Digdir

digdir.no

Sårbarheter og risiko ID-porten og MinID

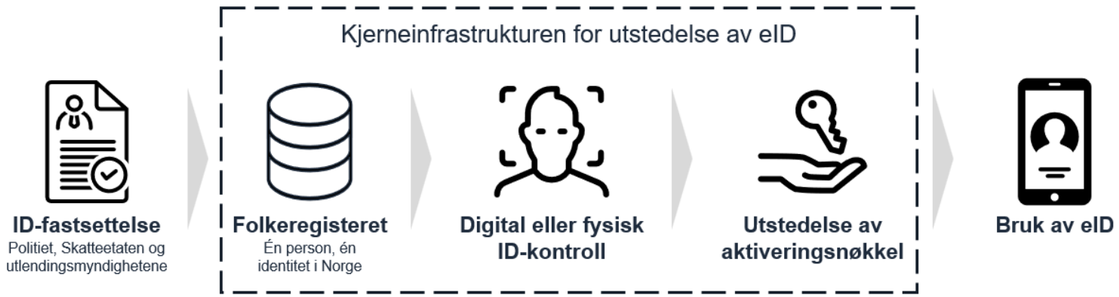
NIFS 27 november 2024

sbr@digdir.no

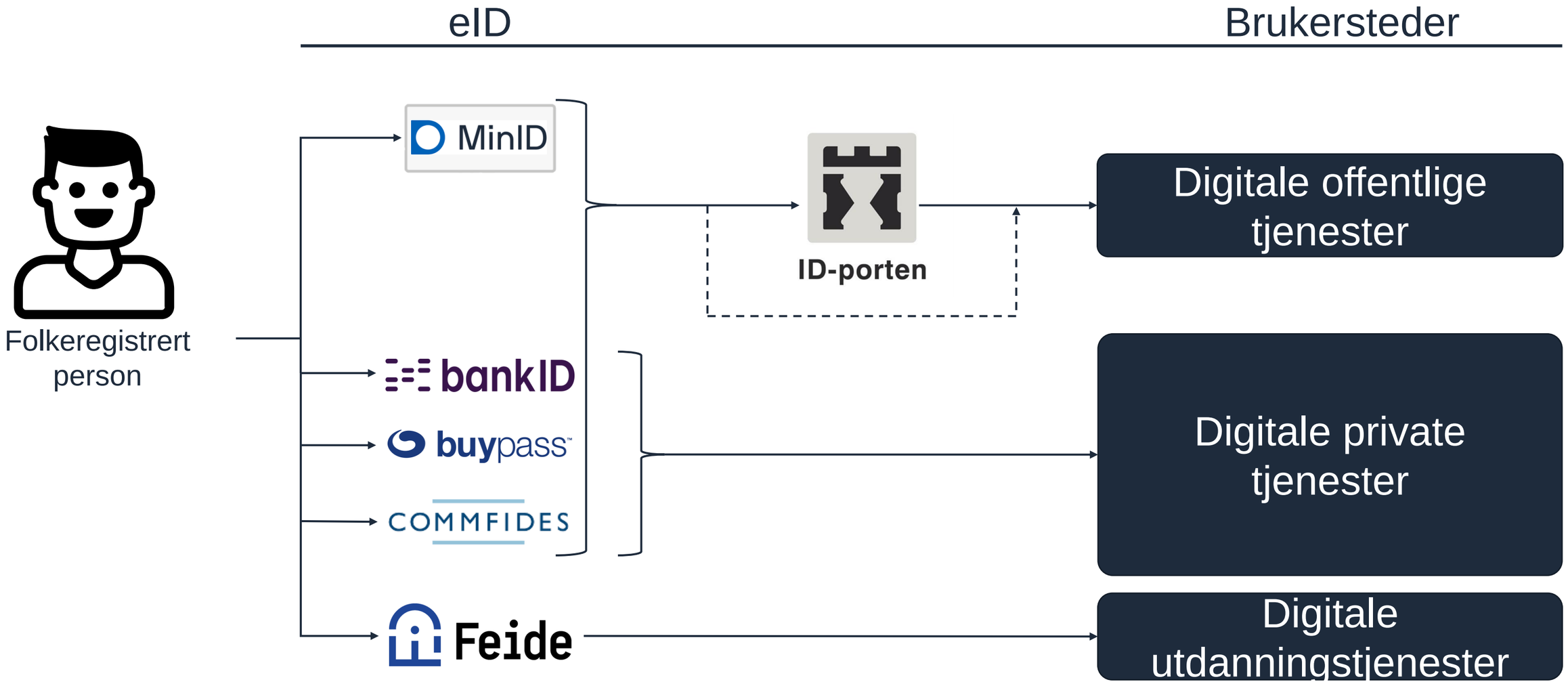
Bakgrunn

Nasjonal eID-infrastruktur - suksesskriterier

- **Samarbeid**: Utstedelse og bruk av eID involverer mange sektorar og krev samarbeid offentleg/privat
- **Risikostyring**: Handtere risiko til det beste for brukarar, tjenesteeigarar og forvaltar
- **Inkludering**: Unngå ekskludering, senke terskelen for å få med fleire



eID i offentleg sektor i dag



eIDAS og risiko

- eIDAS-forordningen: Førende for bruk av eID i offentlig sektor (og til dels også privat)
- Rammeverk for tillit: Krav til eID-løsninger, referanse for risikovurderinger

Nivå	Tillitsnivå	Nivå av tekniske tiltak
