basefarm

INTERNKONTROLL V.3

Sikkerhetssymposiet 2018

18-10-2018

Esten Hoel, SVP Quality & Security

SNAKKEPLAN

1. Outsourcing vs Risikostyring
2. Kontroll av tjenesteleverandør, da og nå
3. SOC-attestasjoner = win-win
4. Oppsummering

OM MEG

Informatiker – Systematiker – Kontrollfrik. Synes KPI'er er skikkelig kult…

Bakgrunn:

- OL94: Tidtaking / Resultatservice / TV-grafikk
- NSB Gardermobanen: Prosjektleder for informasjonssystemer
- Philips: Prosjektledelse
- TRI-MEX/Eurowatch: Sikkerhetstjenester for internasjonal verditransport (anti hijack)
- Jernbaneverket: Etablering av Driftssenter for GSM-R

- Fra 2005: Basefarm. Mandat: «Sette nerder i system»

ITIL Expert, CISM, Fotballtrener og pappa

OM BASEFARM

- Europeisk Managed Service Provider
- Grunnlagt i Norge i 2000. Fortsatt HQ i Norge
- 18 års erfaring med drift av alt fra Datasentre, via nettsider til forretningskritiske applikasjoner og tjenester
- Ca 500 driftskonsulenter og rådgivere
- 6 kontorer i Europeiske hotspots: Oslo, Stockholm, Amsterdam, Berlin, Frankfurt, Wien
- 9 Datasentre (2 i Norge)
- I 2017 kjøpte Basefarm **The unbelievable Machine Company (*um)**, ett ledende cloud og Big Data selskap i Tyskland
- Største kundesegmenter i Norge; Offentlig, Bank/Finans, Travel & eCommerce
- Fokus og satsningsområder: (Public) Cloud, Big Data, Sikkerhet

- I juli 2018 ble Basefarm kjøpt av **Orange**, og blir en del av deres internasjonale **Orange Cloud for Business** divisjon.

OUTSOURCING VS RISIKOSTYRING

Du kan outsource driften,
men ikke
eierskapet til din risiko!

DERFOR

Må du føre tilsyn med,
og kontrollere,
dine tjenesteleverandører!

KUNDENES KRAV TIL INTERNKONTROLL – PRE 2010

Utsetting av drift skjedde i all hovedsak til:

- Lokale virksomheter, basert på lokale datasentre, driftet av lokale mennesker, som kunne ta ansvar for din infrastruktur, og dine systemer. Hensikt: spare penger

Kravspec:

«Følger du ITIL? Ja/Nei»

«Oppfyller ditt foretak IKT forskriften? (Ja/Nei)»

«Er du ISO27001 sertifisert? Kult!»

Tilsyn ved selvsyn

KUNDENES KRAV TIL INTERNKONTROLL – 2010-2014

Utsetting av drift til flere, mer spesialiserte leverandører (multi-sourcing). Virtualisering aktualiserer bruk av delte, leverandøreide, plattformer og tjenester. Overgang fra å kjøpe produksjonsressurser (mennesker) til å kjøpe tjenester. Informasjonssikkerhet gradvis mer i fokus

