifisering/rapportering.

4.5 Samarbeid og sektorinitiativer

Koordinert overgang og felles læring reduserer kostnad og risiko. Dette samsvarer med G7 veikartets intensjon om harmonisert migrasjon og med BIS' vekt på koordinering i et tett sammenkoblet finanssystem. Dette veikartet bygger som nevnt på etablerte, internasjonale veikart og veiledninger. Dermed kan vi anse det å følge dette veikartet som en del av en harmonisert migrasjon.

[19] Regulation on Digital Operational Resilience for the Financial Sector - 2022/2554 - EUR-Lex
[20] NIS2-direktivet - regjeringen.no
[21] Veileder i digitalsikkerhetsloven og -forskriften - Nasjonal sikkerhetsmyndighet
[22] ESAs publish guide on DORA Oversight Activities (eba.europe.eu)

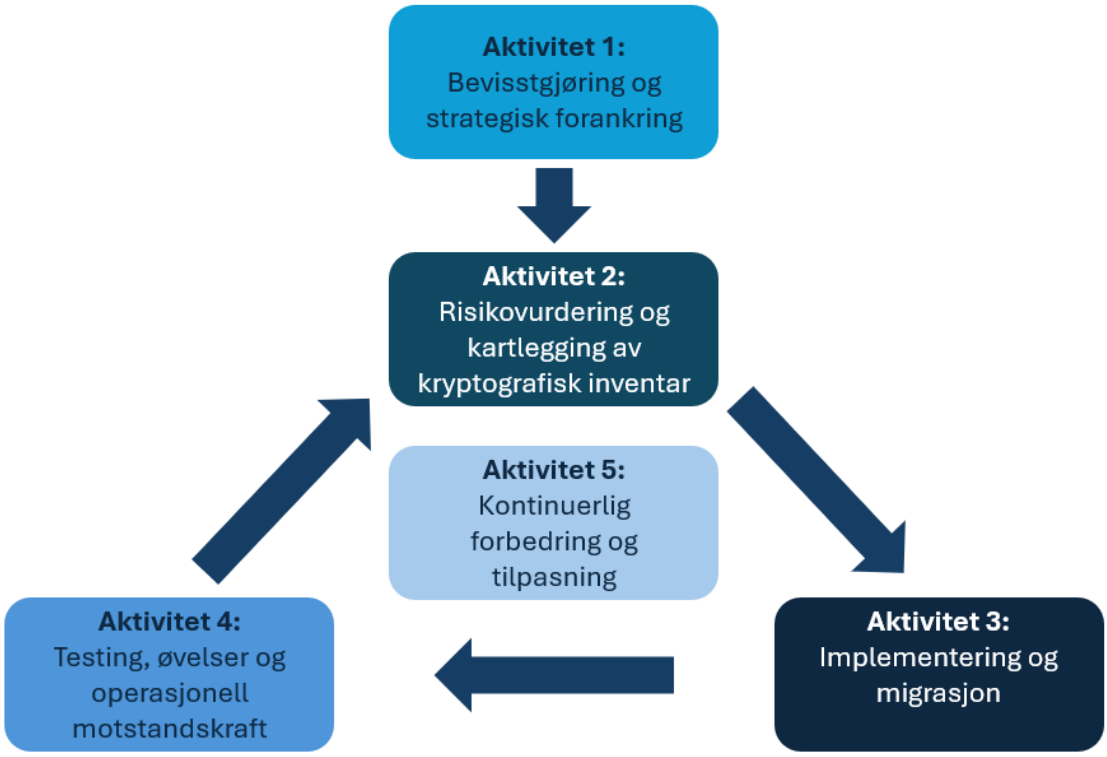
For å lykkes med et slikt samarbeid er det naturlig å tenke seg et formalisert bransjesamarbeid hvor man koordinerer innsats, erfaringer og beste praksis av selskapene. Dette må også inkludere de viktigste leverandørene og fellesprosjekter.

5 Veikart for overgang til en kvantesikker finansnæring

Basert på veletablerte standarder og internasjonale veikart anbefaler Finans Norge følgende tidslinje og aktiviteter for kvantemigrasjon:

Figur: Tidslinje for en kvantesikker finansnæring basert på G7 CSEG[23] sin anbefaling

Internasjonale anbefalinger legger til grunn at migrasjon ikke er lineær. Aktivitetene må pågå parallelt og iterativt, med løpende læring og justering. Veikartet består av 6 hovedaktiviteter:



For å kunne sikre at gjennomførelsen av aktivitetene skjer på best mulig vis, er det noen overordnede rammer som bør være på plass for å sikre modenheten til organisasjonen.

For at kvantemigreringen gjennomføres, er man avhengig av å ha en risikobasert tilnærming der man innlemmer kvanteresistent kryptografi inn i eksisterende styringsmodeller i hver virksomhet. Som et

[23] G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector (treasury.gov)

ledd i dette arbeidet, er det viktig å kontinuerlig overvåke aktivitet rundt utviklingen og modenheten til ulik relevant kvanteteknologi, og ikke minst oppdateringer på standarder, relevante verktøy, og hvilke trusler som oppstår. Informasjonen som denne overvåkningen av eksterne avhengigheter samler inn, må deles med relevante parter i organisasjonen, slik at det igjen gir et tilstrekkelig beslutningsgrunnlag ved den kontinuerlige prioriteringen av ressurser. Denne informasjonsinnhentingen er et ledd i å sikre en viss fleksibilitet for organisasjonen, ved at man hele tiden kan tilpasse justeringer i forhold til hva som passer organisasjonen best, gitt dets stadig utviklede risikobilde.