Lavt	Begrenset grad av tillit til en persons påståtte identitet	Formål å redusere risiko for misbruk eller endring av identitet
Betydelig	Betydelig grad av tillit til en persons påståtte identitet	Formål å betydelig redusere risiko for misbruk eller endring av identitet
Høyt	Høyere grad av tillit til en persons påståtte identitet enn sikkerhetsnivå betydelig	Formål å hindre misbruk eller endring av identitet

Digdir

digdir.no

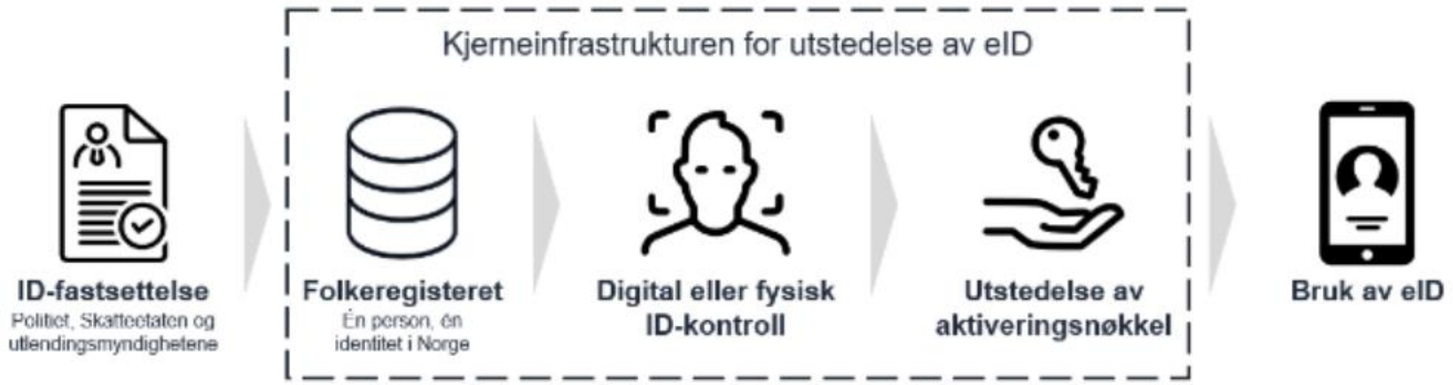
eID trusler og sårbarheter

Trusler i ulike faser ved bruk av eID

Identitetsfastettelse
Folkeregisteret

Utstedelse
av eID-bevis

Bruk
av eID



Trusler i ulike faser ved bruk av eID

Identitetsfastettelse
Folkeregisteret

- Fiktiv identitet
  - Personalia til en ikke-eksisterende person
- Falsk identitet
  - Personalia til en eksisterende person

