



Ledelsesforankring - Strategi



Dr. Dinh Uy Tran

Head of GRC – Gritera & Senior lecturer – UiO

Gritera Security – Head of GRC & Director

UiO – Førstelektor og forsker (Deltid)

Cappelen Damm Akademisk – Forfatter

Sykehuspartner – Spesialrådgiver

UiO / Sykehuspartner – Stipendiat

Martina Hansen Hospital – Innleid CISO

Sykehuspartner – Rådgiver

Sykehuspartner – Teamleder

Sykehuspartner – Spesialkonsulent

Sykehuspartner – Operativt ansvarlig

Utdanning

UiO – Doktorgrad i informasjonssikkerhet

UiO – Mastergrad i IT og Ledelse

UiO – Bachelorgrad, informatikk

Sertifiseringer

CISSP – Certified Information Systems Security Professional

CISM – Certified Information Security Manager

CRISC – Certified in Risk and Information Systems Control

PECB – Certified Trainer

PECB – Certified Chief Information Security Officer (CISO)

ISO/IEC 27001 – Senior Lead Implementer

ISO/IEC 27005 – Senior Lead Risk manager

ISO 31000 – Senior Lead Risk Manager

CISSP ISSMP – Information Systems Security Management Professional



Agenda

- Ledelsesforankring
- Strategi
- Oppsummering

Ledelsesforankring



Lederskap og forpliktelse / Management commitment (ISO/IEC 27001:22; Krav 5.1) =

Ledelsesforankring

Ledelsesforankring

Ledelsesforpliktelse

Brukt om hverandre



Hva er forskjellen mellom ledelsesforankring,- støtte og- forpliktelse?



Forståelse for begrepene kan bidra til å spisse strategiene bedre

Ledelsesforankring

1. Ledelsesforankring

- Sterkt involvering
- Sikre omforent mål

2. Ledelsesstøtte

- Gi støtte for å sikre at sikkerhetsarbeidet lykkes
- Kortsiktig – støtte ved behov

3. Ledelsesforpliktelse

- Bundet til å gjøre
- Støtte er integrert del av jobben til ledelsen
- Formålet er å sikre forpliktelse over tid (langsiktig)

1.Ledelsesforankring



2.Ledelsesstøtte



3.Ledelsesforpliktelse

Kilde: www.snl.no

Strategi

1. Hva slags støtte trenger du fra ledelsen?



2. Hvorfor skal ledelsen hjelpe deg?



3. Hvem sin støtte og forpliktelse trenger du i fra?



4. Hvordan skal du få ledelsesstøtte- og forpliktelse?



5. Når har du fått ledelsesforpliktelse?

1. Hva slags støtte trenger du fra ledelsen

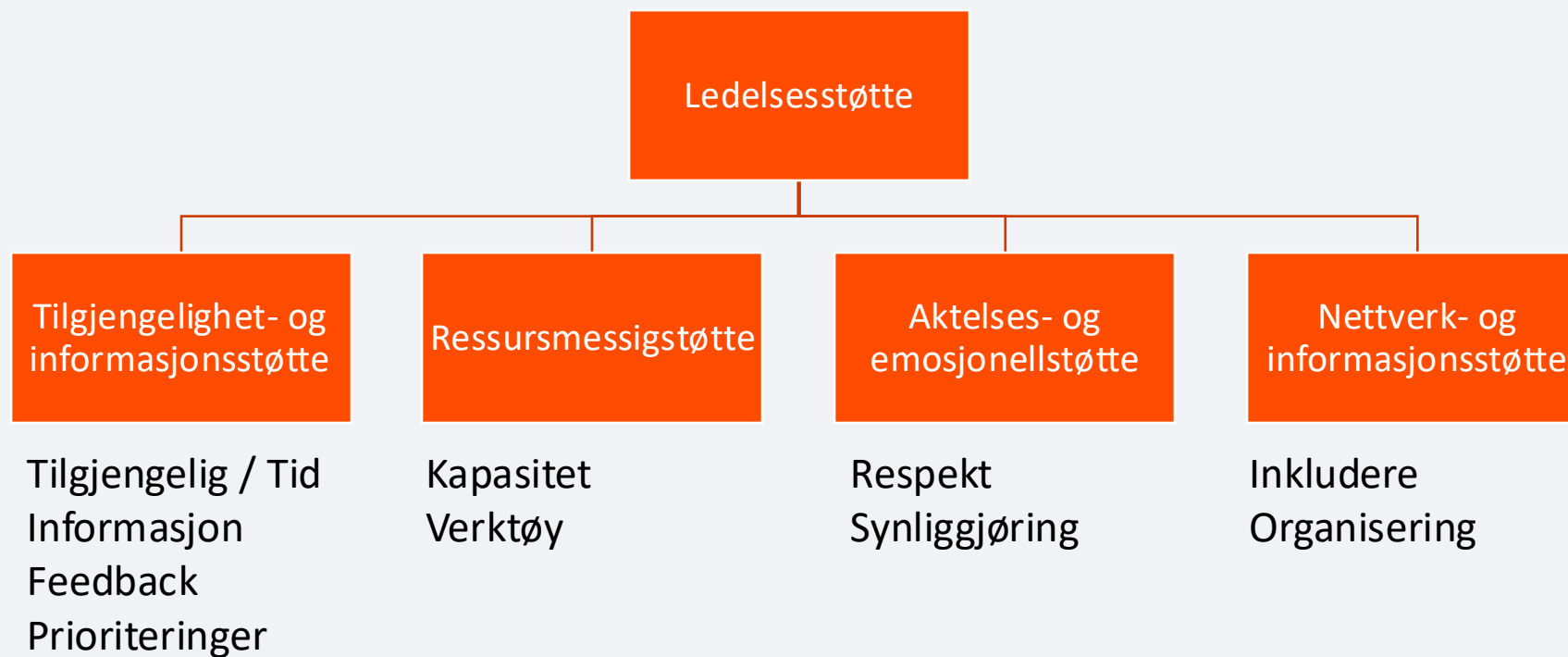
1. Hva slags støtte trenger du fra ledelsen?