Tilrettelegging for god, strukturert dialog med leverandører er avgjørende for å sikre alle ledd i organisasjonen. I møte med denne nye teknologien er dette viktig for å raskt identifisere problemer som måtte oppstå, ikke minst for å dele innsikt og fremme løsninger.

Disse kontinuerlige aktivitetene er med på å støtte opp om effektiv migrasjon og implementering.

Sammendrag av anbefalinger fra NSM Cryptographic Recommendations 2025 (nsm.no)

- ***Bruk etablerte standarder for kryptografi:*** *unngå å utvikle egne kryptografiske løsninger, og benytt kun anerkjente, standardiserte kryptografiske løsninger som er utviklet og vedlikeholdt av anerkjente fagmiljøer.*
- ***Etabler og opprettholde et kryptografisk inventar:*** *kartlegg og dokumenter en detaljert oversikt over all bruk av kryptografiske algoritmer, som grunnlag for risikovurdering og migreringsplaner.*
- ***Bygg kryptografisk smidighet i arkitektur og styring:*** *vær forberedt på å raskt kunne bytte eller oppdatere kryptografiske komponenter uten omfattende endringer i forretningskritiske systemer.*
- ***Styrk styring og kontroll av kryptografiske nøkler:*** **se til at det foreligger en detaljert plan for nøkkelhåndtering i systemene.**
- ***Generer tilfeldige tall på en sikker måte:*** *benytt godkjente og veldokumenterte metoder for generering av tilfeldige tall, som oppfyller krav til sikkerhet og etterprøvbarhet (QRNG).*
- ***Forbered organisasjonen på fremveksten av kvanteteknologi:*** **utarbeid en helhetlig migreringsplan som prioriterer systemer og data med lang beskyttelsesverdi, og som tar høyde for regulatoriske krav og eksterne avhengigheter.**

Aktivitet 1: Bevisstgjøring og strategisk forankring

- Bevisstgjøre, heve kompetanse og forankre kvantesikkerhet i relevante fora
- Plassere ansvaret for kvantesikkerhet innenfor eksisterende rammer for IKT-risikostyring og robusthet
- Tydeliggjøre ansvar for koordinering og ledelse av prosessen, etablere tverrsektorielt team for å sikre overordnet prosjektansvar

Formålet med denne aktiviteten er å etablere en felles realistisk forståelse av kvantetrusselen, samt å forankre kvantesikkerhet som et strategisk anliggende innenfor eksisterende styring av IKT-risiko og operasjonell robusthet.

For å forberede organisasjonen på endringene, kreves det en forankring og forståelse for hvorfor man skal gjøre endringen, hva som bør gjøres, og ikke minst hvorfor man skal gjennomføre det. Derfor er et informasjonsarbeid nødvendig. Både ledelse og andre relevante parter i organisasjonen må få en grunnleggende forståelse for kvantemigrasjon, slik at man kan innrette organisasjonen best mulig. Kompetanseheving, både i det enkelte selskap, men også i næringen blir derfor viktig.

Etter at en god, grunnleggende forståelse for temaet er etablert, er det viktig å definere og kartlegge hvordan organisasjonen skal gjennomføre kvantemigrasjon. For å gjøre dette er man avhengig av å gjennomføre parallelle prosesser, både på et teknisk og strategisk nivå. Det å definere klare mål og en strategi, samt å bygge opp nødvendig intern kapasitet, gjennom for eksempel pilotprosjekter eller workshoper, bør være i fokus. Et viktig ledd i målsettingen, er dermed utarbeidelse av en migrasjonsstrategi, klar ledelse, et dedikert tverrfaglig team bestående av representanter fra blant annet juridisk, HR, operativ sikkerhet og teknologi, og ikke minst at det budsjetteres for dette arbeidet. Denne prosessen krever øremerkede ressurser for å sikre en langsiktig forsikring for at målsetningen som er satt følges opp og operasjonaliseres på en tilstrekkelig måte.

For å sikre at kvantemigrasjonen og prosessen som legges til grunn blir tilstrekkelig fulgt opp, er det viktig å plassere ansvaret for prosessen innenfor eksisterende rammer. Samtidig er det viktig at ledelsen av prosessen får tilgang til de aktuelle partene som kan være relevant på tvers, gitt at denne teknologiutviklingen krever en tilnærming basert på samhandling for å sikre at ingen deler av organisasjonen risikerer å falle utenfor.

Finansforetak og øvrige aktører bør:

- Anerkjenne kvantetrusselen som en langsiktig, men allerede relevant risiko, særlig knyttet til data med lang konfidensialitets- og integritetshorisont
- Forankre kvantesikkerhet i relevante styringsfora (styre, toppledelse eller tilsvarende), uten å etablere parallelle styringsstrukturer
- Plassere ansvaret for kvantesikkerhet tydelig innenfor eksisterende rammer for IKT-risikostyring og robusthet, i tråd med DORA-logikken

Manglende tidlig forankring er en hovedårsak til senere hastetiltak og uforholdsmessige kostnader. Målet blir dermed ikke å ta teknologiske valg, men å sikre at temaet er forstått, prioritert og institusjonalisert på et tidlig tidspunkt. Denne prosessen er også med på å gi et tilstrekkelig grunnlag for kryptografisk smidighet.

