UNINETT-konferansen 2017

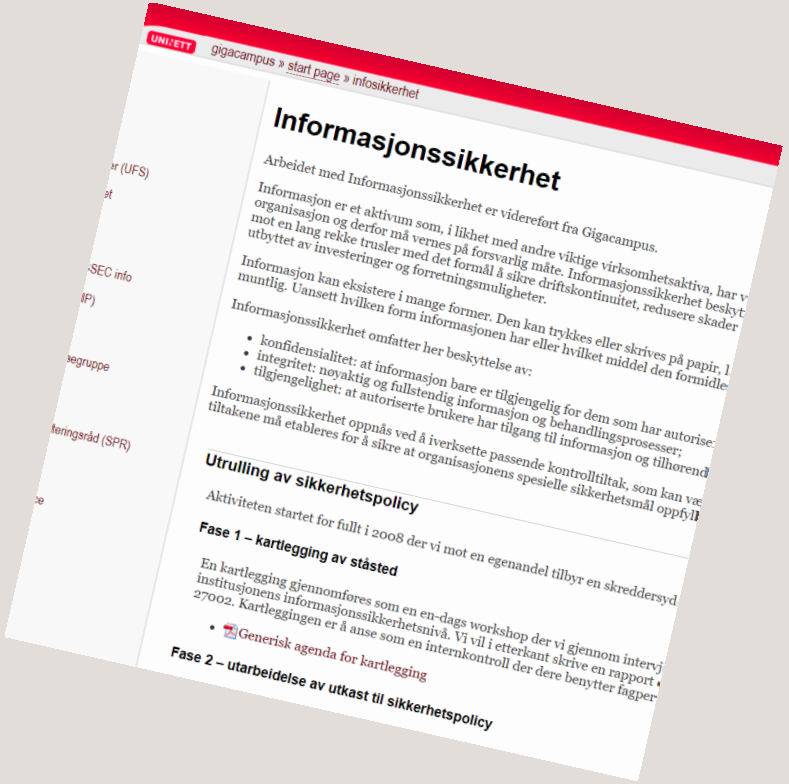
Erfaringer fra Sekretariatet for informasjonssikkerhet: landet rundt med ledelsessystem

Rolf Sture Normann, leder Sekretariat for informasjonssikkerhet i UH -sektoren

UNINETT

Startet i Giga Campus programmet

- Informasjonssikkerhet fra GigaCampus programmet
  - Arbeidet startet etter ønske fra prioriteringsråd (2007)
  - Utrulling av sikkerhetspolicy
    - Kartlegging av ståsted (revisjon)
    - Utarbeide utkast til sikkerhetspolicy (policyworkshop)
    - Vedlikehold (oppfølgingsmøter)
  - ROS



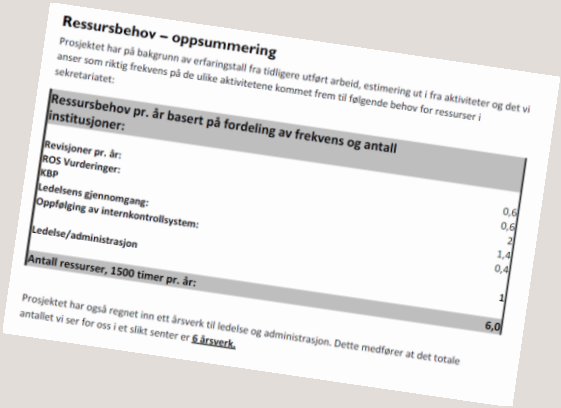
Tilsyn av Riksrevisjonen 2010/11

- Manglende internkontroll på informasjonssikkerhet
- Manglende kartlegging av informasjonsverdier
- Manglende risiko- og sårbarhetsvurderinger
- Manglende kultur og holdningsskapende arbeide

UNINETT

KD ønsker løsninger

- Forprosjektrapport, tilstanden i informasjonssikkerhet i UH sektoren (UNINETT, 20 juni 2011)
- Forslag om en faglig enhet på i størrelsesorden 6 personer
- Sekretariatet ble etablert høsten 2012



Ressursbehov – oppsummering

Prosjektet har på bakgrunn av erfaringstall fra tidligere utført arbeid, estimering ut i fra aktiviteter og det vi anser som riktig frekvens på de ulike aktivitetene kommet frem til følgende behov for ressurser i sekretariatet:

Ressursbehov pr. år basert på fordeling av frekvens og antall institusjoner:	
Revisjoner pr. år:	0,6
ROS Vurderinger:	0,6
KBP	2
Ledelsens gjennomgang:	1,4
Oppfølging av internkontrollsystem:	0,4
Ledelse/administrasjon	1
Antall ressurser, 1500 timer pr. år:	6,0

