

Cybersikkerhet - teknologier og styring

Audun Jøsang

3. utgave 2025

Universitetsforlaget



Oppgaver

Kapittel 18: ISMS – Styring og ledelse av info-sikkerhet

Oppgave 1: Standarder for informasjonssikkerhet

- Se på listen over standarder i ISO 27000 serien, for eksempel på:
<https://www.iso27001security.com/standards>
 - Se på NIST SP800 (Special Publications) serien på:
<https://csrc.nist.gov/publications/sp>
- a. Prøv å identifisere lignende standarder i ISO 27000-serien og i NIST SP800 serien.
 - b. Hva kan være grunner for at ulike organisasjoner utvikler separate lignende standarder?

Oppgave 2: ISMS

- a. Hvordan er standardene ISO/IEC 27001 og ISO/IEC 27002-relatert?
- b. Hva betyr "system" i forkortelsen ISMS (Information Security Management System) (Ledelsessystem for informasjonssikkerhet)?
- c. Hvilken av ovennevnte standarder danner grunnlag for sertifisering, og hvorfor?
- d. Hvordan bør en organisasjon avgjøre hvilke sikkerhetstiltak som skal implementeres?

Oppgave 3: SoA – Statement of Applicability

- a. Hva er Annex A i ISO/IEC 27001?
- b. Hva er SoA (relevanserklæring) (e.g. Statement of Applicability)?
- c. En virksomhet ønsker å benytte en annen tiltaksbank enn ISO/IEC 27002 for å velge informasjonssikkerhetstiltak. Anta at virksomheten ønsker å benytte NSMs Grunnprinsipper for IKT-sikkerhet. Hva må virksomheten gjøre for å utarbeide en SoA?

Oppgave 4: Måling av informasjonssikkerhet

Detaljerte sikkerhetstiltak under hvert prinsipp i NSM-veiledningen er tilgjengelig fra:

<https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/ta-i-bruk-grunnprinsippene/>

- a. Hvordan kan effektiviteten av sikkerhetstiltak måles?
- b. Nedenfor er et eksempel på et sikkerhetstiltak under prinsippet: «*Ha kontroll på identiteter og tilganger*» fra NSM-veiledningen.
Tiltak 2.6.7: «*Bruk multi-faktor autentisering, som smartkort, sertifikater eller engangspassord, for å autentisere brukere.*»
Foreslå metoder for å måle effektiviteten av dette tiltaket.

Oppgave 5: SIS – Styringsgruppe for informasjonssikkerhet

En styringsgruppe for informasjonssikkerhet (SIS) (eller informasjonssikkerhetsråd) er viktig for å sørge for kvalitet og modenhet i ISMS.

- a. Hvilken sammensetning bør SIS ha?
- b. Hvilke oppgaver er passende for SIS?

Oppgave 6: Forvirringen rundt ISMS/LSIS/Internkontroll

LSIS (ledelsessystem for informasjonssikkerhet) og ISMS (styringssystem for informasjonssikkerhet) har samme betydning. I undervisningssektoren benyttes LSIS bl.a. av UiO. LSIS benyttes også av andre statlige virksomheter, bl.a. Sykehuspartner. Standard Norge oversetter ISMS (Information Security Management System) som LSIS. I privat sektor og noen statlige virksomheter som f.eks. NSM benyttes det engelske begrepet ISMS med betegnelsen «Styringssystem for informasjonssikkerhet». I undervisningssektoren benyttes ISMS bl.a. av NTNU. Digdir benytter ofte betegnelsen internkontroll med omtrent samme betydning som ISMS/LSIS. Merk at internkontroll også kan bety «intern sikkerhetsrevisjon».

- a. Gi en forklaring på hvorfor de ulike betegnelsene ISMS/LSIS/Internkontroll benyttes med samme betydning.

Ta en titt på dokumentasjonen av UiO sitt LSIS.

<https://www.uio.no/tjenester/it/sikkerhet/lsis/>

- b. Hva heter de ulike nivåene i hierarkiet av policyer?
- c. Hva menes med «internkontroll» i kapittel 14 av UiO sin dokumentasjon av LSIS. Er det i overensstemmelse med Digdir sin tolkning av internkontroll.

Oppgave 7: NISTs cybersikkerhetsrammeverk

Nevn og forklar hva som menes med hver av de fem sikkerhetsfunksjonene i NISTs cybersikkerhetsrammeverk (og i cyberforsvarsmatrisen).

Oppgave 8: Cyberforsvarsmatrisen for GAP-analyse

Forklar hvordan cyberforsvarsmatrisen kan benyttes til GAP-analyse, dvs. for å vise hvilke sikkerhetstiltak virksomheten har, og hvilke sikkerhetstiltak virksomheten ønsker å implementere for ulike verdier og sikkerhetsfunksjoner.