DORA-logikken:
DORA regulerer digital operasjonell motstandskraft. Det er altså ikke et teknologivalg. Forordningen stiller krav til IKT-risikostyring, tredjeparts- og leverandørstyring, testing, hendelseshåndtering og rapportering. Dette innebærer at virksomhetene må forstå, styre og redusere risiko som kan true digital robusthet.
PQC vil være et viktig ledd i å sikre fremtidig operasjonell digital motstandskraft. Dermed er prioriteringen av kvantemigrering viktig.

Aktivitet 2: Risikovurdering og kartlegging av kryptografisk inventar

- Etablere kryptografisk inventar: oversikt over hvor og hvordan kryptografi brukes i dag
- Vurdere datatype og beskyttelseshorisonten for å definere prioriteringsrekkefølge
- Skissere en risikobasert migrasjonsstrategi
- Definere en tidslinje for gjennomføring av migrasjon

Formålet med aktiviteten er å skape en oversikt over virksomhetens kryptografiske avhengigheter. Et sentralt element for denne prosessen er etablering av et kryptografisk inventar, som gir oversikt over hvor og hvordan kryptografi brukes i virksomheten og i verdikjeden.

Siden en samtidig migrasjon av den fullstendige porteføljen ikke er realistisk, må organisasjonen vurdere datatype og beskyttelseshorisonten til dataen for å rangere prioriteringsrekkefølgen for hvilken data som må kvantesikres først. Utfra prioriteringsarbeidet som er gjort, skal organisasjonen utvikle en risikobasert migrasjonsstrategi og skissere en intern tidslinje der den mest kritiske dataen med lengst beskyttelseshorisont migreres først.

Gradert kommunikasjon, forretningskritiske data og andre kritiske finansielle systemer der kompromittering eller svikt kan få betydelige konsekvenser for drift, finansiell stabilitet eller omdømme, bør prioriteres. For å sikre en tilstrekkelig kartlegging er det videre viktig å kategorisere ytterligere. Viktige spørsmål å stille seg i denne prosessen er dermed hvor dataen befinner seg, om det finnes krav til konfidensialitet, dataens sensitivitet, hvem ansvaret ligger hos, hvem som har tilgang på det, og hva formålet med kryptografien er.

Faktorer som påvirker vurderingene på beskyttelseshorisonten av dataen, vil blant annet være hvilke PQC-standarder som eksisterer på inneværende tidspunkt, og dets modenhet og tilgjengelighet. Dette må sees opp mot hvilken implementeringsinnsats som kreves, altså kompleksiteten i gjennomføringen. Her må innsatsen, kostnaden og tiden som kreves for en sikker kvantemigrering vurderes.

Ved vurderingen av hvilken data som skal prioriteres først, er det ulike kjennetegn man kan ta utgangspunkt i. Data med langvarige avhengigheter, lang beskyttelseshorisont, og lavthengende frukt som kan overføres umiddelbart, er eksempler på data som bør prioriteres høyt. Etter dette kan data med kortere migrasjonsløp og tekniske tiltak som vil føre til fremtidig operasjonell fortjeneste prioriteres. Til slutt kan data med lav risiko, eller data som kan håndteres gjennom eksisterende programmer for modernisering prioriteres.

For å gjennomføre dette prioriteringsarbeidet, er man avhengig av god koordinering og samhandling med eksterne interessenter. Dette er sentralt for å sikre at alle parter tilfredsstiller de kravene og behovene organisasjonen har i den satte tidsrammen. Disse aktørene inkluderer blant annet standardiseringsmiljøer, leverandører, tilsynsmyndigheter og øvrige samarbeidspartnere. Overfor

leverandører må organisasjonene legge krav om PQC til grunn, spesielt mot de som understøtter kritiske funksjoner.
En annen viktig vurdering av når migrasjonen skal finne sted, er hensynet som må tas til internasjonale prioriteringer og anbefalinger. Det er skissert opp ulike tidslinjer i ulike anbefalinger, men de viktigste fellesnevnerne er at det er enighet om at all kritisk data skal være kvantesikker innen 2030. Dette inkluderer systemer som behandler data med beskyttelseshorisont til tidligst 2030 eller benytter seg av logisk adgangskontroll basert på asymmetriske algoritmer[24]. 2035 er det andre årstallet man må ta hensyn til. Det er det overordnede målet for at all data skal være kvantesikret.

Internasjonale anbefalinger understreker at planleggingen må være fleksibel og iterativ. Strategien som utvikles bør derfor ses som en levende prosess som skal justeres i takt med standardutvikling, leverandørmodenhet og regulatoriske forventninger. Fleksibiliteten vil være med på å legge grunnlaget for å ta i bruk innsikten som samles gjennom prosessen for å tilpasse strategien ytterligere til organisasjonens behov. Dermed vil den understøtte en kunnskapsbasert beslutning om migrasjon, og smidigheten som må være på plass for å kunne raskt tilpasse tiltak etter behov som kommer frem ved eventuelle endrede rammevilkår, som for eksempel reviderte internasjonale standarder.

For å sikre at organisasjonen er rigget godt nok til å operasjonalisere strategien, er det også viktig å tilpasse interne prosesser for å bygge opp organisasjonen sin kapabilitet. Gap i intern kompetanse, kapabiliteten til teknologien som brukes, prosessene som er på plass, og organisasjonen er andre avhengigheter som må vurderes. Her må man vurdere hvordan disse faktorene kan påvirke hva man kan og bør prioriterer først.