2. Hvorfor skal ledelsen hjelpe deg?

3. Hvem sin støtte og forpliktelse trenger du i fra?

4. Hvordan skal du få ledelsesstøtte- og forpliktelse?

5. Når har du fått ledelsesforpliktelse?



Hatlem, Thea Fritzvold (2024)

2. Hvorfor skal ledelsen hjelpe deg?

1. Hva slags støtte trenger du fra ledelsen?

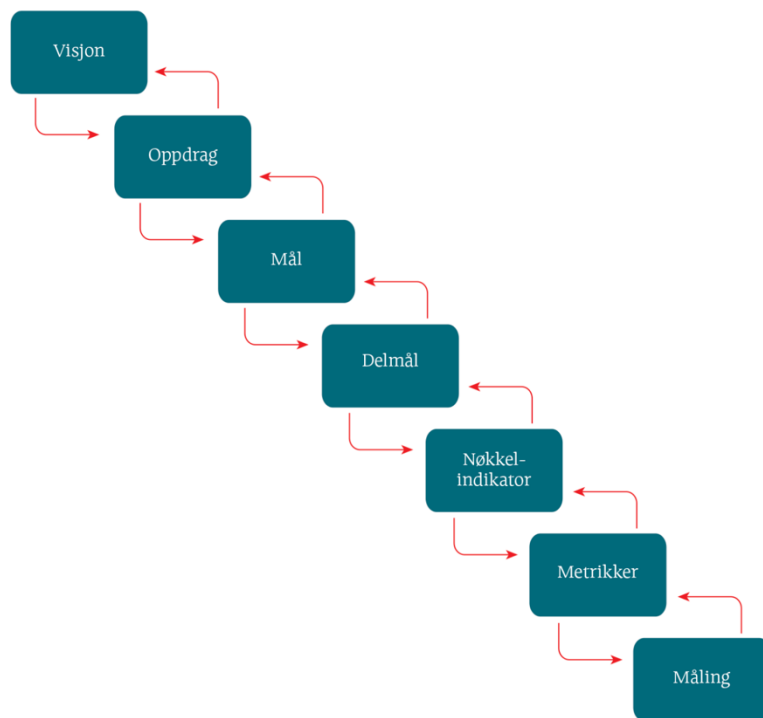
2. Hvorfor skal ledelsen hjelpe deg?

3. Hvem sin støtte og forpliktelse trenger du i fra?

4. Hvordan skal du få ledelsesstøtte- og forpliktelse?

5. Når har du fått ledelsesforpliktelse?

- Felles mål og retning, og du kan bidra!



Figur 3.6.3 – Fra måling til visjon

Saman for ein enklare digital kvardag.