Utstedelse
av eID-bevis

- Personen bruker falskt ID-bevis
- Personen bruker usant ID-bevis
- Personen bruker ekte ID-bevis, men samsvarskontrollen (person-id-bevis) er svak
- Sårbarheter i utstedelsesprosess (f.eks post)

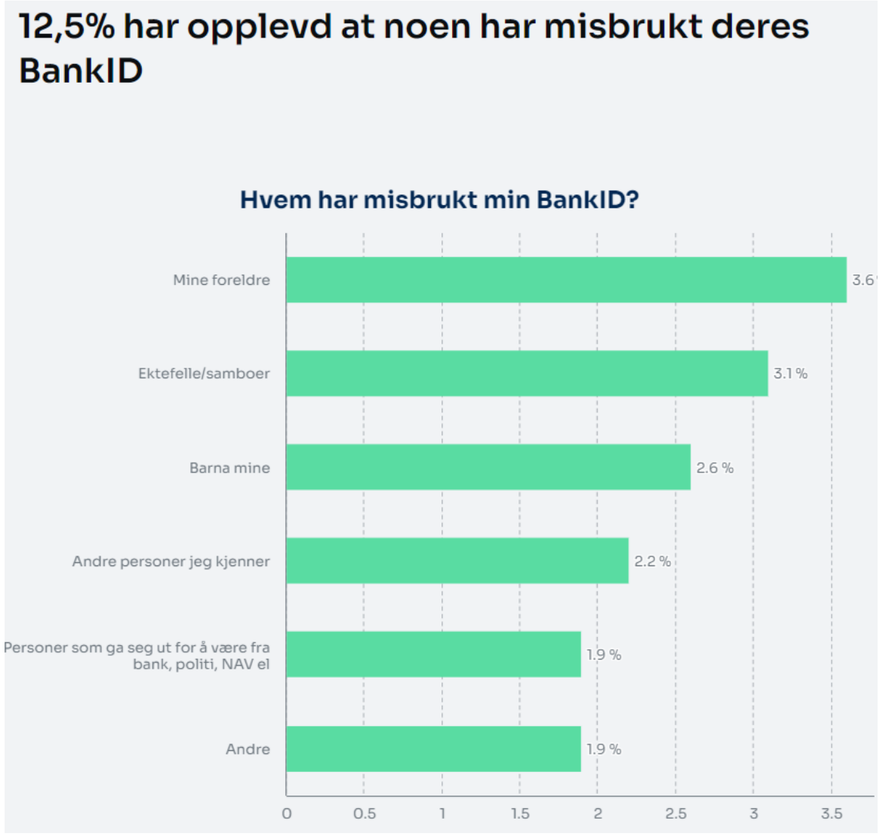
Bruk
av eID

- Fullmaktsmisbruk
- Utleie, utlån
- Utnyttelse av tillitsforhold/sosial manipulasjon
- Tjuveri
- Kopiering
- Resetting (driftspersonell)
- Trojanere, MITM