Disse aktivitetene støtter sentrale behov i DORA, herunder kravet om helhetlig oversikt over IKT-avhengigheter og tredjepartsflater[25]. EU-[26] og G7[27]-veikartene fremhever moden kryptografisk forvaltning som en forutsetning for både migrasjon og utvikling av kryptografisk smidighet.

Aktørene bør:

- identifisere systemer, tjenester og prosesser som er avhengige av kryptografiske mekanismer
- vurdere datatyper og beskyttelseshorisonten til dataen
- rangere prioritert data utfra identifisert migreringsbehov
- prioritere kritiske funksjoner, felles infrastrukturer og data med lang beskyttelseshorisont
- vurdere overgangsbehov i lys av både kvantetrussel og migrasjonskompleksitet

[24] Veileder, kvantemigrasjon (nsm.no)
[25] Regulation on Digital Operational Resilience for the Financial Sector - 2022/2554 - EUR-Lex
[26] A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryprography (digital-strategy.ec.europa.eu)
[27] G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector (treasury.gov)

- utforme overordnet strategi, og detaljerte planer som legger til rette for kryptografisk smidighet, slik at fremtidige endringer kan gjennomføres med lavere risiko og kostnad

Det finnes flere etablerte ressurser som kan støtte organisasjonen i å kartlegge, strukturere og vurdere sitt kryptografiske inventar:

- ***EUROPOL: Post quantum cryptography report (europol.europa.eu)***
  - *Inneholder egen metodikk for å vurdere datatyper, beskyttelseshorisont og eksponering.*
- ***PQC-coalition: PQC Inventory Workbook (pqcc.org)***
  - *Et detaljert regneark for å samle, klassifisere og vedlikeholde kryptografiske komponenter på tvers av systemer og leverandører.*
- ***TNO, AIVD, CWI: Handbook for Quantum-Safe Cryptography (tno.nl)***
  - *Oppdatert håndbok som gir konkret veiledning i å finne kryptografiske komponenter, gjennomføre inventarbygging, vurdere kvantetrussel (Figure 2.7) og etablere kryptografisk smidighet.*

Aktivitet 3: Implementering og migrasjon

- Kryptografisk smidighet må oppnås
- Benytte standardiserte transformasjoner

Denne aktiviteten omfatter gradvis og kontrollert implementering av kvantesikre løsninger, ofte i form av hybride overgangsmodeller der klassiske og kvantesikre mekanismer benyttes parallelt. For at denne aktiviteten skal kunne gjennomføres uten større driftsforstyrrelser og tap av interoperabilitet, er det grunnleggende arbeidet som legges ned i aktivitet 1-3 avgjørende.

For å sikre en så smidig prosess som mulig, kan for eksempel utviklingen av automatiserte støtteverktøy være hensiktsmessig. I tillegg må nødvendige systemoppgraderinger gjennomføres, i tråd med produksjonssettingen av skisserte løsninger.

Det er viktig å understreke at dette ikke er et enkelt teknologisk skifte, men en flerårig transformasjon som krever tett samspill mellom teknologi, prosesser og styring. Migrasjonen bør derfor gjennomføres fasevis, med kontinuerlig monitorering, og ikke minst tydelige stoppunkter for evaluering og justering. Her er det viktig at overordnet ledelse av prosessen er tett koblet på, slik at de kan jobbe fortløpende med å identifisere og fjerne eventuelle barrierer som måtte dukke opp. Denne kontinuerlige monitoreringen vil også være med på å kunne tilpasse prosessen og tempoet i overgangen til utviklingen av trusselbildet og teknologiutviklingen.

Sentrale hensyn er:

- å unngå driftsforstyrrelser og tap av interoperabilitet
- å sikre koordinering på tvers av interne systemer og eksterne avhengigheter
- å håndtere ytelse, integrasjon og kompatibilitet som del av helhetlig endringsstyring

Som nevnt tidligere er det ikke anbefalt å skape egne kryptografiske algoritmer, men å bruke en standardisert tilnærming. NIST har oppdaterte lister over hvilke algoritmer som kan brukes til dette formålet[28].

Et utvalg godkjente og standardiserte PQC-algoritmer:

- ML-KEM (Kyber). NIST-standard *FIPS 203* (nist.gov)
- MLDSA (Dilithium). NIST-standard *FIPS 204* (nist.org)
- SL-DSA (SPHINCS+). NIST-standard *FIPS 205* (nist.org)
- LMS. Standardisert i *RFC 8554* (ietf.org)
- XMSS. Standardisert i *RFC 8391* (ietf.org)

[28] Post-Quantum Cryptography - Computer security Resource Center (nist.gov)

Aktivitet 4: Testing, øvelser og operasjonell motstandskraft

- Pilotering av migrering
- Jevnlig funksjonstesting

Kvantesikkerhet må inngå som en integrert del av virksomhetens testing og øvingsregimer. De nye kryptografiske implementeringene må testes for å sikre at den fungerer innenfor organisasjonens infrastruktur. Her er det også viktig å verifisere at endringene som er gjennomført opprettholder nødvendige ytelsesnivå. Slik kan organisasjonen følge fremdriften til implementeringen og vurdere modenheten fortløpende. Denne aktiviteten handler altså om å verifisere at endringer ikke svekker operasjonell robusthet eller systemenes integritet.