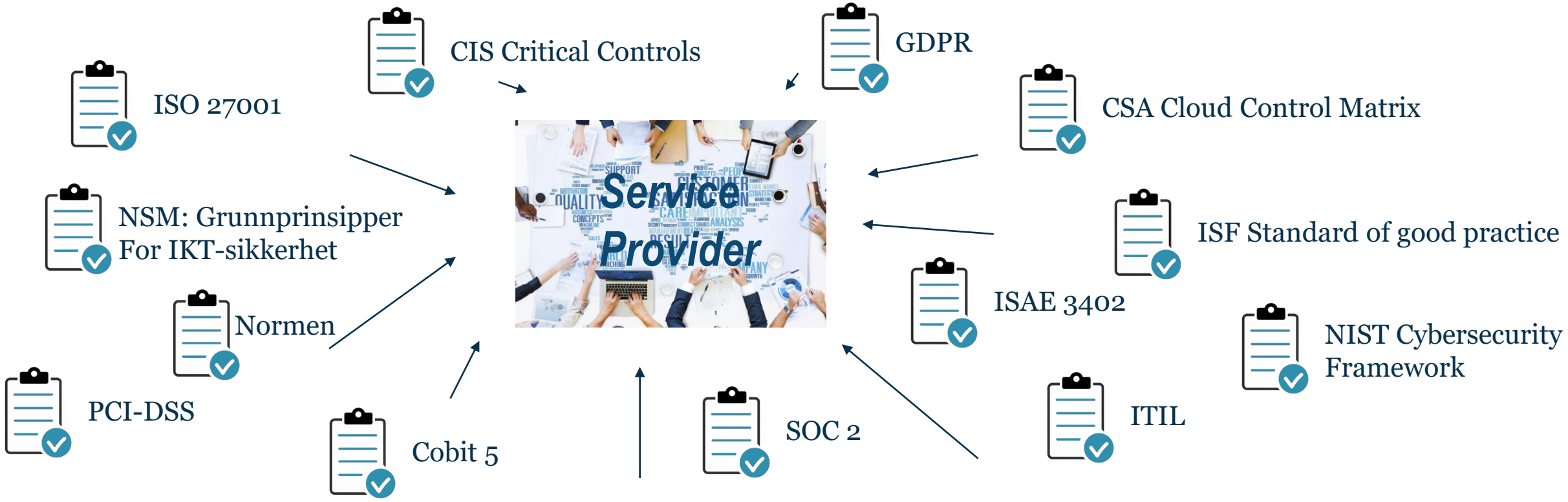
- ISO27001 går fra å være en differensiator til en de facto forutsetning for leverandører
- Bank/Finans går online, PCI-DSS blir et krav for de som håndterer kredittkort
- Revisjon av service providere starter for alvor
- ISAE3402 dukker opp sporadisk

Tilsyn ved innsyn og selvsyn

KUNDENES KRAV TIL INTERNKONTROLL – 2014 →

I stor grad leverer Service Providere i dag tjenester, der Kundene ikke lengre eier eller har kontroll over infrastrukturen. Tjenester produseres i lokale, regionale eller globale skyer. Data flyter potensielt fritt i et økosystem av leverandører, underleverandører og partnere.

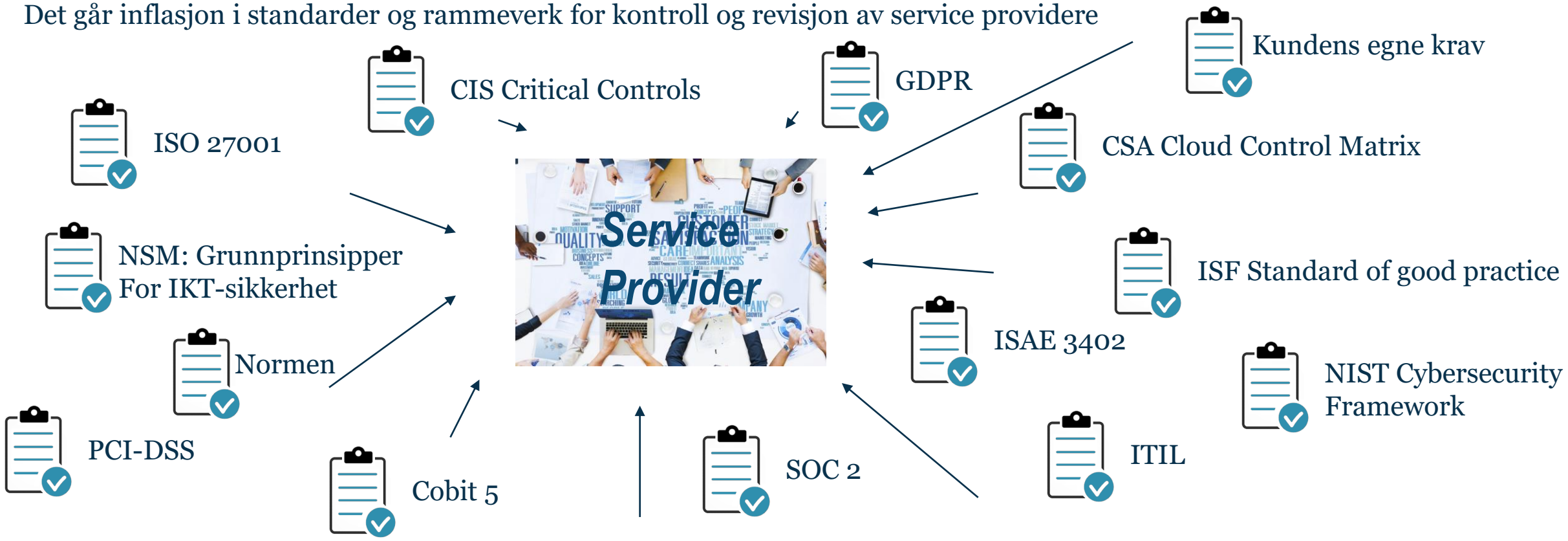
Det går inflasjon i standarder og rammeverk for kontroll og revisjon av service providere