Prosjektet har også regnet inn ett årsverk til ledelse og administrasjon. Dette medfører at det totale antallet vi ser for oss i et slikt senter er **6 årsverk.**

UNINETT

Sekretariat for informasjonssikkerhet

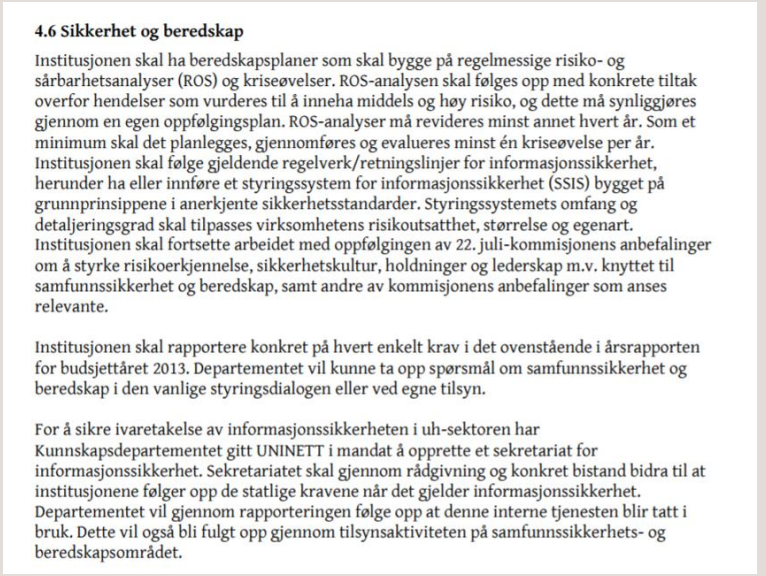
- Teller i dag 3 årsverk
- Mandat:
  - Legge til rette for ROS for enkeltinstitusjoner og dele erfaringer
  - Bidra til å utarbeide kontinuitet og beredskapsplaner, dele erfaringer
  - Bistå med revisjoner for å finne avvik
  - Ledelsessystem (Internkontroll) for informasjonssikkerhet, felles standard og metodikk
  - Ledelsens årlige gjennomgang
  - Opplæring og holdningsskapende arbeide
  - Rådgiving

UNINETT

Ledelsessystem (styringssystem) - tildelingsbrev

2013

- *«Institusjonen skal følge gjeldende regelverk/retningslinjer for informasjonssikkerhet, herunder ha eller innføre et styringssystem for informasjonssikkerhet (SSIS) bygget på grunnprinsippene i anerkjente sikkerhetsstandarder.»*



4.6 Sikkerhet og beredskap

Institusjonen skal ha beredskapsplaner som skal bygge på regelmessige risiko- og sårbarhetsanalyser (ROS) og kriseøvelser. ROS-analysen skal følges opp med konkrete tiltak overfor hendelser som vurderes til å inneha middels og høy risiko, og dette må synliggjøres gjennom en egen oppfølgingsplan. ROS-analyser må revideres minst annet hvert år. Som et minimum skal det planlegges, gjennomføres og evalueres minst én kriseøvelse per år. Institusjonen skal følge gjeldende regelverk/retningslinjer for informasjonssikkerhet, herunder ha eller innføre et styringssystem for informasjonssikkerhet (SSIS) bygget på grunnprinsippene i anerkjente sikkerhetsstandarder. Styringssystemets omfang og detaljeringsgrad skal tilpasses virksomhetens risikoutsatthet, størrelse og egenart. Institusjonen skal fortsette arbeidet med oppfølgingen av 22. juli-kommisjonens anbefalinger om å styrke risikoerkjennelse, sikkerhetskultur, holdninger og lederskap m.v. knyttet til samfunnssikkerhet og beredskap, samt andre av kommisjonens anbefalinger som anses relevante.

Institusjonen skal rapportere konkret på hvert enkelt krav i det ovenstående i årsrapporten for budsjettåret 2013. Departementet vil kunne ta opp spørsmål om samfunnssikkerhet og beredskap i den vanlige styringsdialogen eller ved egne tilsyn.

For å sikre ivaretakelse av informasjonssikkerheten i uh-sektoren har Kunnskapsdepartementet gitt UNINETT i mandat å opprette et sekretariat for informasjonssikkerhet. Sekretariatet skal gjennom rådgivning og konkret bistand bidra til at institusjonene følger opp de statlige kravene når det gjelder informasjonssikkerhet. Departementet vil gjennom rapporteringen følge opp at denne interne tjenesten blir tatt i bruk. Dette vil også bli fulgt opp gjennom tilsynsaktiviteten på samfunnssikkerhets- og beredskapsområdet.