Her er det også sentralt å se at samspill på tvers av aktører fungerer som forutsatt. Dermed kan man også teste smidigheten til organisasjonen, altså at man har rigget organisasjonen slik at man er i stand til å bytte mellom algoritmer i takt med den stadige utviklingen. Et viktig ledd i testingen av denne smidigheten er å se at systemene fortsatt er kompatible med samarbeidspartnere, uavhengig av deres prosess for å gjøre seg selv kvantesikre. Her er det viktig å se at de styringsrammene som er satt faktisk fordrer samarbeid på tvers.

Aktiviteter kan omfatte:

- teknisk testing av ytelse, stabilitet og interoperabilitet
- operasjonelle øvelser som inkluderer kvantesikkerhetsrelaterte endringer
- sektorvis, eller tverraktør-tester, der det er hensiktsmessig

DORA stiller tydelige forventninger til digital operasjonell testing, og for utvalgte aktører også til trusselbasert testing (TLPT)[29]. Kvantesikkerhet bør derfor integreres i eksisterende testregimer på en risikobasert og proporsjonal måte, fremfor å etableres som et separat spor.

[29] Regulation on Digital Operational Resilience for the Financial Sector - 2022/2554 - EUR-Lex

Aktivitet 5: Kontinuerlig forbedring og tilpasning

- Regelmessig oppdatering av eksisterende inventar, strategier og målsettinger på bakgrunn av behov avdekket under testing

Kvantesikkerhet er ikke et sluttmål, men en vedvarende kapabilitet som organisasjonen skal innrette seg mot. I denne aktiviteten integreres kvantesikkerhet i virksomhetens løpende forbedringsarbeid og styringsprosesser.

Dette innebærer blant annet:

- regelmessig oppdatering av kryptografisk inventar
- justering av prioriteringer i takt med ny kunnskap om trusselbilde og teknologi
- videreutvikling av krav og forventninger til leverandører
- vedlikehold og styrking av kryptografisk smidighet over tid

Det er sentralt å gjennomføre praktisk testing, å ha en tydelig styringsstruktur og ikke minst ha en langsiktig forpliktelse til kryptografisk sikkerhet. Disse elementene i prosessen skal, etter beskrivelsen i tidligere aktiviteter, kontinuerlig testes for å sikre måloppnåelse. En slik kontinuerlig, dynamisk vurderingssyklus er med på å understøtte langsiktig måloppnåelse ved å gi et grundig vurderingsgrunnlag for videre forbedring og tilpasning. For hver vurderingssyklus er det viktig å vurdere, og eventuelt inkorporere oppdaterte eller nye standarder. Slik er man med på å drive prosessene fremover, samtidig som man bygger opp under kryptografisk smidighet.

Internasjonale rammeverk er samstemte om at evnen til kontinuerlig tilpasning gjennom kryptografisk smidighet er avgjørende for å håndtere usikkerhet rundt både teknologiutvikling og tidshorisonter. Denne aktiviteten sikrer at kvantesikkerhet forblir relevant, proporsjonal og innlemmet i ordinær virksomhetsstyring. Slik kan organisasjoner forberede seg på kvanteteknologien på en smidig måte uten at det går på bekostning av operasjonell integritet eller tillit.

6 Standarder og internasjonale rammeverk

Veikartet bygger på internasjonale autoritative rammeverk og standarder for å sikre interoperabilitet og felles retning.

6.1 Finanssektorspesifikke rammeverk

BIS[30] skisserer et strategisk veikart for hvordan finansnæringen kan forberede seg på kvantetrusselen. Det fremhever tidlig handling, inventar, hybridmodeller, forsvar i dybden og kryptografisk smidighet. G7 CEG veikartet[31] er utviklet for å støtte koordinert migrasjon og overgang til kryptografisk smidighet på tvers av finanssektoren.

6.3 Nasjonale og europeiske koordineringsspor

Veikartet til EU/NIS Cooperation Group[32] anbefaler en koordinert overgang til PQC og peker eksplisitt på moden kryptografisk forvaltning for å støtte migrasjon og forbedre kryptografisk smidighet generelt.

I tillegg til internasjonale standardiserings- og policyprosesser har Europol de senere årene etablert seg som en sentral aktør i arbeidet med kvantesikkerhet for finanssektoren. Gjennom sitt arbeid i European Cybercrime Centre (EC3), Europol Innovation Lab og det tverrsektorielle Quantum Safe Financial Forum (QSFF)[33], har Europol bidratt med et tydelig operasjonelt perspektiv på overgangen til post-kvante-kryptografi.

I 2026 publiserte Europol, i samarbeid med finansnæringen og internasjonale partnere, rapporten *Prioritising Post-Quantum Cryptography Migration Activities in Financial Services*[34]. Rapporten introduserer et strukturert rammeverk for prioritering av migrasjonstiltak, basert på en kombinasjon av kvantetrussel, databeskyttelseshorisont, eksponering, forretningsmessig konsekvens og tids- og kompleksitetskostnad ved migrasjon.

Europols tilnærming understøtter en fasevis og risikobasert overgang, der finansforetak oppfordres til å identifisere tiltak som både styrker sikkerheten på kort sikt og reduserer fremtidig teknisk gjeld. Dette omfatter blant annet forbedret oversikt over kryptografiske avhengigheter, bruk av hybride løsninger der det er hensiktsmessig, og tidlig dialog med leverandører.