Samfunnsoppdraget til Digdir er å vere regjering sitt fremste verktøy for raskare og meir samordna digitalisering av samfunnet

Samordnar og pådrivar i offentleg sektor sitt arbeid med førebyggjande informasjonssikkerheit

Felles fagspråk gjennom veileder for styringssystem for informasjonssikkerhet

Mål: 80 % av virksomheter i offentlig sektor benytter DigDirs veiledere

$\text{Antall virksomheter benytter DigDirs veiledere} / \text{Totalt antall virksomheter} * 100$

Antall virksomheter, antall som benytter Digidirs veiledere, antall ISO27001 sertifiserte og etc

Hvem sin støtte og forpliktelse trenger du i fra?

1. Hva slags støtte trenger du fra ledelsen?

2. Hvorfor skal ledelsen hjelpe deg?

3. Hvem sin støtte og forpliktelse trenger du i fra?

4. Hvordan skal du få ledelsesstøtte- og forpliktelse?

5. Når har du fått ledelsesforpliktelse?



Top-Down



Mye fokus på top-down
Hva gjør du når det ikke går?



I flere tilfeller kan andre
interessenter være dine
støttespillere og påvirke
toppledelsen

Kan kjøre en kombinasjon
av tilnærmingene

Nøkkelen er god
interessentanalyse

Bottom-Up

1. Hva slags støtte trenger du fra ledelsen?

2. Hvorfor skal ledelsen hjelpe deg?

3. Hvem sin støtte og forpliktelse trenger du i fra?

4. Hvordan skal du få ledelsesstøtte- og forpliktelse?

5. Når har du fått ledelsesforpliktelse?

4. Hvordan skal du få ledelsesstøtte- og forpliktelse?

Those working in technical fields like IT and Information Security must **"speak their language."** They must be forced to **speak a common language** in the **business**, where specialized terminology and shared assumptions are either removed or carefully spelled out (Whitman & Mattord, 2014).

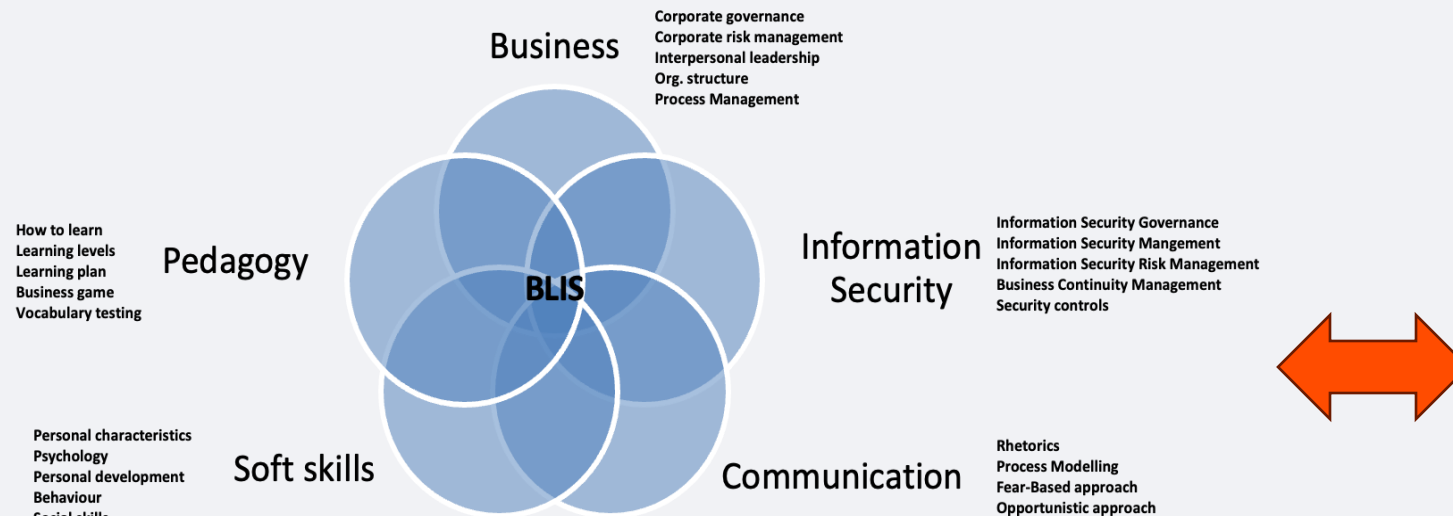
CISO who reports to the CEO should be an **IT security expert** and a **business strategist** capable of engaging with the CEO using **business language** (Karanja, 2017)

The information security is a part of information risk management, which in turn has a place in the business risk management. This shift in approach enables clever information security professionals **talk similar language as business people**; those who actually bring money to the company (Jirasek, 2012).