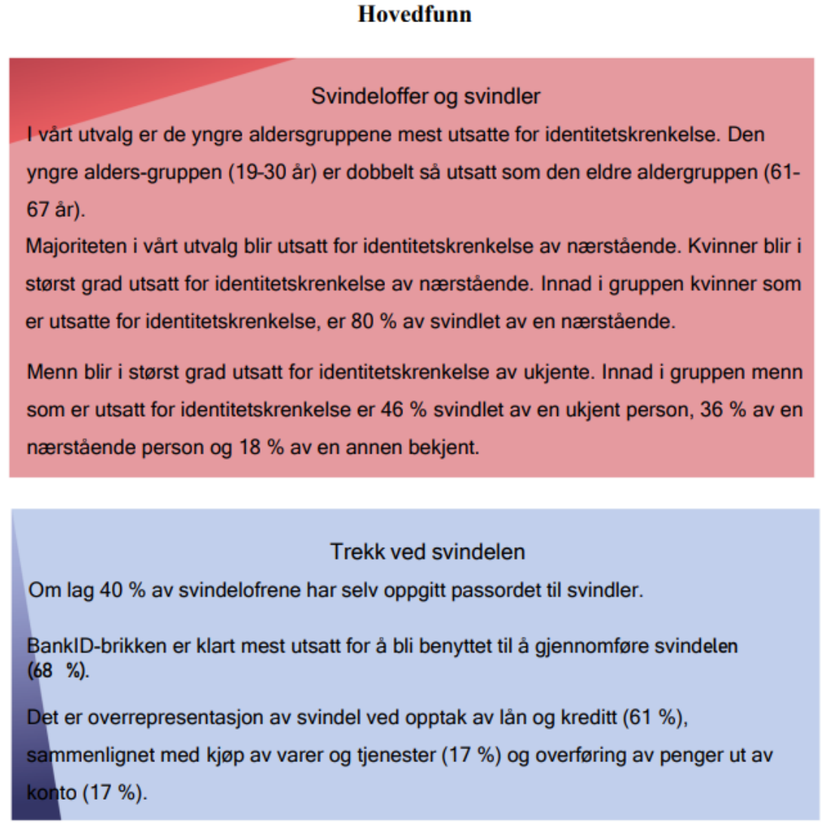
Sårbarheter

- Utbredelse
  - Unge: Vanskelig tilgjengelig prosess for nivå høyt, samtykke, kunnskap
  - Utlendinger: Mangler ID-bevis / folkeregistrert ID, bank sine krav
- Identifikasjon
  - Dublerte IDer i folkeregisteret (tiltak: unik/kontrollert)
- Utstedelse
  - Revokerte ID-bevis (tiltak: bruk av ToVE)
  - Sammenligning av ID-bevis og fysisk person (tiltak: maskinell gjenkjenning av ID-bevis & biometri)
- Bruk
  - Fysisk nærhet, nærstående (tiltak: opplæring, biometri)
  - Utlån eller utleie av e-ID i ulike fullmaktsforhold (tiltak: biometri)
  - Brukerutstyr med sårbarheter, tekniske angrep (tiltak: kreve "siste versjon")

Størst risiko i bruksfasen: Mellommenneskelige forhold



NORSIS, "Nordmenn og digital sikkerhetskultur" (2023)



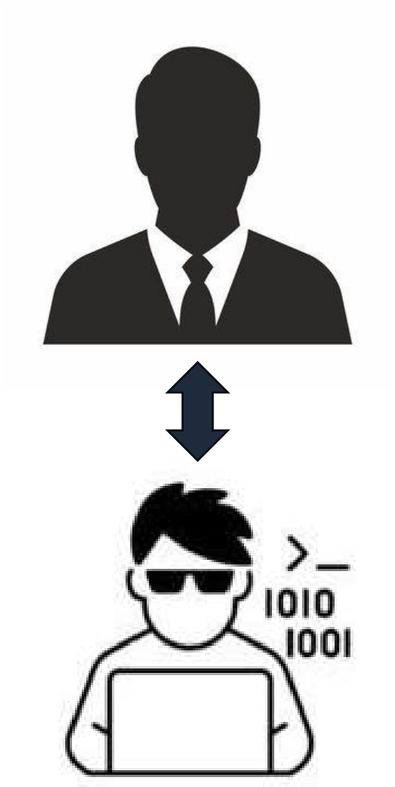
UIO, "Rapport om misbruk av eID", SODI 1/22 (2022)