Nasjonal Sikkerhetsmyndighet (NSM) har også laget et veiledende dokument for overgangen til en kvantesikker digital infrastruktur[35].

[30] Quantum-readiness for the financial system: a roadmap (bis.org)
[31] G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector (treasury.gov)
[32] A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryprography (digital-strategy.ec.europa.eu)
[33] About Quantum Safe Financial Forum (europol.europa.eu)
[34] Prioritising Post-Quantum Cryptography Migration Activities in Financial Services (europol.europa.eu)
[35] NSM Cryptographic Recommendations 2025 (nsm.no)

Dette arbeidet utfyller rammeverk fra G7, BIS og EU, ved å gi konkrete føringer for hvordan kvantesikkerhet kan operasjonaliseres i komplekse finansielle miljøer, og er særlig relevant i sammenheng med krav til risikostyring, prioritering og tredjepartsavhengigheter.

6.3 Standardiserings- og implementeringsspor

ETSI beskriver kvantesikker kryptografi som nødvendig for å beskytte bl.a. finans- og banktransaksjoner og peker på risikoen ved «store now, decrypt later»[36], det vi har valgt å definere som «harvest now decrypt later».

ETSI har også publisert et rammeverk for kvantesikre migrasjoner[37], som gir en kompakt steg-for-steg-modell å planlegge, gjenomføre og evaluere overgangen til kvantesikker kryptografi.

[36] Quantum-Safe Cryptography (etsi.org)

[37] Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum-Safe Migrations (etsi.org)

7 Implisitte konsekvenser for styring, risiko og etterlevelse

Kvantesikkerhet må integreres i virksomhetens helhetlige styring av IKT risiko og operasjonell robusthet. DORA er et relevant rammeverk fordi det etablerer en felles struktur for nettopp disse elementene i finanssektoren. Kvantetrusselen vil i praksis berøre flere av DORAs «pilarer» (IKT risikostyring, testing, tredjepartsrisiko og hendelseshåndtering/rapportering)[38].

7.1 Styring og kontroll

BIS understreker at overgangen ikke er et algoritmebytte, men en flerårig transformasjon som krever styring og koordinert planlegging.
I DORA kontekst betyr dette at kvantesikkerhet bør behandles som en del av den overordnede IKT risikostyringen og kontrollrammen, ikke som en isolert teknisk aktivitet.

7.2 Risiko

HNDL scenarioer og lange konfidensialitetskrav tilsier at risiko må vurderes over tidshorisont, ikke bare dagens trusselbilde. Dette bør gjenspeiles i prioritering av kritiske funksjoner, felles infrastrukturer og leverandørflater.

7.3 Tredjepartsstyring

EBA beskriver at DORA[39] (fra 17. januar 2025) innebærer at finansielle enheter må ha et omfattende register over IKT tredjepartsleverandører for å monitorere tredjepartsrisiko og støtte tilsyn og utpeking av kritiske leverandører. Dette er direkte relevant for kvantesikkerhet, fordi leverandørkjeden ofte bestemmer tempo, mulighetsrom og interoperabilitet i migrasjon.

7.4 Testing og robusthet

DORA forsterker forventninger til digital robusthetstesting. ESAs har utviklet tekniske standarder for TLPT under DORA, i tråd med TIBER EU, og beskriver mandatet og strukturen for slike tester[40].
For kvantesikkerhet betyr dette at testregimer og øvelser bør utvides til å omfatte migrasjonsrelaterte endringer som kan påvirke ytelse, interoperabilitet og operasjonell drift. For å sikre best mulig læring bør erfaringer og kompetanse deles i sektoren.

[38] Forordningen om Digital operasjonell motstandskraft, DORA (finansnorge.no)
[39] Digital operational resilience Regulation (DORA), European Banking Authority (eba.europa.eu)
[40] Final report - DORA Regulatory Technical Standards on TLPT (eba.europa.eu)

8 Anbefalinger for norsk finansnæring

9.1 Etabler felles minimumsgrunnlag for kryptografisk inventar og smidighet

Bygg et felles inventar rammeverk og en felles begrepsplattform for kryptografiske avhengigheter. Dette gir et bedre grunnlag for å utvikle kryptografisk smidighet som varig evne. EU veikartet anbefaler nettopp moden kryptografisk forvaltning for å støtte migrasjon og forbedre smidighet generelt.

9.2 Bruk DORA-drivere til å styrke leverandørdialogen

DORA kravet om register over leverandørkontakter og tredjepartsavhengigheter gir en naturlig mekanisme for å identifisere kvantesikkerhetsavhengigheter i leverandørkjeden og stille mer presise forventninger. ESAs tekniske standarder under DORA styrker harmoniseringen av tredjeparts- og IKT risikostyring og bør utnyttes til å skape sektorvis konsistens i kravbildet.

9.3 Piloter smidig overgang

BIS peker på hybridmodeller, fasevis migrasjon og kryptografisk smidighet som del av en realistisk overgang. Anbefalingen er å prioritere piloter som samtidig bygger varig smidighet. Selskapene bør ha gode styringsmekanismer. Endringene må testes, være sporbar og selskapene må ha evne til å justere når standarder og løsninger utvikler seg.

