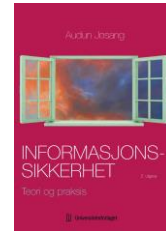


# Informasjonssikkerhet: Teori og praksis

Audun Jøsang

2. utgave 2023

Universitetsforlaget



## Oppgaver

### ***Kapittel 12: ISMS – Styling og ledelse av info-sikkerhet***

#### **Oppgave 1: Standarder for informasjonssikkerhet**

- Se på listen over standarder i ISO 27000 serien, for eksempel på Wikipedia, <https://www.iso27001security.com/>
  - 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) (Ledessystem 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: NSM grunnprinsipper og NIST Cybersecurity Framework**

NSMs "Grunnprinsipper for IKT-sikkerhet" og NIST sitt Cybersecurity Framework har mer eller mindre samme fokus. Se NSM:

<https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf>

Se NIST:

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Denne oppgaven krever ikke å lese de detaljer, bare prinsippene og kategoriene listet opp i tabellen nedenfor.

- a. Bruk tabellen nedenfor til å kartlegge en omtrentlig ekvivalens mellom NSM sine grunnprinsipper og prinsippene i NIST CyberSecurity Framework.

	NSM Grunnprinsipper for IKT-sikkerhet	NIST Cyber Security Framework	
Identifisere og kartlegge	Kartlegg styring, leveranser og systemer	Asset Management	Identify
	Kartlegg enheter og programvare	Business Environment	
	Kartlegg brukere og behov for tilgang	Governance	
Beskytte og opprettholde	Sikker anskaffelses- og utvikling	Risk Assessment	Protect
	Etabler sikker IKT-arkitektur	Risk Management Strategy	
	Ivareta sikker konfigurasjon	Supply Chain Risk Management	
	Beskytt virksomhetens nettverk	Identity Management and Access Control	
	Kontroller dataflyt	Awareness and Training	
	Kontroll på identiteter og tilganger	Data Security	
	Beskytt data i ro og i transitt	Info Protection Processes and Procedures	
	Etabler evne til gjenoppretting av data	Maintenance	
	Sikkerhet i endringshåndtering	Protective Technology	
Oppdage	Oppdag og fjern kjente sårbarheter	Anomalies and Events	Detect
	Etabler sikkerhetsovervåking	Security Continuous Monitoring	
	Analys data fra sikkerhetsovervåking	Detection Processes	
	Gjennomfør inntrengningstester		
Håndtere og gjenopprette	Forbered håndtering av hendelser	Response Planning	Respond
	Vurder og klassifiser hendelser	Communications	
	Kontroller og håndter hendelser	Analysis	
	Evaluer og lær av hendelser	Mitigation	
		Improvements	
			Recover
	Recovery Planning		
	Improvements		
		Communications	

- b. Etter kartleggingen, vurder hvor like NSM-prinsippene og ISO-kategoriene er.  
c. Hvilken nytte har det at NSM sine grunnprinsipper og NIST sin Cyber Security Framework er relativt like.

## Oppgave 5: Kategorisering av informasjonssikkerhetstiltak

Standarder og veiledere som beskriver informasjonssikkerhetstiltak benytter ulike kategoriseringer av sikkerhetstiltakene. Tre vanlige kategoriseringer er:

- Prosesskategorier (kartlegge > beskytte > detektere > respondere > gjenopprette)
- Generelle domenekategorier (organisatoriske, personell, fysiske, og teknologiske tiltak)
- Operasjonelle kategorier (f.eks. tiltak for tilgangskontroll, data/media-beskyttelse, IAM, nettverkssikkerhet, system/applikasjonssikkerhet, hendelsesrespons, opplæring, leverandørsikkerhet etc.)

For hver standard/veileder nedenfor, spesifiser hvilken kategorisering den benytter.

- ISO/IEC 27002:2022 Information security controls
- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations
- NSMs Grunnprinsipper for IKT-sikkerhet
- NIST Cyber Security Framework
- CIS Critical Security Controls

## Oppgave 6: Måling av informasjonssikkerhet

Detaljerte sikkerhetstiltak under hvert prinsipp i NSM-veiledningen er tilgjengelig fra:  
<https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/>

- 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 7: 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 8: 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/lis/>

- 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.