The CISO is expected to have broad security knowledge in each of these areas are important to the business. The ability to work up and down the organization, **translating technical jargon into a language appropriate for the CEO, CIO, business executives, middle management, end users, and external parties** is an essential skill (Fitzgerald, 2007).

Business acumen is also necessary to **communicate technical risks in language that nontechnical people in the business can grasp**, and to understand that some risks are worth taking. Risk-taking is fundamental to business. Without it, no business value would be created (Harkins, 2016).

Ledelsesspråket for informasjonssikkerhet



(Business language for Information Security (BLIS), Tran & Jøsang 2023)

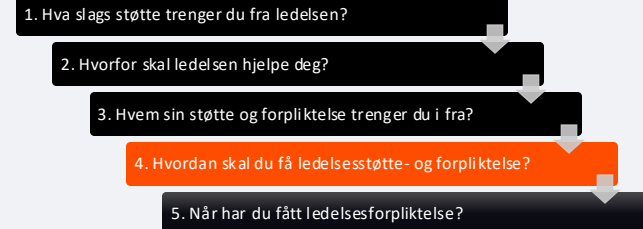
1. Hva slags støtte trenger du fra ledelsen?
2. Hvorfor skal ledelsen hjelpe deg?
3. Hvem sin støtte og forpliktelse trenger du i fra?
4. Hvordan skal du få ledelsessøtte- og forpliktelse?
5. Når har du fått ledelsesforpliktelse?



Figur 2.5.1 – Metode for ledelsesspråk

Er det nok å snakke samme språk?

- Nei!
 - Strategier for å anvende språket



Kommunikasjon



1. Fryktbasert
2. Løsningsorientert

Tilpasses målgruppen

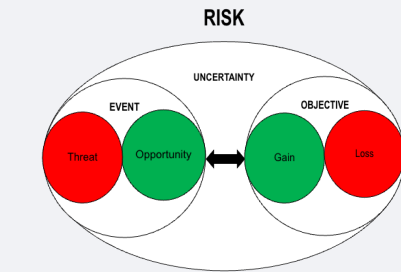
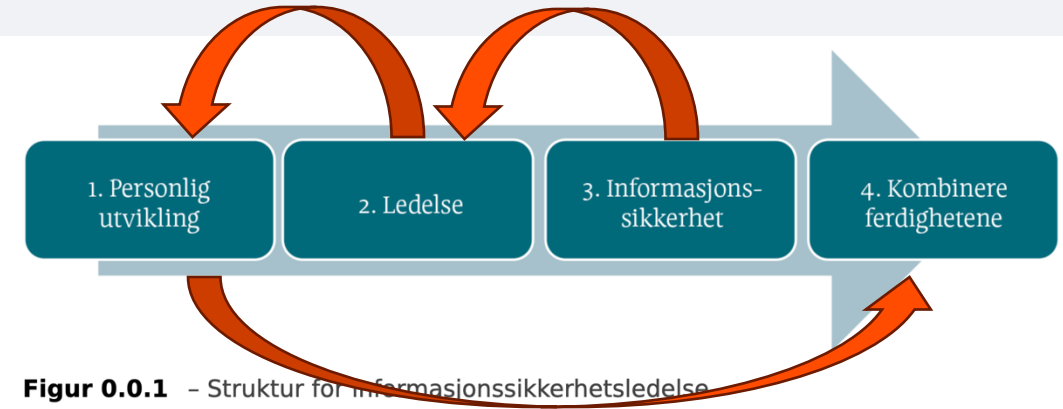


Table 2. Risk description strategies.

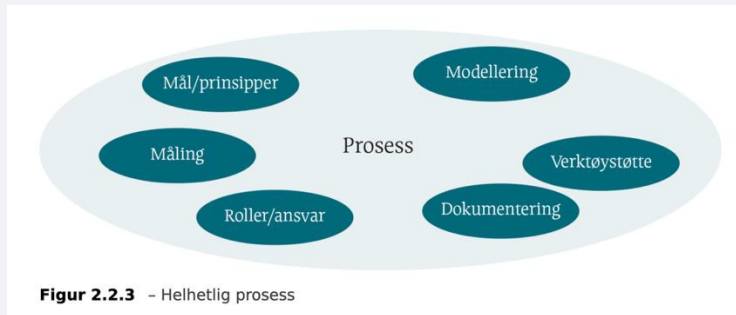
Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>



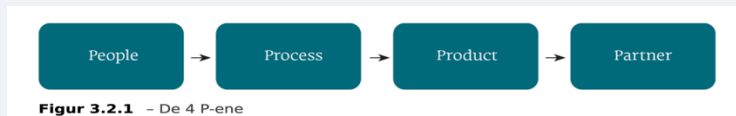
Figur 0.0.1 – Struktur for informasjonssikkerhetsledelse



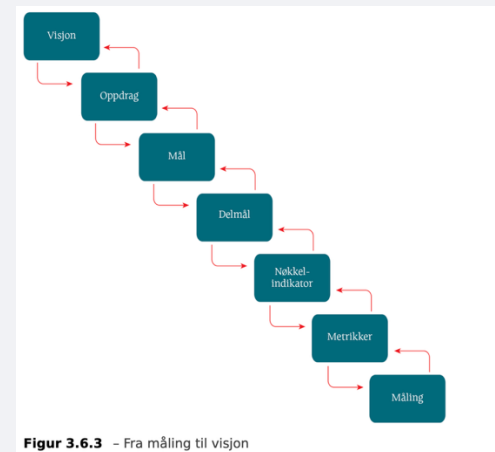
Struktur og fagligdybde



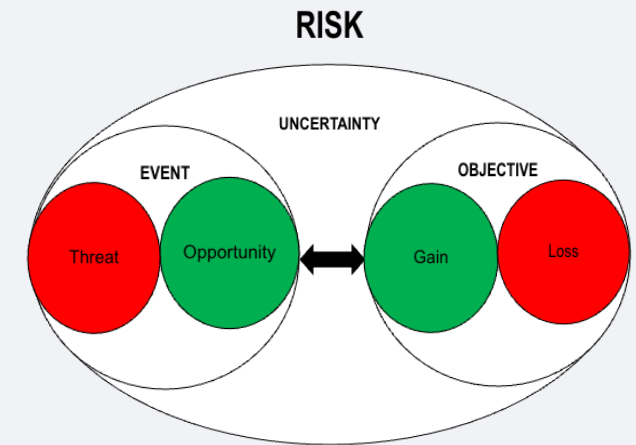
Organisere og strukturere



Estimere kostnader



Knytte arbeidet mot virksomhetens mål



Oversikt over risiko og muligheter
Håndtere dem for å nå mål

Tillit



Når har du fått ledelsesforpliktelse?

1. Hva slags støtte trenger du fra ledelsen?

2. Hvorfor skal ledelsen hjelpe deg?

3. Hvem sin støtte og forpliktelse trenger du i fra?

4. Hvordan skal du få ledelsessøtte- og forpliktelse?

5. Når har du fått ledelsesforpliktelse?

Når har du fått ledelsesforpliktelse?

Kjennetegn

Beslutninger fra
topplederen blir
logget og håndtert

Ledelsesgjennomgang
er en del av en prosess

Kommunisert gjennom
policy

Definert risikoeierskap
og "accountability"

Kjenner
sikkerhetsrisikoer og
sine tjenester

Risiko blir håndtert
kontinuerlig

Sikkerhetsopplæring er
prioritert

Oppsummering

- Diskutert forskjellen mellom ledelsesforankring,- støtte og- forpliktelse
- Rammeverk:

1. Hva trenger du fra ledelsen?

2. Hvorfor skal ledelsen hjelpe deg?

3. Hvem sin støtte og forpliktelse trenger du i fra?

4. Hvordan skal du få ledelsesstøtte- og forpliktelse?

5. Når har du fått ledelsesforpliktelse?

Tilpasses til situasjonen:

1. Kommunikasjon
2. Strukturert tilnærming

Bygge tillit

Lederstøtte er like viktig som ledelsesstøtte!

Litteraturliste

- Tran, D.U. (2023). Informasjonssikkerhetsledelse – En holistisk tilnærming. Cappelen Damm Akademisk
- Tran, D. U., Jøsang, A., Hagen, J., og Sigrid Haug Selnes, S. H. (2023) An Opportunity-Based Approach to Information Security Risk.
- NS-EN ISO/IEC 27001:2023: Informasjonssikkerhet, cybersikkerhet og personvern – Ledelssystemer for informasjonssikkerhet
- Tran & Jøsang (2023). Business Language for information security. HAISA 2023.
- Hatlem, Thea Fritzvold (2024). Ledelsesstøtte for informasjonssikkerhetsledere i Helse Sør-Øst

Takk for oppmerksomheten!



Dinh Uy Tran, PhD

Head of GRC & Director @ Gritera Security | Senior
lecturer & Researcher @ UiO | Author |



Kontakt:

uy.dinh.tran@gritera.com

Deler tanker og erfaringer om:

- Informasjonssikkerhetsledelse
- Sikkerhets- og risikostyring