9.4 Intergrer kvantesikkerhet i testing

DORA understøtter forventningen om systematisk testing av operasjonell robusthet, og TLPT standardene gir et tydelig signal om modenhet på tvers av sektoren for utvalgte aktører. Kvantesikkerhet bør derfor planlegges inn i eksisterende test- og øvingspraksis på en måte som er risikobasert og proporsjonal.

9.5 Etabler koordinert samhandling nasjonalt og nordisk

G7 veikartet er eksplisitt laget for koordinert og harmonisert migrasjon. Norsk finansnæring bør bruke dette som grunnlag for felles arenaer, deling av erfaringer og samordnet dialog mot leverandørmarkedet og myndigheter.

9 Avslutning

Dette veikartet er i tråd med G7 Cyber Expert Group sitt veikart fra 2026, som fremhever overgang til kryptografisk smidighet, ikke-lineær migrasjon og koordinert handling på tvers av finanssektorens verdikjeder.
Kvanteteknologi markerer et skifte i forutsetningene for digital sikkerhet. For finansnæringen er dette ikke et akutt sammenbrudd, men en forutsigbar overgang som må håndteres med langsiktighet, struktur og samarbeid. BIS understreker at dette ikke er et enkelt algoritmebytte, men en flerårig transformasjon som bør omfatte kryptografisk smidighet, forsvar i dybden, hybridmodeller og fasevis migrasjon.

9.1 Kvantesikkerhet som konkurransefortrinn

Finansforetak som tidlig etablerer oversikt, styring og planverk, og som bygger kryptografisk smidighet som varig evne, vil stå bedre rustet til å møte endringer i standarder, leverandørlandskap og regulatoriske forventninger. Veikartet fra EU peker på moden kryptografisk forvaltning som et grep som både støtter migrasjon og forbedrer smidighet generelt.
Kvantesikkerhet bør derfor ses både som risikoreduksjon og som modenhets- og tillitsbygging som styrker robusthet og konkurransekraft.

9.2 Tidlig handling fører til lavere kostnad

Tidlig handling handler ikke om å gjøre alt på én gang, men om å etablere oversikt, prioritering og gjennomføringskraft før hastverk blir styrende. BIS peker på at implementeringsutfordringer og systemintegrasjon gjør at koordinert planlegging er nødvendig.
Smidighet er nøkkelen til å holde kostnader nede over tid. Når evnen til kryptografisk smidighet er bygget inn, blir fremtidige skifter billigere, raskere og mindre risikofylte.

9.3 Samarbeid

G7 veikartet fremhever behovet for en koordinert og harmonisert overgang til post kvante kryptografi og overgang til kryptografisk smidighet. I tillegg styrker DORA et felles forventningsbilde for robusthet, tredjepartsstyring og testing i finanssektoren.
Samarbeid på tvers av foretak, infrastrukturer, leverandører og myndigheter er en forutsetning for å oppnå kontrollert overgang og interoperabilitet.

10 Referanser

1. **AIVD, CWI, TNO**
   The PQC Migration Handbook – Guidelines for migrating to Post-Quantum Cryptography
   Desember, 2024
2. **Bank for International Settlements (BIS)**
   Quantum-Radiness for the Financial System: a Roadmap
   BIS Papers NO 158
   Juli, 2025
3. **Bank for International Settlements (BIS)**
   Quantum Computing and the Financial System: Opportunities and Risks
   BIS Papers No 149
   Oktober, 2024
4. **ENISA (European Union Agency for Cybersecurity)**
   Post-Quantum Cryptography: Current State and Quantum Mitigation
   Mai, 2021
5. **ENISA (European Union Agency for Cybersecurity)**
   Cryptographic Products and Servuces Market Analysis
   August, 2024
6. **ETSI (European Telecommunications Standards Institute)**
   Quantum Safe Cryptography and Security
7. **ETSI (European Telecommunications Standards Institute)**
   Framework for Quantum Safe Cryptographic Migration
8. **European Commission / NIS Cooperation Group**
   A Coordinated Implementation Roadmap for the Transition to Post Quantum Cryptography
   Juni 2025.
9. **European Supervisory Authorities (EBA, EIOPA, ESMA)**
   Regulatory Technical Standards and Implementing Technical Standards under DORA
   Publisert 2024–2025.
10. **Europol (2026)**
    Prioritizing Post Quantum Cryptography Migration Activities in Financial Services
    Publications Office of the European Union, Luxembourg.
11. **Federal Reserve Board**
    «Harvest Now Decrypt Later»: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks
    September, 2025
12. **FS-ISAC**
    Bulding Cryptographic Agility in the Financial Sector
    Oktober, 2024
13. **G7 Cyber Expert Group (CEG)**
    G7 Fundamental Elements of Cybersecurity for the Financial Sector – Post Quantum Cryptography

G7, 2022.

14. **G7 Cyber Expert Group (2026)**
    Advancing a Coordinated Roadmap for the Transition to Post Quantum Cryptography in the Financial Sector
    Januar, 2026.
15. **Nasjonal Sikkerhetsmyndighet (2023)**
    Kvantemigrasjon – veileder
16. **Nasjonal Sikkerhetsmyndighet (2025)**
    Guidance document NSM Cryptographic Recommendations
    Marrs, 2025
17. **NIST (National Institute of Standards and Technology)**
    Computer Security Resource Center
    Post Quantum Cryptography (PQC)
    PQC Standardization Process
18. **Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA)**
    Official Journal of the European Union, 27.12.2022.
19. **TIBER EU Framework (ECB m.fl.)**
    How to implement the European framework for Threat Intelligence-Based Ethical Red teaming
    Januar, 2025

Ordliste

Ord	Forklaring
API	*Application Programming Interface.* Programmeringsgrensesnitt. Et sett med regler som gjør at ulike programvarer kan kommunisere og utveksle data automatisk.
CRQC	*Cryptographically Relevant Quantum Computer.* Kvantedatamaskin som er tilstrekkelig kraftig til å være i stand til å kompromittere dagens kryptografi, som for eksempel løsninger basert på RSA og ECC.
Cryptographic inventory Kryptografisk inventar	En strukturert oversikt over virksomhetens kryptografiske komponenter som bruker i organisasjonens systemer og tjenester.
DORA	Forordning om digital operasjonell robusthet (*Digital Operational Resilience Act).* Felles rammeverk for håndtering av IKT-risiko, hendelser, testing, tredjepartsrisiko og informasjonsdeling.
ECC	*Elliptic Curve Cryptography*. En krypteringsmetode som bruker matematiske elliptiske kurver for å skape små, effektive og svært sikre nøkler.
HNDL	*Harvest now – Decrypt later*. Enkelte aktører samler masse krypterte data i dag for å kunne dekryptere og anvende den på et senere tidspunkt.
Kryptografisk smidighet (agilitet)	Evnen til å tilpasse seg og bytte kryptografiske algoritmer sømløst og effektivt. Gjør det mulig for organisasjonen å ligge i forkant av kryptografiske sårbarheter.
NIS2	EUs cybersikkerhetsdirektiv som skjerper kravene til risikostyring, hendelsrapportering og ledelsesansvar i kritiske sektorer.
PQC	*Post Quantum Cryptography*. Kryptografisk fagområde som omfatter utvikling og standardisering av kryptografiske algoritmer som er konstruert for å motstå angrep fra både klassiske og kvantebaserte beregningsmodeller.
Q-day	Viser til dagen en kvantedatamaskin blir kraftig nok til å knekke dagens kryptering.
QKD	*Quantum Key Distribution.* En sikker kommunikasjonsmetode som bruker kvantemekanikk til å generere og dele hemmelige nøkler, og som garanterer datakonfidensialitet ved at avlytting kan detekteres.
QRNG	*Quantum Random Number Generator.* En generator som bruker kvantefysikk til å lage uforutsigbare tilfeldige tall. En nøkkelkomponent for sterk og fremtidssikker kryptering.
RSA	RSA er en asymmetrisk krypteringsmetode som benytter en offentlig nøkkel for å kryptere klartekst, og en privat nøkkel for å dekryptere den krypterte teksten. Oppkalt etter *Rivest, Shamir og Adleman*.
TIBER	*Threat Intelligence-Based Ethical Red-teaming*. Felles europeisk rammeverk der myndigheter, finansforetak og leverandører samarbeider om testing av cybersikkerhet i det finansielle systemet.
TLPT	*Threat-Led Penetration Testing*. Sikkerhetstesting der realistiske angrepsscenarier basert på faktisk trusseletterretning brukes for å vurdere hvor godt en organisasjon klarer å oppdage, motstå og respondere på sofistikerte angrep.

TLS	*Transport Layer Security*. Utbredt kryptografisk protokoll som brukes for å sikre kommunikasjon over et datanettverk. Sørger for konfidensialitet, integritet og autentisitet mellom klient og en server.
BIS	*Bank for International Settlements.* Internasjonal organisasjon som fungerer som en bank for sentralbanker, og som jobber for global finansiell stabilitet gjennom samarbeid, forskning og støtte til sentralbankenes arbeid.
EC3	*European Cyber Crime Centre*. Europols senter for cyberkriminalitet. Etablert for å styrke EUs felles evne til å forebygge, avdekke og bekjempe alvorlig cyberkriminalitet.
ENISA	*European Union Agency for Cybersecurity*. EUs byrå for cybersikkerhet, som skal styrke og harmonisere cybersikkerhet i EU.
ESA	*European Supervisory Authorities.* De tre europeiske finalstilsynene, EBA, EIOPA og ESMA, som har ansvar for å harmonisere og styrke tilsyn av banker, forsikring, pensjon og finansmarkeder i EU.
ETSI	*European Telecommunications Standards Institute*. Europeisk standardiseringsorganisasjon som utvikler åpne og globalt anvendbare standarder for telekom, UT og digitale tjenester.
EUROPOL	EUs byrå for politisamarbeid. Støtter medlemslandene i å forebygge og bekjempe alvorlig internasjonal kriminalitet, cyberkriminalitet og terrorisme.
G7	Uformell gruppe bestående av sju av verdens ledende industriland; Canada, Frankrike, Tyskland, Italia, Japan, Storbritannia og USA.
NIS Cooperation Group	Samarbeidsgruppe bestående av representanter fra medlemsstater i EU, EU-kommisjonen og ENISA. Opprettet for å styrke strategisk samarbeid og informasjonsutveksling, for å sikre et høyt felles nivå av cybersikkerhet i EU.
NIST	*National Institute of Standards and Technology.* Utvikler målemetoder, standarder og teknologiske retningslinjer for å styrke innovasjon, konkurransekraft og cybersikkerhet.
NSA	*National Security Agency*. USAs føderale etat for etterretning og cybersikkerhet.
NSM	*Nasjonal sikkerhetsmyndighet*. Fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven) i Norge.

Finans Norge