KUNDENES KRAV TIL INTERNKONTROLL – 2014 →

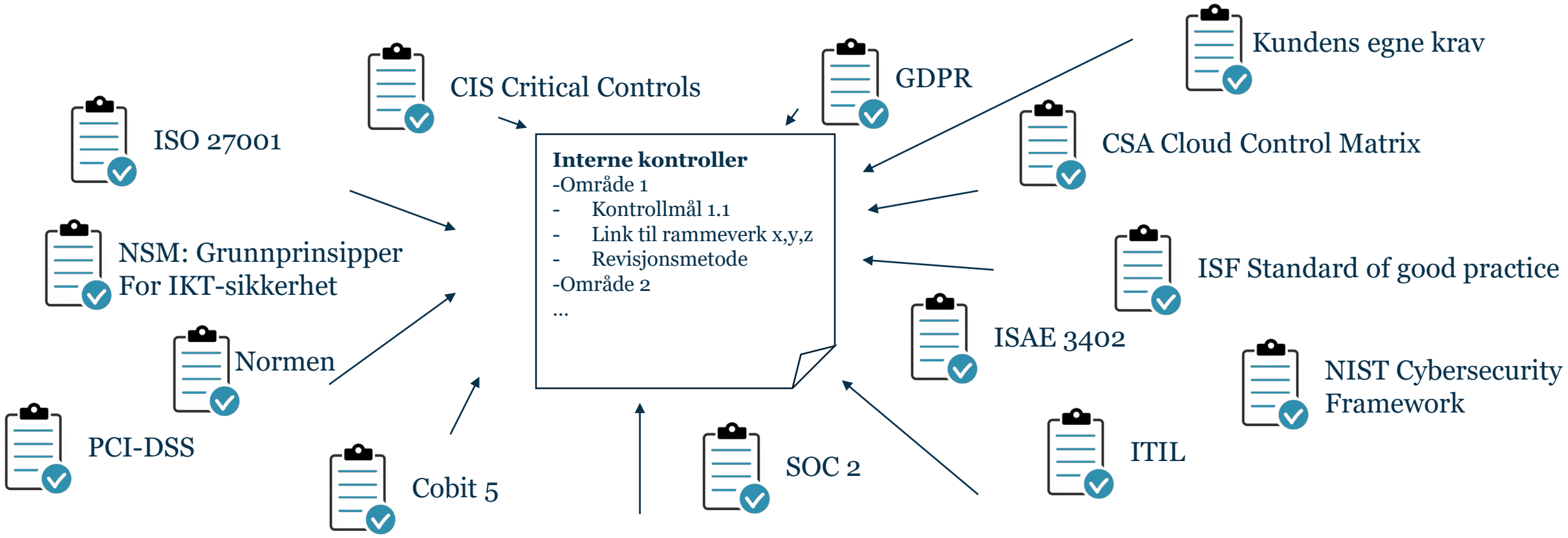
I stor grad leverer Service Providere i dag tjenester, der Kundene ikke lengre eier eller har kontroll over infrastrukturen. Tjenester produseres i lokale, regionale eller globale skyer. Data flyter potensielt fritt i et økosystem av leverandører, underleverandører og partnere.

