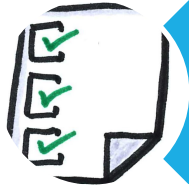


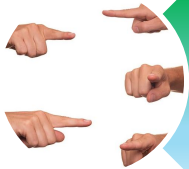
Kva gjer vi for å sikre oss mot digitale truslar ?



Kvifor



Kva



Kven har
ansvaret

Vigleik Hustadnes
CISSP, CISM
Leiar informasjonssikkerheit
Tussa IKT

En av fire norske virksomheter tror de er nærmest immune mot dataangrep



«Vi har lite konfidensiell info»

«det skjer nok ikkje oss»

«Vi greier oss ei stund uten data»

«vi bør jo ta tak i dette»

«Dette skal opp i neste styremøte»



«Risikoen øker ved at vi digitaliserer verdiene våre samtidig som trusselaktørene blir mer avanserte»



NASJONAL
SIKKERHETSMYNDIGHET

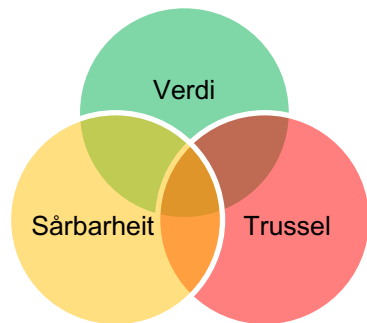


NASJONAL
SIKKERHETSMYNDIGHET

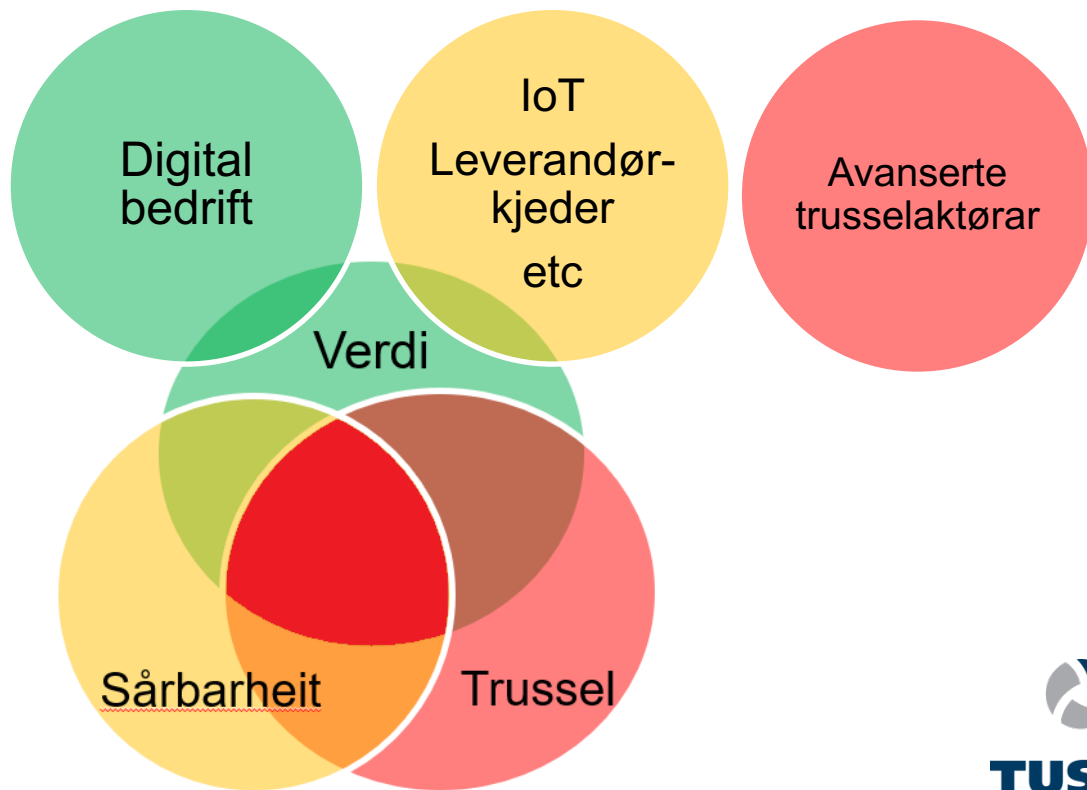
RISIKO 2019
Krafttak for et sikrere Norge