Digdir

digdir.no

Risikolandskap for ID-porten og MinID

Risikolandskap

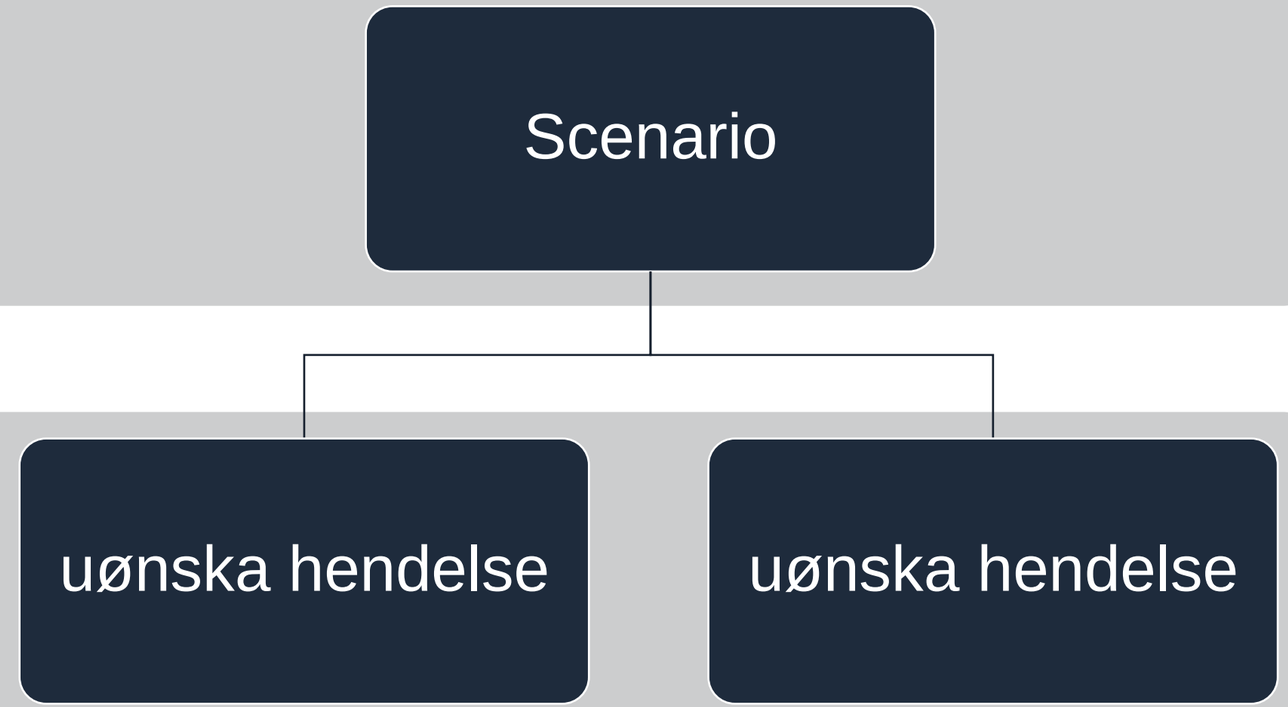


”Det som leiinga fryktar"

- overordna
- max 10 stk per produkt
- tvinger leiinga til å “løfte seg”

“Kva kan faktisk gå gale?”