Det går inflasjon i standarder og rammeverk for kontroll og revisjon av service providere



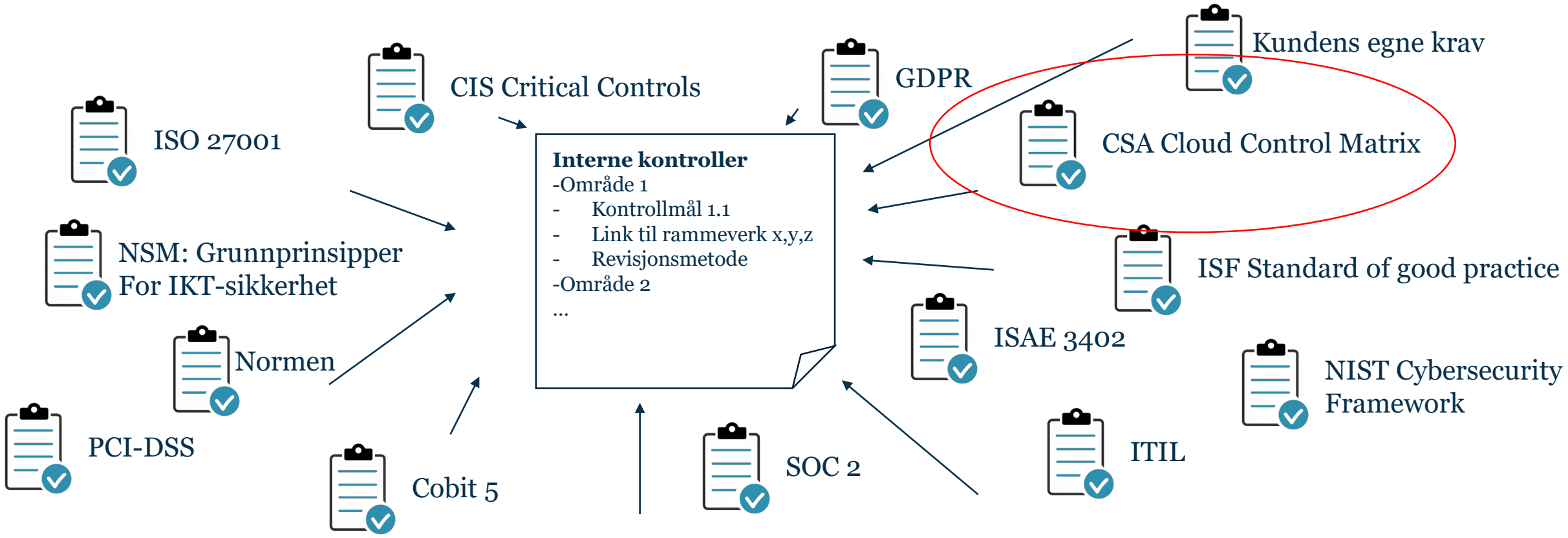
KONSOLIDER KRAV TIL ÉN LISTE MED KONTROLLER

- I de fleste tilfeller definerer standardene **Hva**, men overlater til oss å bestemme **Hvordan**
- Det er stor overlapp i **Hva** mellom de ulike rammeverkene



KONSOLIDER KRAV TIL ÉN LISTE MED KONTROLLER

- I de fleste tilfeller definerer standardene **Hva**, men overlater til oss å bestemme **Hvordan**
- Det er stor overlapp i **Hva** mellom de ulike rammeverkene



TRADISJONELL MODELL

- Kunder har en kravspec med krav til informasjonssikkerhet
- Kunder krever etterlevelse til sine foretrukne standarder og rammeverk
- Kunder reviderer sin Service Provider årlig
  - Scope begrenses av hensyn til tid/penger
  - Hver revisjon starter på scratch
  - Revisjoner fokuseres på kundens dedikerte systemer og tjenester
  - Revisjonen sjekker et øyeblikksbilde (nåsituasjonen)
  - Kunden må bære kosten for IT-revisor, egne ressurser og leverandørens medgåtte tid

- For Service Providere innebærer dette:
  - Ikke-strukturert revisjons-syklus
  - Stadige ad-hoc revisjoner
  - De samme kontrollene revideres mange ganger, med hårfine variasjoner
  - Ukoordinerte forbedringssløyfer for å lukke funn