Digitalisering aukar cyber-risiko



Sannsynlighet * Konsekvens



Spesielt er SMB-markedet ekstra sårbart





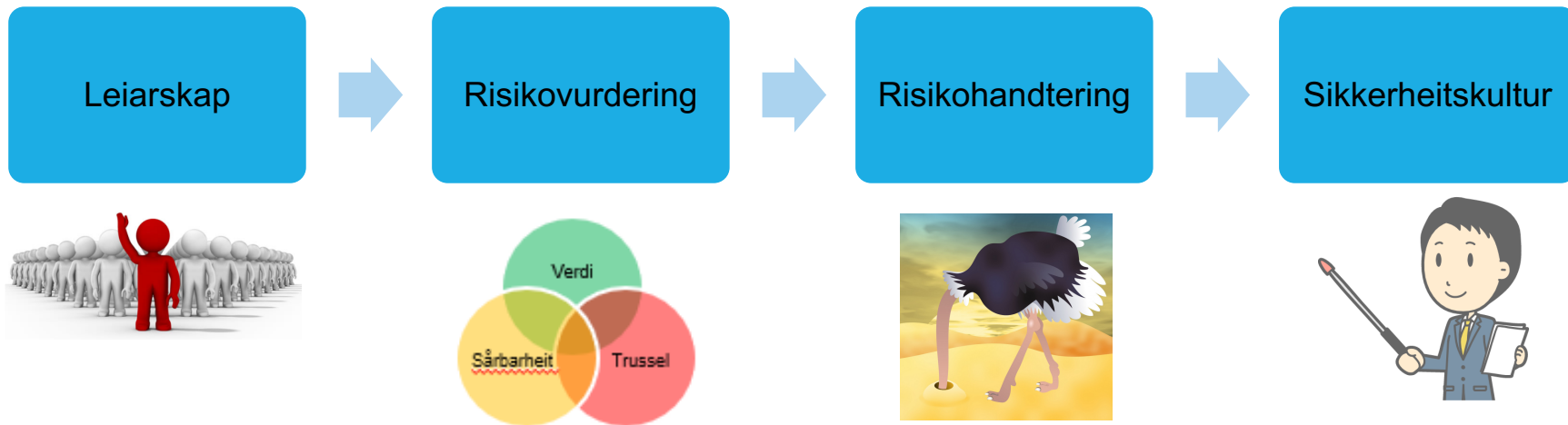
Svakheiter i norske bedrifter

1. Ufullstendig risikobilde
2. Manglende sammenheng mellom tiltak
3. Svakt personellsikkerhetsarbeid
4. Økende digitalisering uten tilsvarende sikkerhet
5. Dårlig oversikt over hva som bør sikres
6.





Bedrifter må ta tak i



Leiarskap

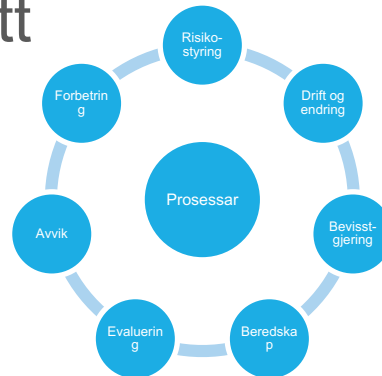
- Strategi
 - Forretningsmål, sikkerheitsmål
- Policy
 - Risikovilje, ansvar og roller
- Ressursar og budsjett
- Rapportering
- Kontinuitet



Styre

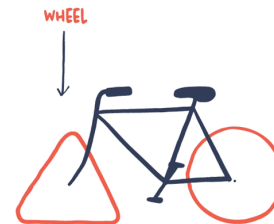


Dagleg leiar



Jobb systematisk

Lytt til erfarne fjellfolk



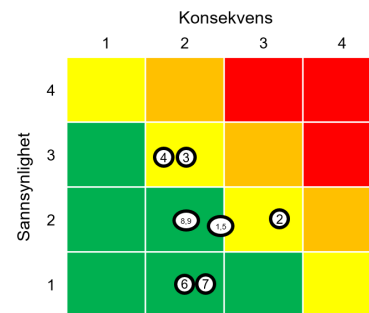
- Nasjonal strategi for digital sikkerhet
- NSM – Grunnprinsipper for IKT-sikkerhet
- Difi* – Internkontroll Informasjonssikkerhet
- NIST five functions
- Cloud Security Alliance Security Guidance
- ISO27001
- SANS – Security Awareness Maturity Model



Tegn ditt eige risikobilde

- Verdier
 - «kva lever vi av»
- Konsekvensar
 - Forretningsrisiko
 - «det verste som kan skje oss?»