UNINETT

Ledelsessystem for UH – en viktig oppgave for sekretariatet

- Studie av tilstanden i sektoren
  - Hva var drivkreftene (KDs krav, påvirkning fra UNINETT, etterlevelse av rettslige pålegg)
  - Administrasjonen (administrative behandlinger)
  - Dokumentinnhold vs. praksis
  - Sikkerhetsorganisasjonen var ukjent for mange av de som var omfattet av den
  - Tekniske sikringstiltak var på plass
  - Sikkerhetsdokumentasjonen var en formalitet

UNINETT

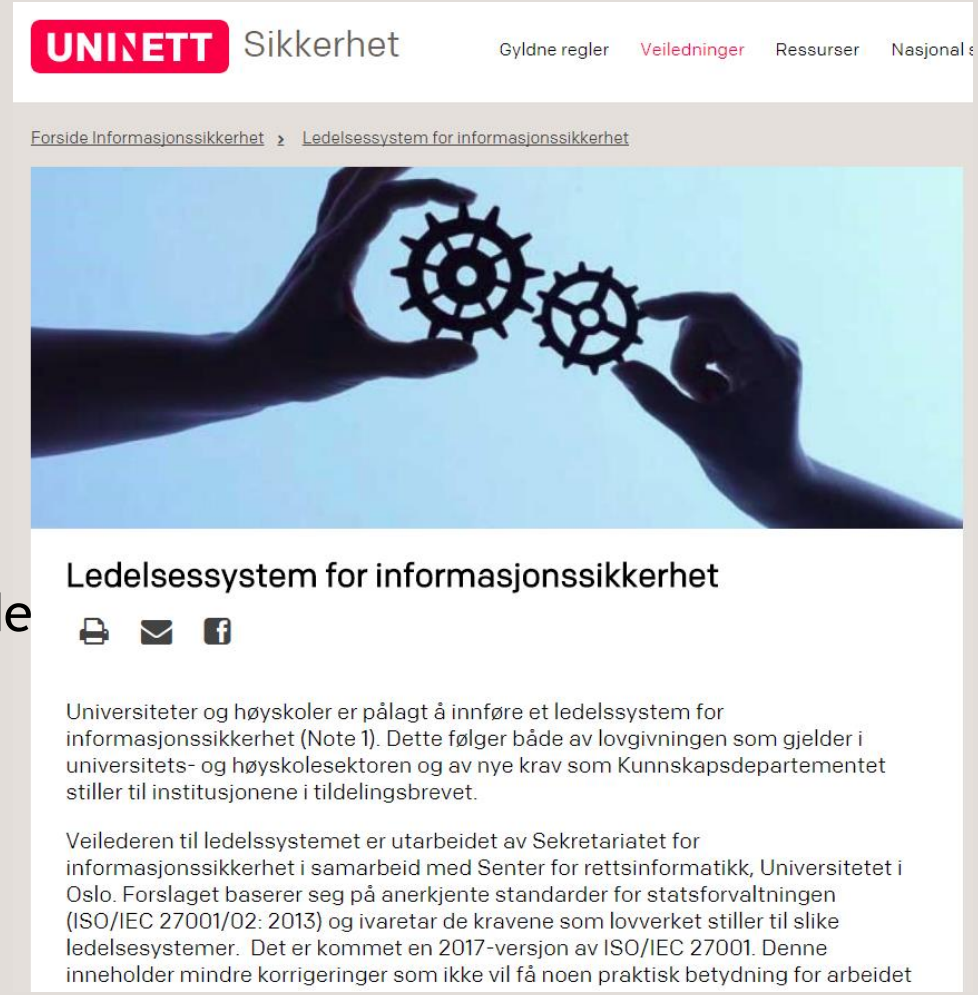
Utfordringer (2013/14)

- Prioritering av ressurser
  - Utilstrekkelig
  - Kompetanse
  - Tid
- Utforming av ledelsessystemet
  - Manglende tilpasning
  - For ambisiøse
  - Terminologi
- Institusjonenes art og organisatoriske utfordringer
  - Komplekse
  - Åpenhet og akademisk frihet
  - Forskerfrihet vs. Sentral styring av informasjonssikkerhet

UNINETT

Ledelsessystem for informasjonssikkerhet i UH

- Tilgjengelig fra 2014
- Studien som bakgrunn
  - Styrende, gjennomførende og kontrollerende
- Veiledning fra sekretariatet på enkeltinstitusjoner
- Fra 2016 et mer systematisk arbeid mot de statlig eide institusjonene



UNINETT

Landet rundt

- 2016 Ledelsessystem og IRT
- 2017 Ledelsessystem og GDPR (pågående)

Status i UH sektoren

- Styrende del på plass hos de fleste
- Gjennomførende del er krevende
  - Hendelseshåndteringsteam på plass
  - Risiko og sårbarhetsvurdering – tja
  - Håndtering av risiko – njeaeii
  - Ressurser? Kompetanse? Holdningsarbeide (sikresiden.no/sikkerhetsmåneden)
- Kontrollerende del er ikke på plass før en har gjennomført ledelsens gjennomgang og startet forbedringsprosessen
- Noen få kan sies å ha et helhetlig ledelsessystem på plass

UNINETT

Konkrete utfordringer

- Tilstrekkelig med ressurser? (noen må faktisk måke snø)
- Kontinuitet i arbeidet med ledelsessystemet
- Integrere eksisterende sikkerhetsarbeid (drift, backup, etc) (SOA?)
- Administrasjonen vs. forskning/utvikling
- Risikovurdering gjort → Ah ☺ «kjør på!»
- Benytte seg i for liten grad av ledelsens «mandat» «… sørge for tilstrekkelige ressurser…»
- Fungerer sikkerhetsorganisasjonen? «Agendapunkt på ledermøter?»
  - Personer med ansvar for IS oppgaver må involveres i arbeidet med å utarbeide sikkerhetsorganiseringen
  - Avgjørende at sikkerhetsorganisasjonen fungerer

UNINETT

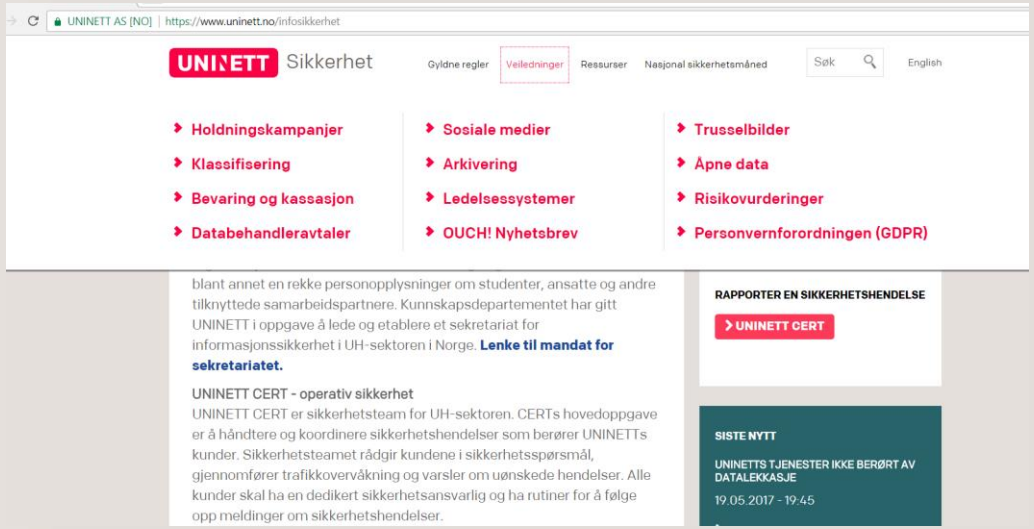
Positivt

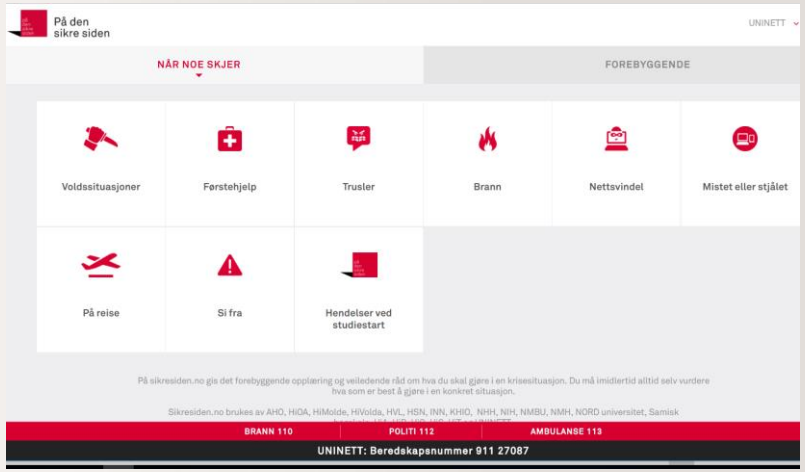
- Informasjonssikkerhet har mediefokus
- Påstand: Vi har mer lederforankring enn noen gang tidligere (vi må bare få dem til å virkelig mene det ;-))
- IRT, hendelseshåndteringsteam på plass i sektoren
- Sikresiden.no en fantastisk dugnadsinnsats!
- Direktører med på nesten alle «Landet rundt» møter
- GDPR vil trolig fremtvinge et kartleggingsarbeid (informasjonsaktiva)

Hvor finner man ting…

- https://uninett.no/infosikkerhet

- https://www.sikresiden.no/





Spørsmål?