VI ØNSKER OSS HIT…

- Service Provider etablerer samordnet internkontroll
- Attestasjonsmaler utarbeides basert på internasjonale standarder og rammeverk
- Uavhengig IT-revisor gjennomfører revisjoner i et årshjul
- Kunder abonnerer på rapport(er)
- Kundespesifikke revisjoner kan helt eller delvis utgå

- Kunder får revisjonsrapporter som:
  - Beskriver leverandørens kvalitetssystemer og internkontroll
  - Dekker «alt» i tjenestespekteret
  - Dekker hele kontrollperioden
  - Dekker dokumentasjonsbehovet for eksterne revisorer
  - Koster en brøkdel av det man ville måttet betale for en egen, like grundig, revisjon

ISAE3402 (SOC1)

- **Beskrivelse:** Attestasjonsrapport som beskriver og verifiserer internkontroll relatert til prosessering av finansiell informasjon.
- **Vanlige fokusområder:** IT Governance, informasjonssikkerhet, applikasjonsendringshåndtering, IT-drift, Backup & Recovery og incidenthåndtering.
- **Målgruppe:** Primært Kundens revisorer.
- **Bruksområder:** Brukes ofte for å erstatte eller minimere behov for egne kontrollaktiviteter hos leverandøren. Type I-rapporter er point-in-time rapporter mens Type II-rapporter dekker en periode (oftest et år).

I Norge har ISAE3402 ofte vært (mis)brukt til å kontrollere sikkerhet mer generelt enn den opprinnelig er utviklet for

SOC2

- **Beskrivelse:** Attestasjonsrapport om internkontroller som dekker alle vesentlige og relevante deler av informasjonssikkerhet
- **Vanlige fokusområder:** Internkontroll relatert til generell informasjonsikkerhet, tilgjengelighet, integritet, konfidensialitet og personvern (Trust Principles)
- **Målgruppe:** Kunder med behov for å bekrefte at leverandøren har gode og fungerende rutiner relatert til de spesifikke områdene dekket av rapporten
- **Bruksområder:** Bekreftelse av at leverandøren har gode internkontrollrutiner for sikkerhet generelt, eller i forhold til bestemte regulatorisk krav eller bransjenormer. Type I-rapporter er point-in-time rapporter mens Type II-rapporter dekker en periode (oftest et år).

SOC2 rapporter vil inneholde detaljerte beskrivelser av leverandørens systemer, prosesser og sikkerhetskontroller. Rapportene er derfor strengt konfidensielle

SOC3

- **Beskrivelse:** Scope er det samme som for SOC2, men selve rapporten vil være mer overordnet og summarisk, og vil normalt gjøres fritt tilgjengelig for kunder og andre interessenter via f.eks en webside
- **Vanlige fokusområder:** Internkontroll relatert til generell informasjonsikkerhet, tilgjengelighet, integritet, konfidensialitet og personvern (Trust Principles)
- **Målgruppe:** Kunder med behov for å bekrefte at leverandøren har gode og fungerende rutiner relatert til de spesifikke områdene dekket av rapporten, men uten å behøve detaljerte beskrivelser om kontroller eller revisjonsfunn
- **Bruksområder:** Tilsvarende ISO27001, en bekreftelse på at selskapet jobber systematisk med informasjonssikkerhet

OPPSUMMERING

- Dine tjenester og dine data er ditt ansvar, selv om du outsourcer
- ISO27001 er fint det, men sier antagelig ikke alt du behøver å vite om hvordan din leverandør ivaretar sikkerheten
- Kundespesifikke revisjoner er enten veldig dyre å gjennomføre, eller vil ikke kunne gå bredt/dypt nok
- Sikkerheten i din tjeneste avhenger også av leverandørens delte systemer, ressurser, prosesser og rutiner
- Still gjerne krav til din leverandør, men fokuser på **hva**, ikke **hvordan**
- Still krav/be om tredjeparts attestasjonsrapporter, f.eks ISAE3402 (SOC1), SOC2 eller SOC3
- Les rapporten, og ta stilling til relevansen i eventuelle funn
- Vurder hva (om noe) du trenger å kontrollere i tillegg