1. Ufullstendig risikobilde
5. Dårlig oversikt over hva som bør sikres



Risikohandtering

Risikohandtering



- Akseptere
- Unngå
- Redusere sannsynlighet
- Redusere konsekvens
- Overføre

Aktuelle tekniske tiltak

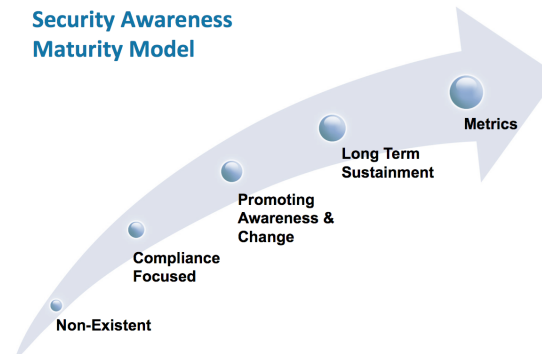
- *Oppgrader og oppdater*
- *Tofaktor-autentisering*
- *Identitets-styring/SSO*
- *Klientadministrasjon*
- *Sikring av Office 365*



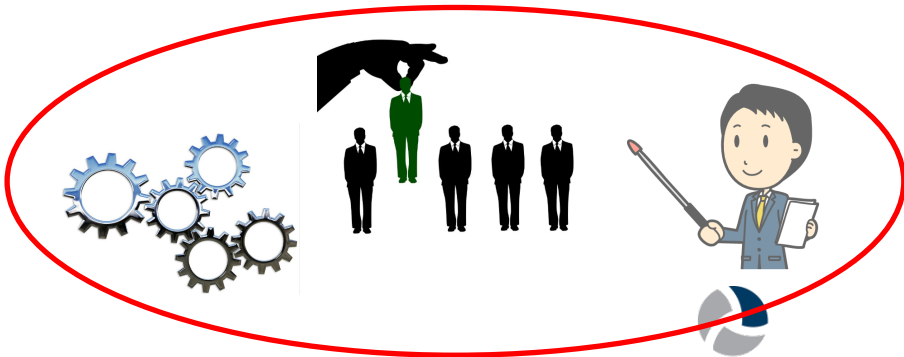
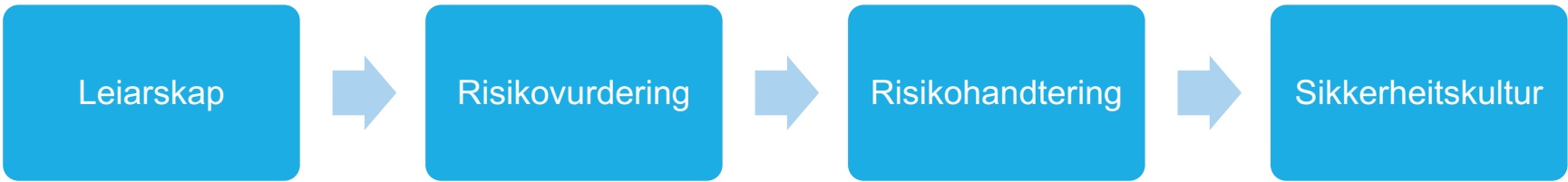
Sikkerheitskultur

- Del av organisasjonskulturen
- Leiinga sine krav, våre felles mål
- Generell bevisstgjøring/opplæring
- Testing, konkurranse og måling

Security Awareness Maturity Model



Kven har ansvaret



Risikoreduserande tiltak



Ansvar for sikringstiltak



Styret



Dagleg leiar



IT-sjef



CISO

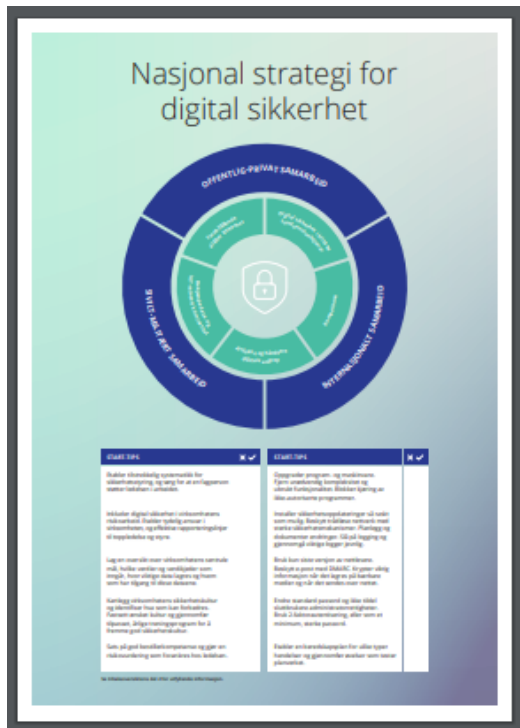
- HR-sjef
- Økonomisjef
- Kommandolinje

- SaaS-leverandør
- PaaS-leverandør
- Huseigar

Nasjonal strategi for digital sikkerhet

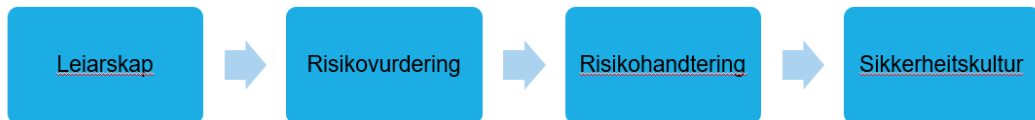


Tiltaksoversikt del 2 - for bedrifter



1. Ledelse
2. Risikostyring
3. Kartlegg verdikjeder, informasjonsverdier etc
4. Inkluder digital sikkerhet i virksomhetskulturen
5. Leverandørkontroll
6. Sikker konfigurasjon
7. Kontroll på nettverk og systemkomponenter
8. E-post og websikkerhet
9. Tilgangskontroll
10. Hendelsesberedskap

Leierskap



TUSSA - MED KRAFT TIL Å SKAPE



Modning og læring – ISO27001

MOTIVASJON



SPRÅK



NYTTEVERDI



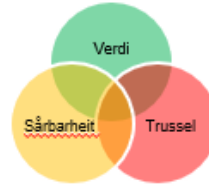
«WHOLISTIC APPROACH»





Facebook profile page for Alexandra Nilsen. The browser address bar shows "www.facebook.com/profile.php?id=100002032617882&ref=ts". The profile name is "Alexandra Nilsen" with "ete" next to it. Her birth date is "Fødd 8. februar 1995". There are several photos of her, including a large one with a grey scarf. A post from "Aksel Sørensen" is visible, dated "Sundag kl. 22:05", with the text "Aldri hatt sex, kyssa, rota i skolen, fått en dårlig karakter, vært sur, kommet for tror meg". The page also shows a "Sponsa" section with an advertisement for "Noel Gallagher Soloalbum" and "Åpningsfest for Mestersykel.no". The Windows taskbar at the bottom shows the time as 16:54 on 09.11.2011.

Kjelder



<https://threatpost.com/4b-records-exposed-breaches-2019/147446/>
<https://www.bleepingcomputer.com/news/security/russian-apt-abuses-iot-devices-to-infiltrate-corporate-targets/>
<https://www.nsm.stat.no/aktuelt/risiko-2019/>
<https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf>
<https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>
<https://www.trygghandel.no>

<https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
<https://pixabay.com>
<https://www.needpix.com/>

<https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/plakat-nasjonal-strategi-for-digital-sikkerhet.pdf>
<https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/grunnprinsipper-for-ikt-sikkerhet-1-1/>
<https://internkontroll-infosikkerhet.difi.no/>
<https://www.nist.gov/cyberframework>
<https://cloudsecurityalliance.org/artifacts/security-guidance-v4/>
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>
<https://www.sans.org/security-awareness-training/blog/security-awareness-maturity-model>
<https://lovdata.no/dokument/SF/forskrift/2003-05-21-630>
<https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgstjenesten>
<https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/kraftberedskapsforskriften-har-tradt-i-kraft/>
[http://www.imo.org/en/OurWork/Security/Guide to Maritime Security/Pages/Cyber-security.aspx](http://www.imo.org/en/OurWork/Security/Guide%20to%20Maritime%20Security/Pages/Cyber-security.aspx)
<https://norsis.no/nasjonal-undersokelse-id-tyveri/>