- konkrete hendingar som kan motverkast med konkrete tiltak
- unngå "banaliteter"

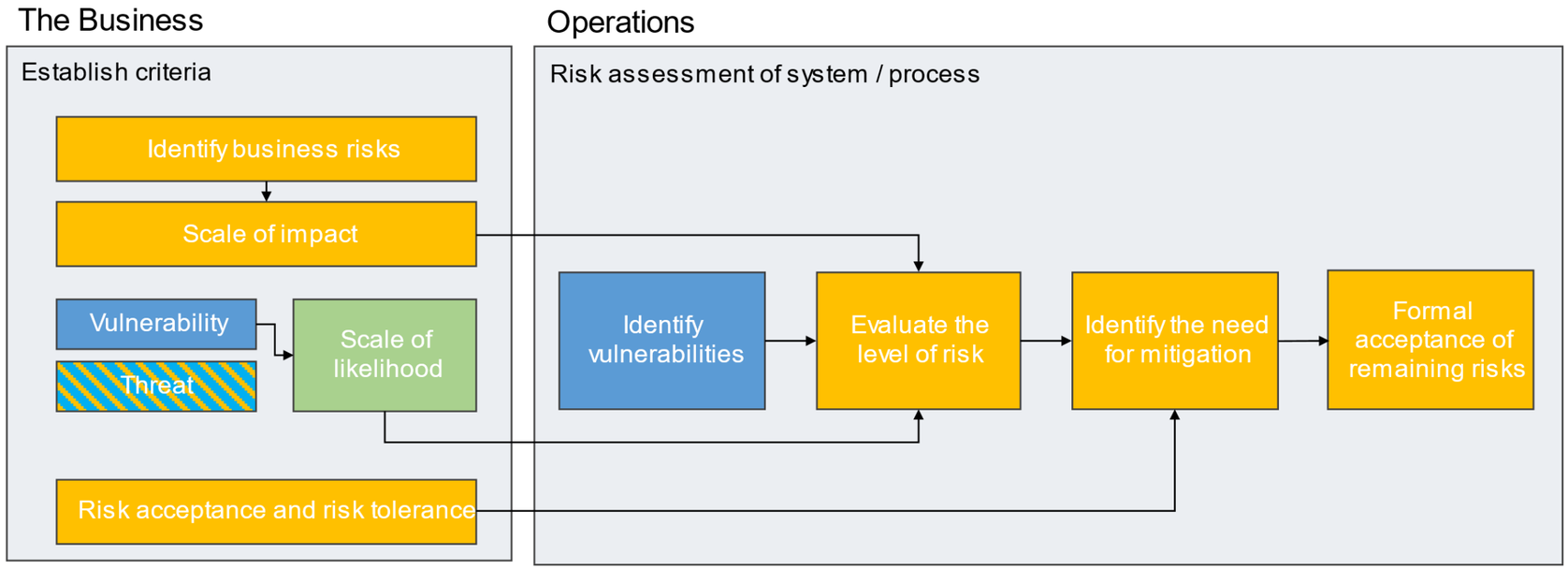


- Skal sikre kontinuerleg risikostyring både på operativt og leiar-nivå
- Er både eit “mindset”, samt ein struktur av risikoregisteret
- Til støtte for risikovurderingar som skjer ved smidig utvikling (RRA på komponenter - Mozilla Foundation) og risikovurdering på individuelle brukarhistorar

Etablering av eit risikolandskap er samspel mellom top-down og bottom-up

Operasjonalisering

- Ledelse
- Utviklerteam



Produktrisiko for ID-porten oppsummert

- Modernisert driftsregime gjer at tekniske sårbarheiter i liten grad kan utnyttast
  - stabilt team m/høg domenekunnskap, sikkerheitskontroller i utvikling og platform
- Vi har få verktøy i verktøykassa for detektere at innbygger blir lurt av angripere
  - eller får hjelp av andre for å løyse digitale utfordringar

Produktrisiko for MinID oppsummert

- MinID sin risiko-landskap er på veg ned
  - dei tekniske sårbarheitene vurderer vi no som lite attraktive angrepsvektorar
- Største risiko: Målretta angrep i nære relasjoner
  - deler denne med BankID m.fl.
  - angrep er noko lettare med MinID enn på nivå høgt, pga. utstedelsespross (aktiveringsbrev) og autentiseringsfaktor (sms)
- Slit med for treig migrering av brukarmassen frå SMS til app/TOTP

digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarevegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo