

Sikkerhetskrav i offentlige anskaffelser

- Et sjærerende oppussingsobjekt med stort potensiale





OM MEG

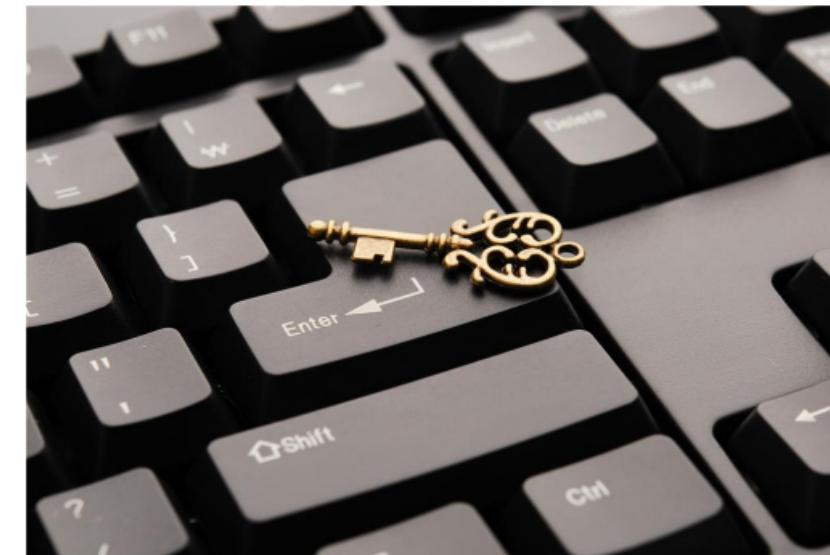
- Hans Kristian Henriksen
- Datateknikk NTNU
- Utvikler i BEKK

Sikkerhetskrav i offentlige anskaffelser

Hans Kristian Henriksen

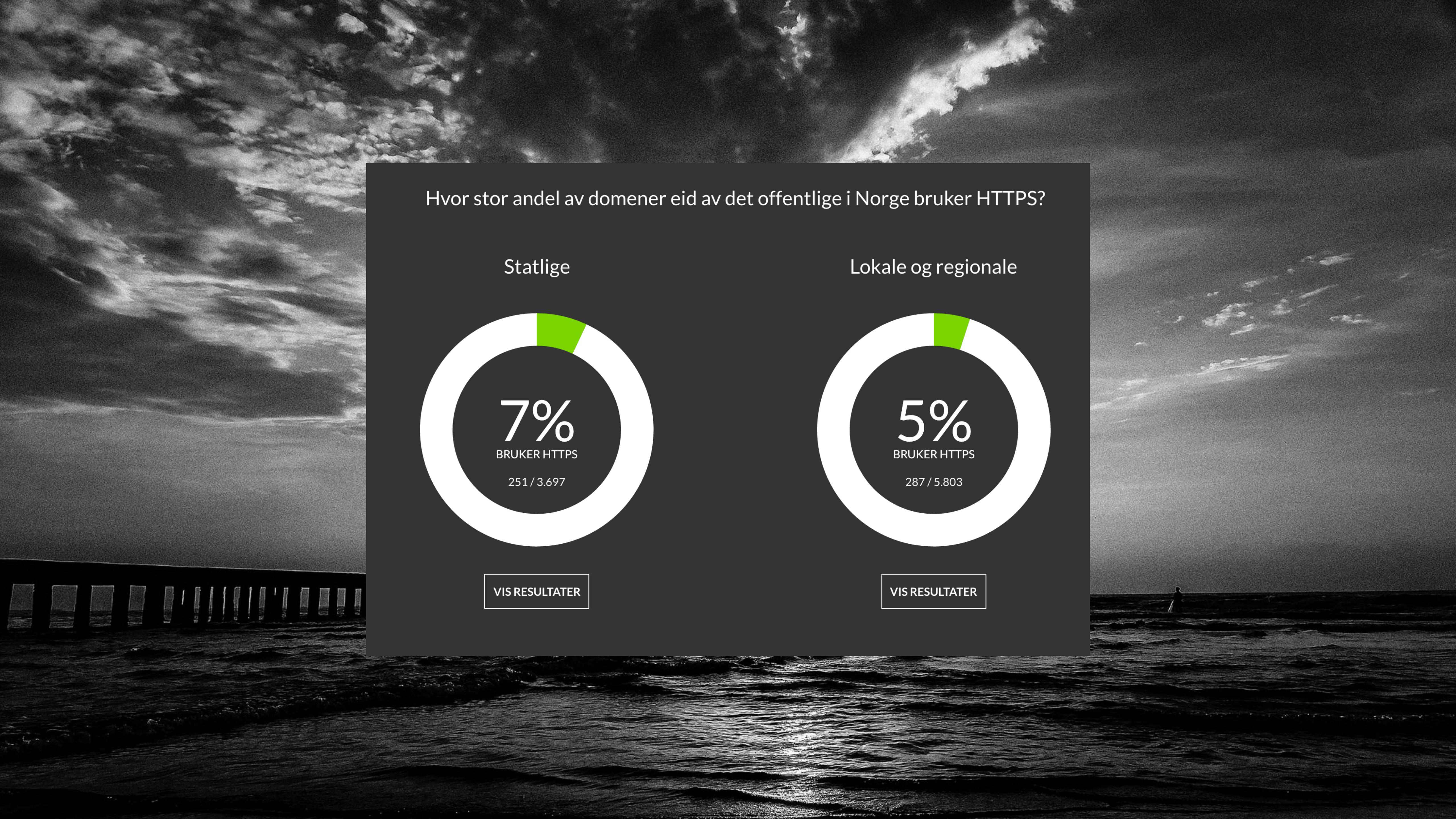
Recommendations for
Improvement of Security
Requirements in Norwegian Public
Procurements

Trondheim, June 2016



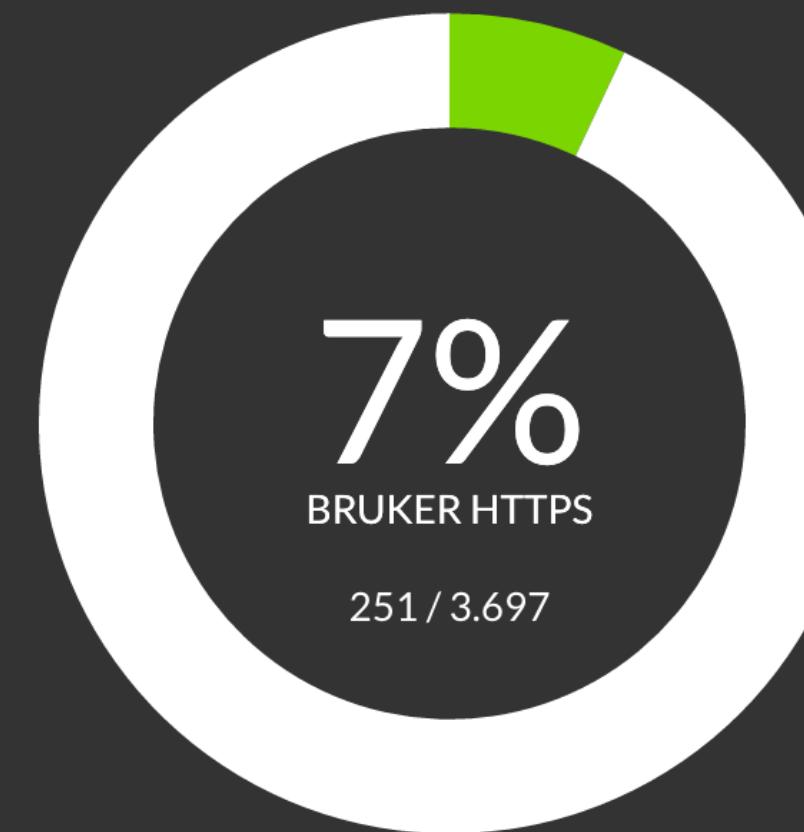
NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology,
Mathematics and Electrical Engineering
Department of Computer and
Information Science

 NTNU
Norwegian University of
Science and Technology



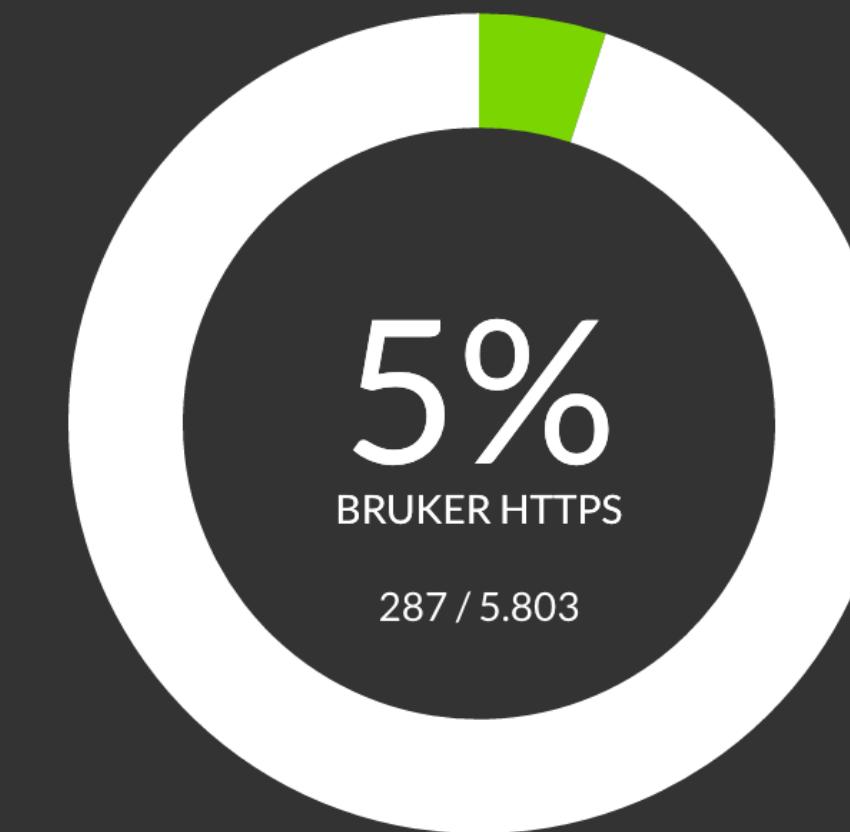
Hvor stor andel av domener eid av det offentlige i Norge bruker HTTPS?

Statlige

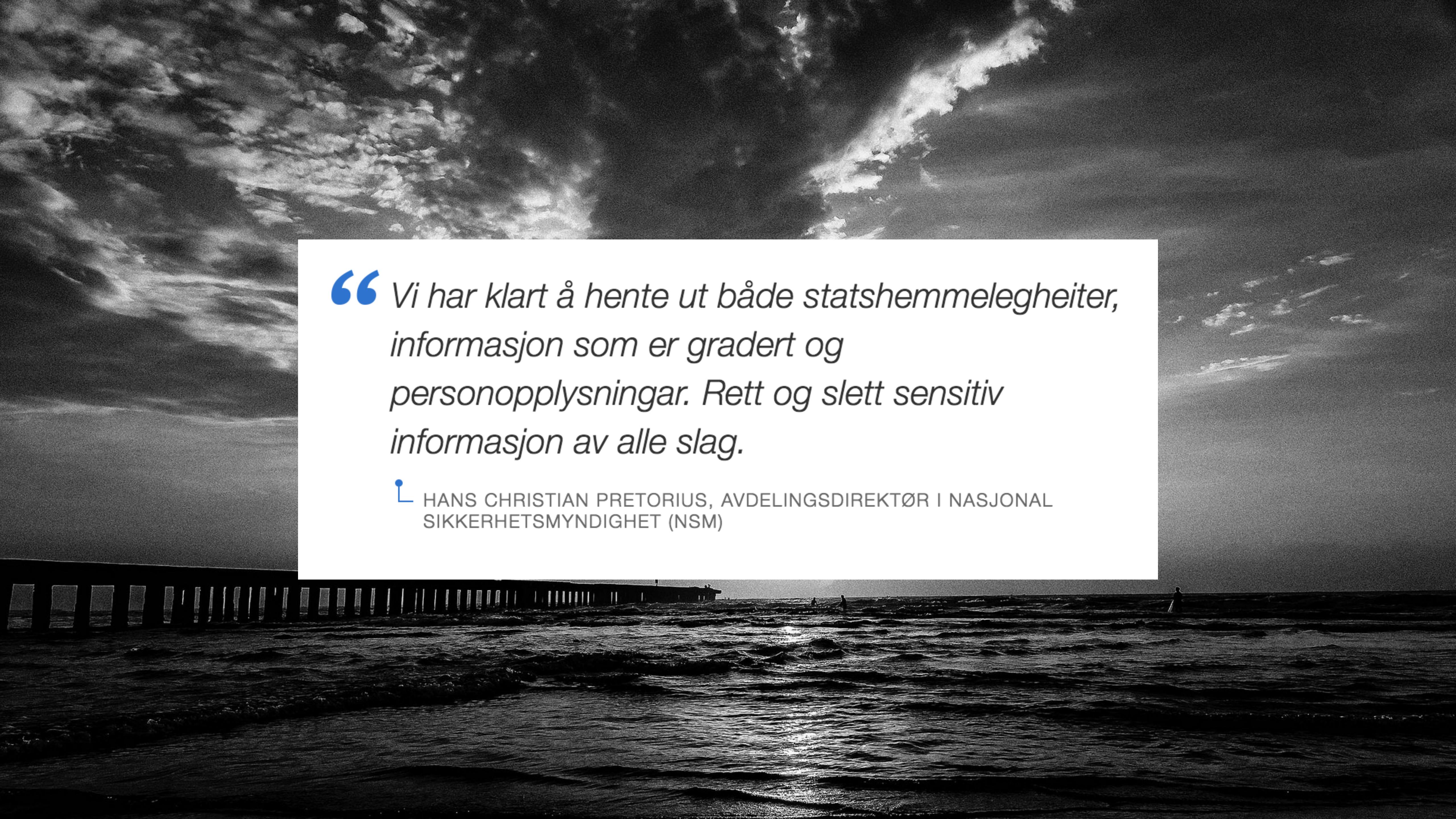


[VIS RESULTATER](#)

Lokale og regionale



[VIS RESULTATER](#)



“Vi har klart å hente ut både statshemmeligheiter, informasjon som er gradert og personopplysningar. Rett og slett sensitiv informasjon av alle slag.



HANS CHRISTIAN PRETORIUS, AVDELINGSDIREKTØR I NASJONAL SIKKERHETSMYNDIGHET (NSM)

Offentlige nettsteder kan brukes til å svindle eller angripe deg

Utdatert og sårbar kode på offentlige nettsteder gjør at ondsinnede aktører i verste fall kan svindle og lure deg med nettadresser du stoler på. Blir du lurt med en adresse fra det offentlige kan de også angripe datamaskinen din.

The screenshot shows a web-based security scanner interface. At the top, it displays the URL [http:// .no/](http://.no/). Below the URL, the text "Detected libraries:" is followed by a list of vulnerabilities:

- jquery - 1.11.1 : (active¹) http:// .no/_style/lib/jquery/jquery-1.11.1.min.js
 - Info: Severity: medium
 - <https://github.com/jquery/jquery/issues/2432>
 - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>- jquery - 1.4.4 : http:// .no/misc/jquery.js?v=1.4.4
 - Info: Severity: medium
 - <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969>
 - <http://research.insecurelabs.org/jquery/test/>- jquery - 1.4.4 : http:// .no/misc/jquery.js?v=1.4.4
 - Info: Severity: medium
 - <http://bugs.jquery.com/ticket/11290>
 - <http://research.insecurelabs.org/jquery/test/>- jquery - 1.4.4 : http:// .no/misc/jquery.js?v=1.4.4
 - Info: Severity: medium
 - <https://github.com/jquery/jquery/issues/2432>
 - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>- jquery-ui-autocomplete - 1.11.2 : (active¹) http:// .no/1. (active) - the library was also found to be active by running code

2 vulnerable libraries detected

Scanner output:

- Scanning http:// .no/ ...
- Script loaded: http://www...
- Script loaded: http://www...
- Script loaded: http://www...



Øyvind Bye Skille

@Byeskille

Journalist

MER OM DATASIKKERHET I NORGE

Publisert 11.05.2016, kl. 22:52

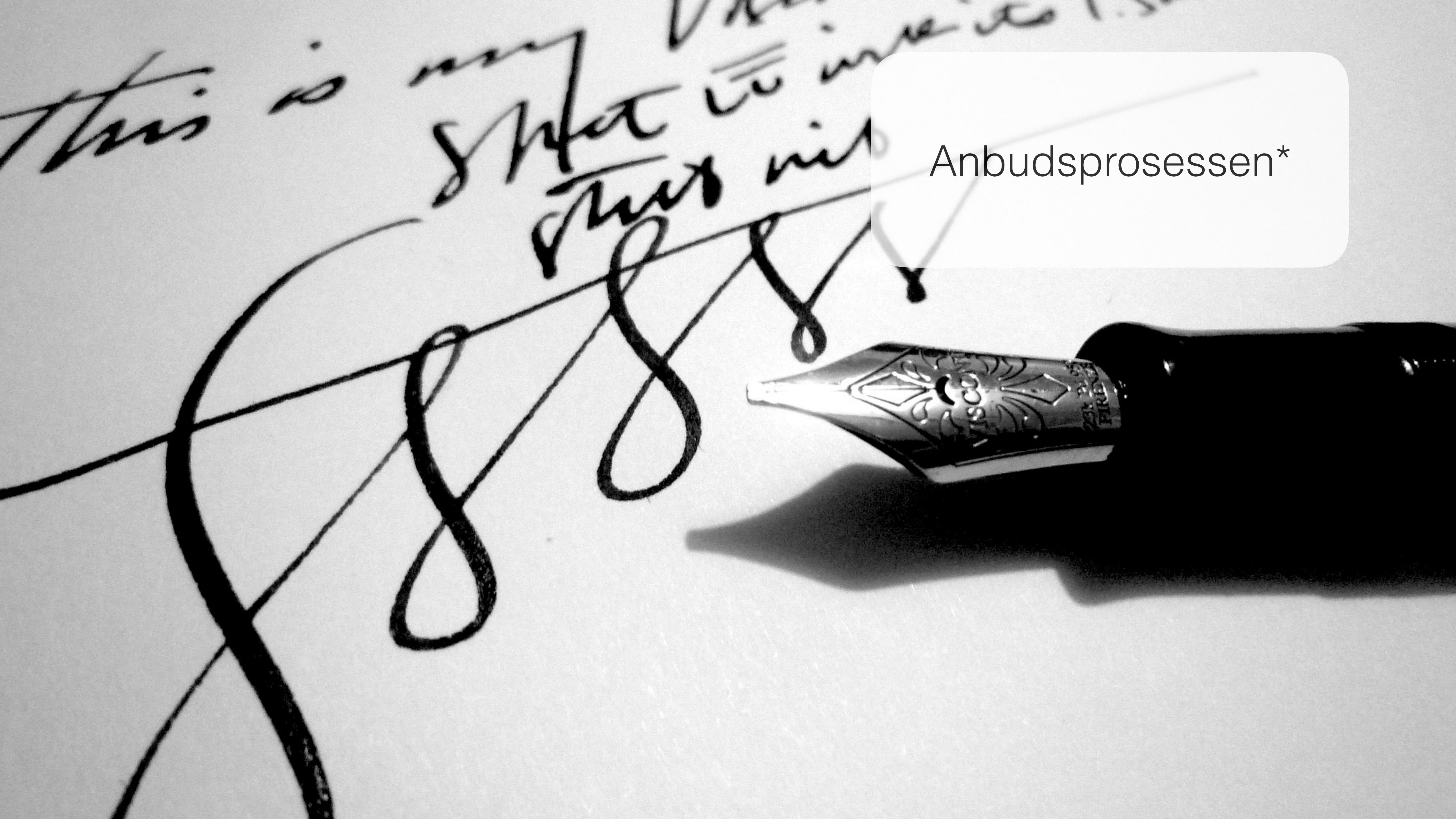


Akademisk vinkel

Agenda

- Kort om anbudsprosessen
- Hva er gode sikkerhetskrav?
- Dagens tilstand i anbud
- Anbefalinger for fremtiden

Anbudsprosessen*





Anbudstyper

1. Åpen anbudskonkurranse
2. Begrenset anbudskonkurranse
3. Konkurranse med forhandling
4. Konkurransepreget dialog





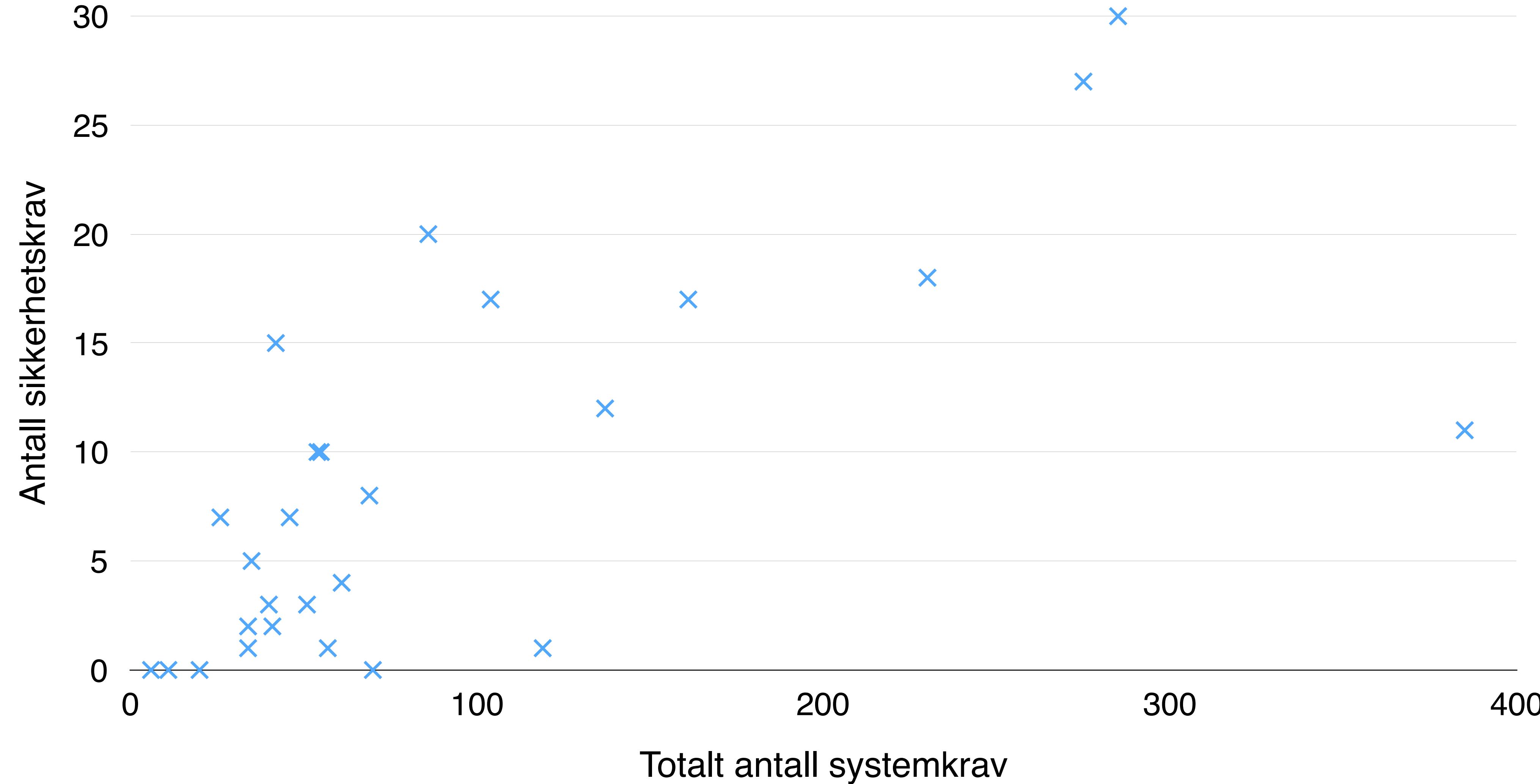
Gode sikkerhetskrav
i anbud

Gode sikkerhetskrav

- Sikkerhetskrav må ikke være for spesifikke
- Sikkerhetskrav må ikke være for åpne
- Utvalget av krav må være konsekvent
- Detaljnívået for krav må være konsekvent
- Samle sikkerhetskrav på ett sted
- Kravdokumentene må ikke være for store
- Velkjente standarder må følges



Lokale helter





Dagens
tilstand i anbud

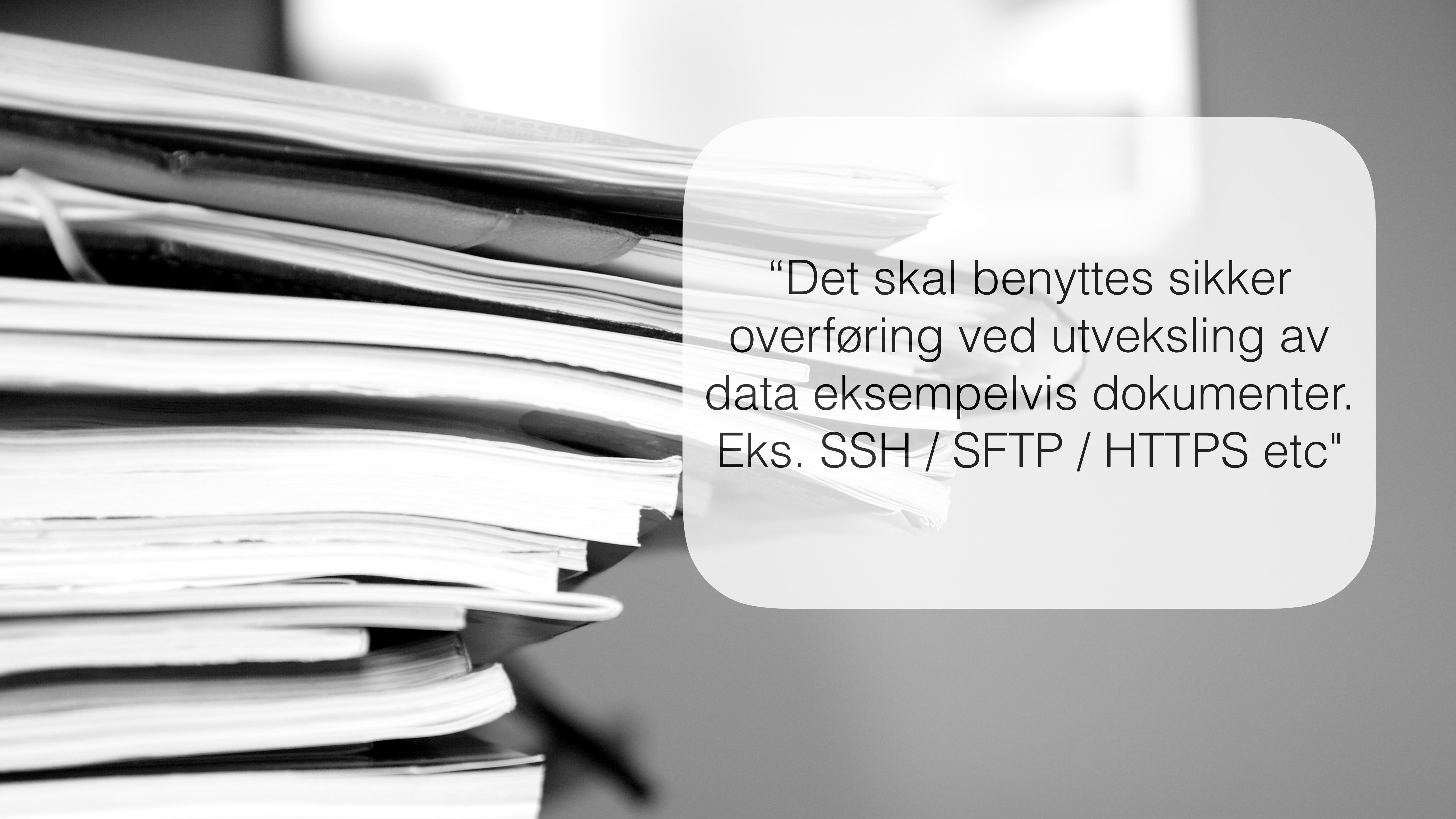


“Leverandøren skal benytte de høyeste relevante industristandarder for sikker programvareutvikling”



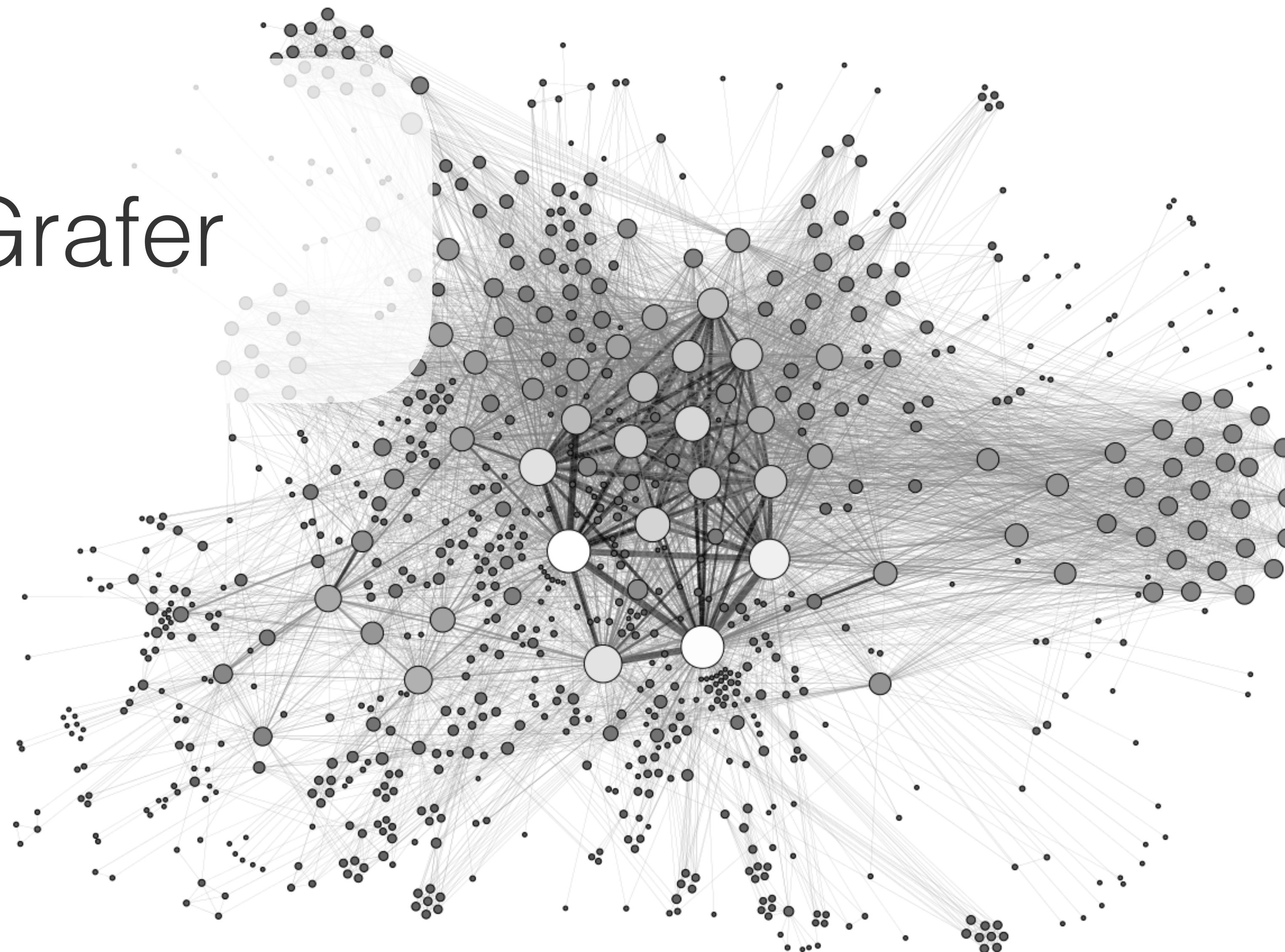
“Leverandøren skal ha gode
tiltak mot hacking av tjenesten.”





“Det skal benyttes sikker overføring ved utveksling av data eksempelvis dokumenter. Eks. SSH / SFTP / HTTPS etc”

Grafer



ISO 27002, Common Criteria og PCI-DSS

Kryptering

Beskyttelse av data og verdier

Operasjonssikkerhet

Autentisering av brukere

Hendelseshåndtering

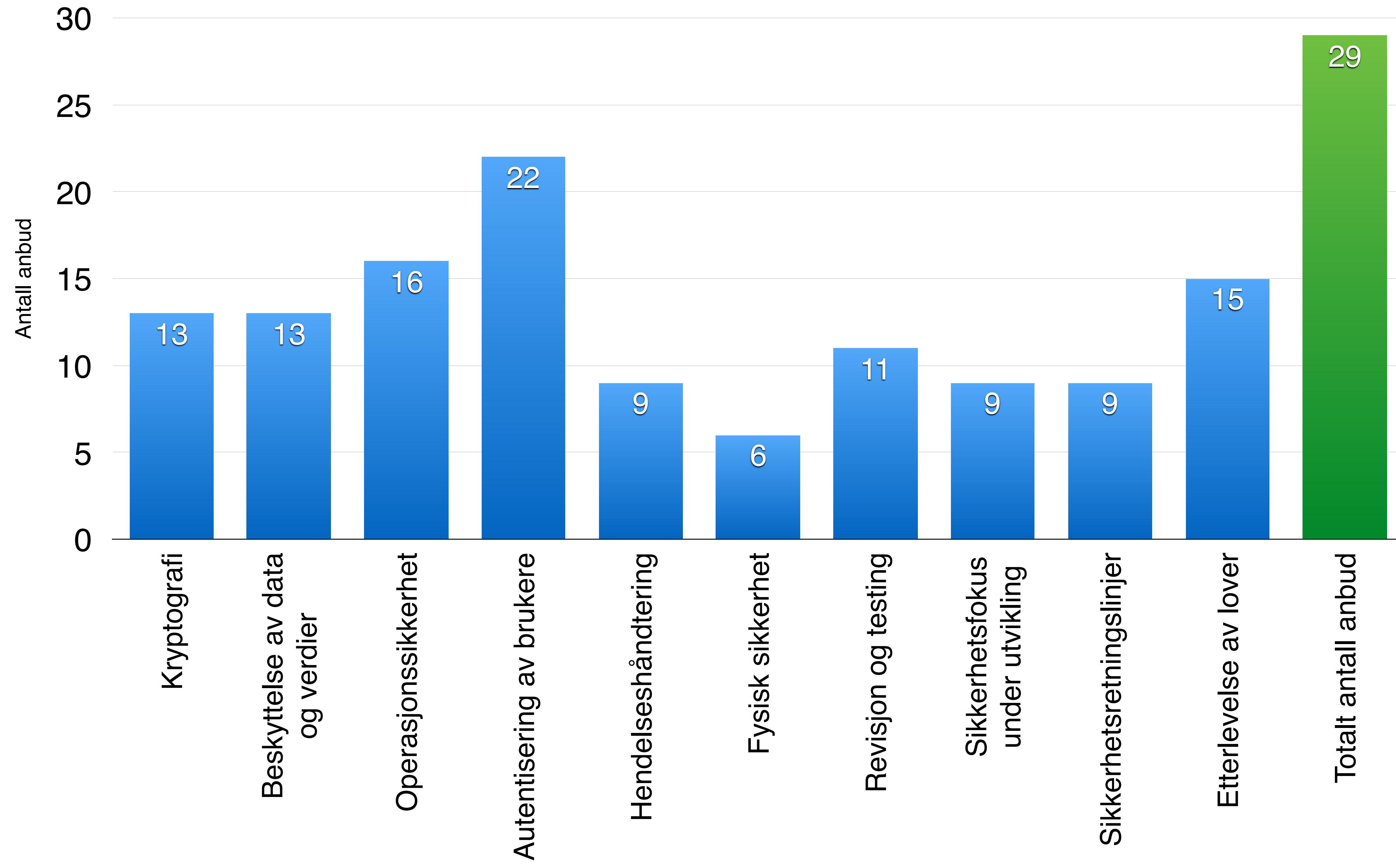
Fysisk sikkerhet

Revisjon og testing

Sikkerhetsfokus under utvikling

Sikkerhetsretningslinjer

Etterlevelse av lover





Anbefalinger og
veien videre

Anbefalinger

- Prosess med forhandlinger
- Standardiserte sjekklister
- Beholde sikkerhetskompetanse
- Sikkerhetsfokus i SSA



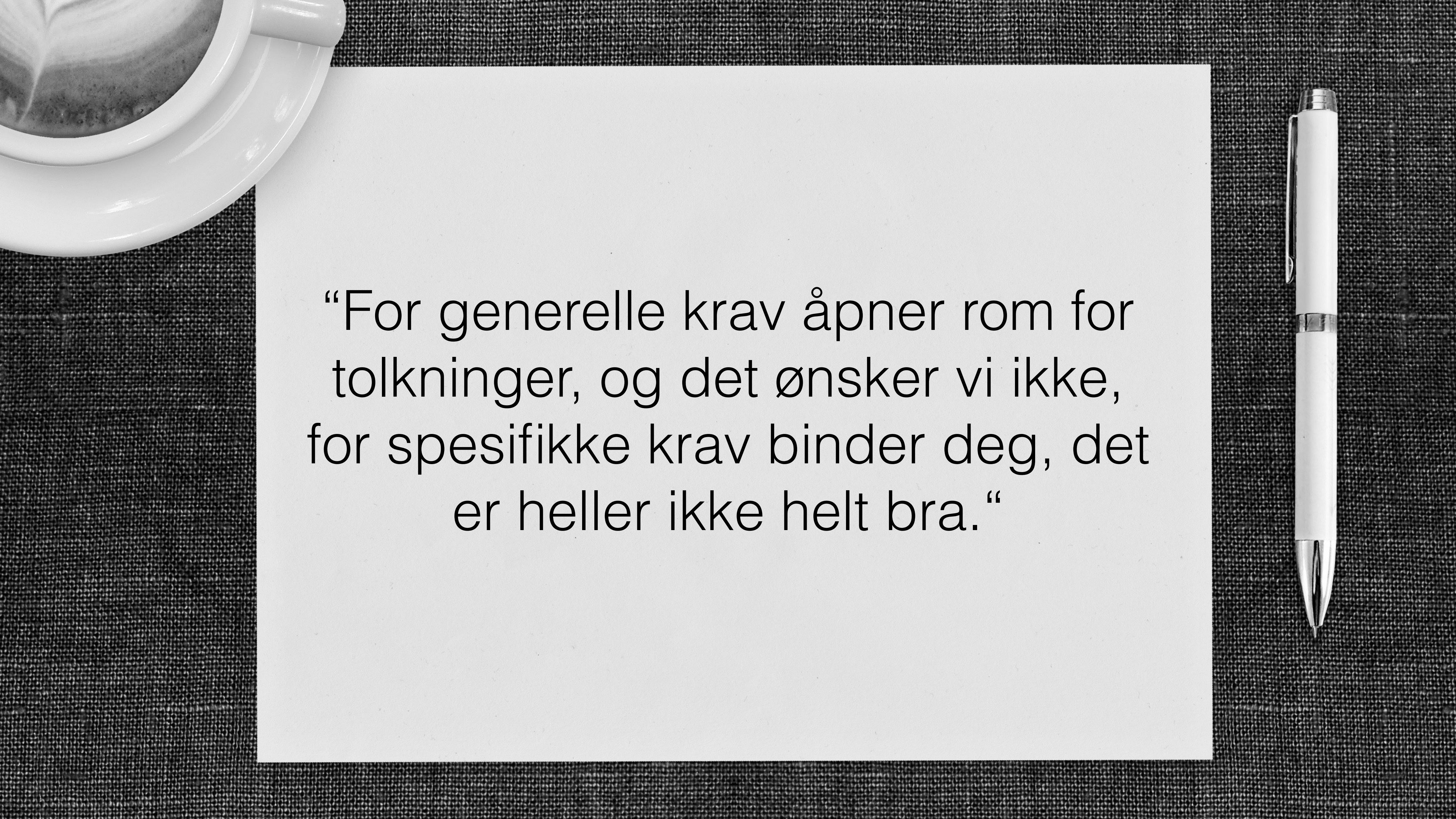
Prosess med
forhandlinger



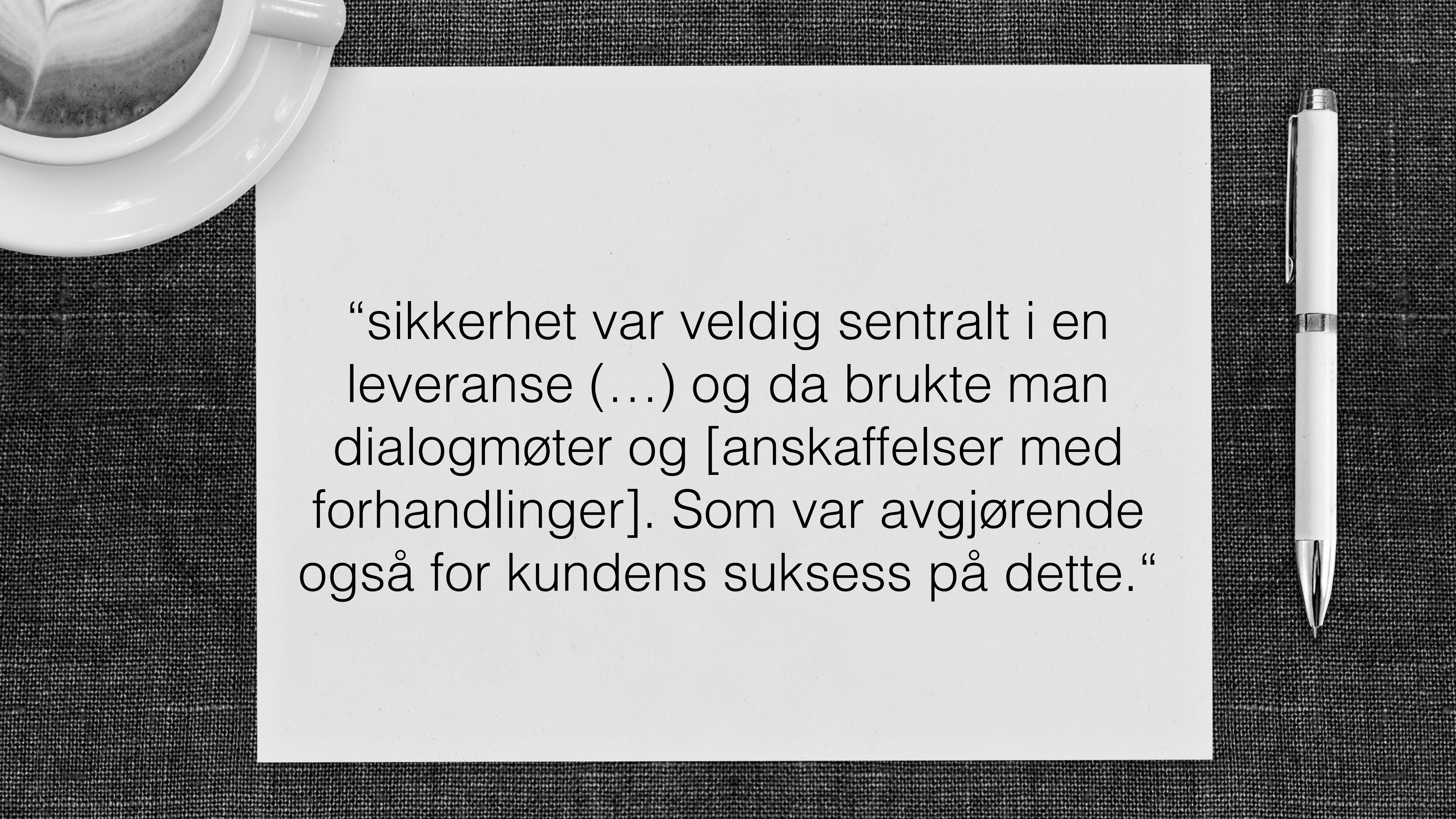
“(...) som leverandør vil man si at dette er bra saker, for her er det absolutt muligheter for mersalg.”

“(...) for å komme i mål tidsnok, for å ikke skremme bort leverandører, for å få et initiellt tilbud fra leverandøren som er innenfor budsjettet, så reduserer man på sikkerhetskrav, så reduserer man på funksjonalitetskrav (...)“





“For generelle krav åpner rom for tolkninger, og det ønsker vi ikke, for spesifikke krav binder deg, det er heller ikke helt bra.“



“sikkerhet var veldig sentralt i en leveranse (...) og da brukte man dialogmøter og [anskaffelser med forhandlinger]. Som var avgjørende også for kundens suksess på dette.”

Anbefaling:

Bruk anbudsformer med
forhandling



Standardiserte
sjekklist

SPRAY PAINT

SEED CII

DUCT TAPE

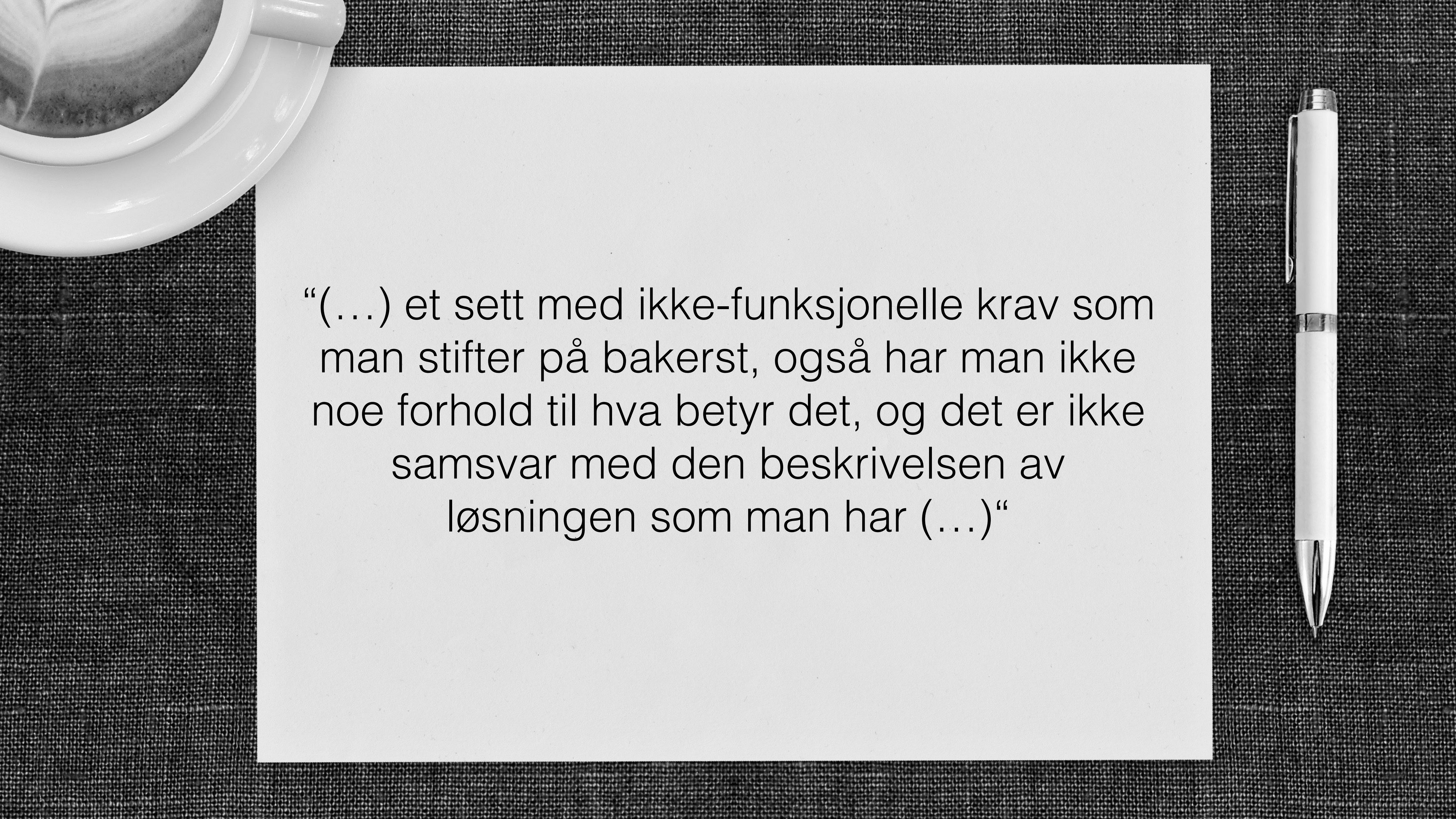
GOOD IDEA TO

IT'S A GOOD IDEA TO



“å utarbeide maler og sjekklister som jeg viste til, det gjør jobben lettere for de virksomhetene som ikke har kompetanse eller resurser på dette området, og vi kan i alle fall få *noe* sikkerhet.“





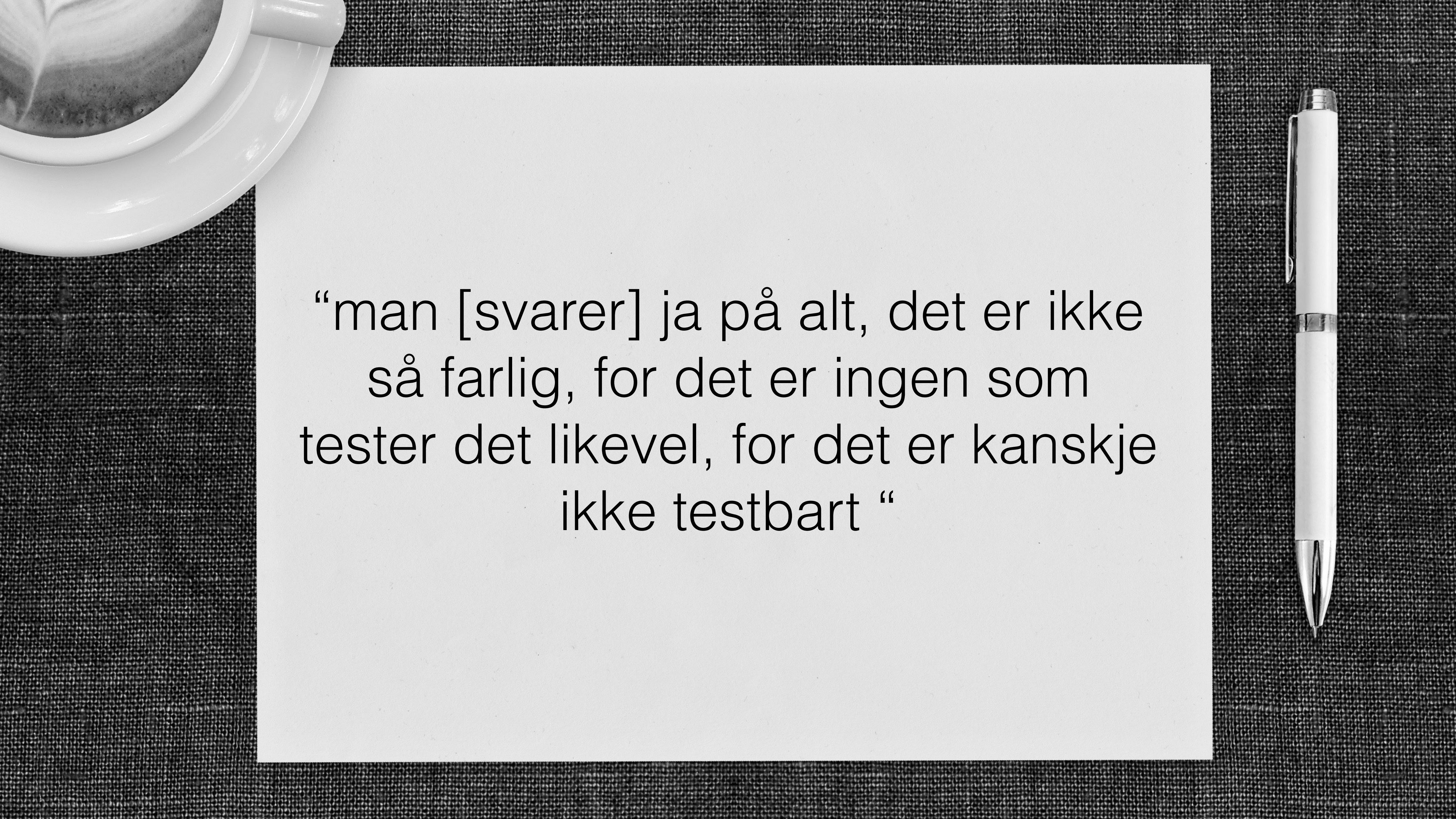
“(...) et sett med ikke-funksjonelle krav som man stifter på bakerst, også har man ikke noe forhold til hva betyr det, og det er ikke samsvar med den beskrivelsen av løsningen som man har (...)“

Anbefaling

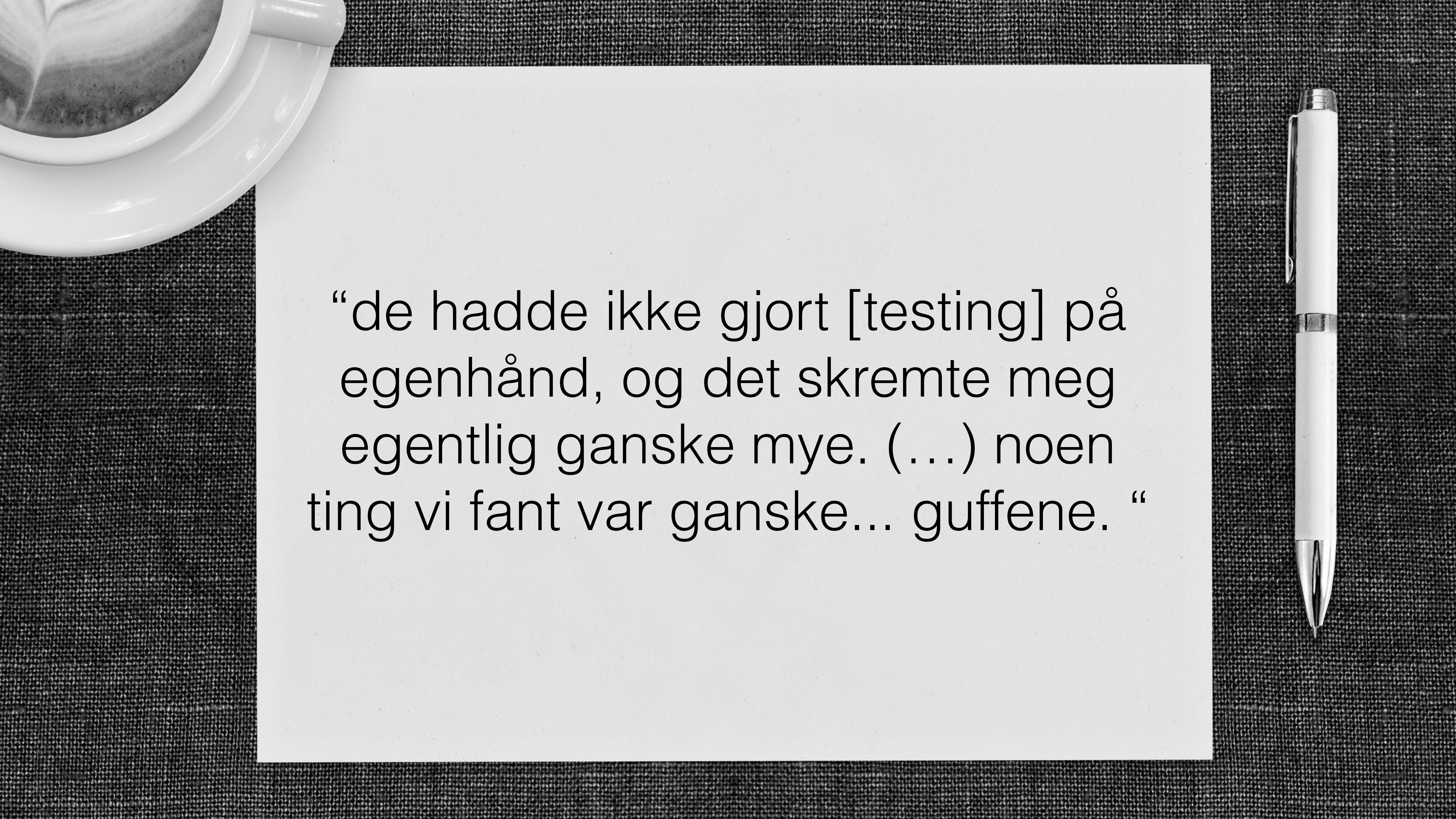
- Kryptering
 - Alle data som sendes over internett skal være kryptert
- Beskyttelse av data og verdier
 - ...
- Operasjonssikkerhet
- Autentisering av brukere
- Hendelseshåndtering
- Fysisk sikkerhet
- Revisjon og testing
- Sikkerhetsfokus under utvikling
- Sikkerhetsretningslinjer
- Etterlevelse av lover



Beholde
sikkerhetskompetanse



“man [svarer] ja på alt, det er ikke
så farlig, for det er ingen som
tester det likevel, for det er kanskje
ikke testbart “



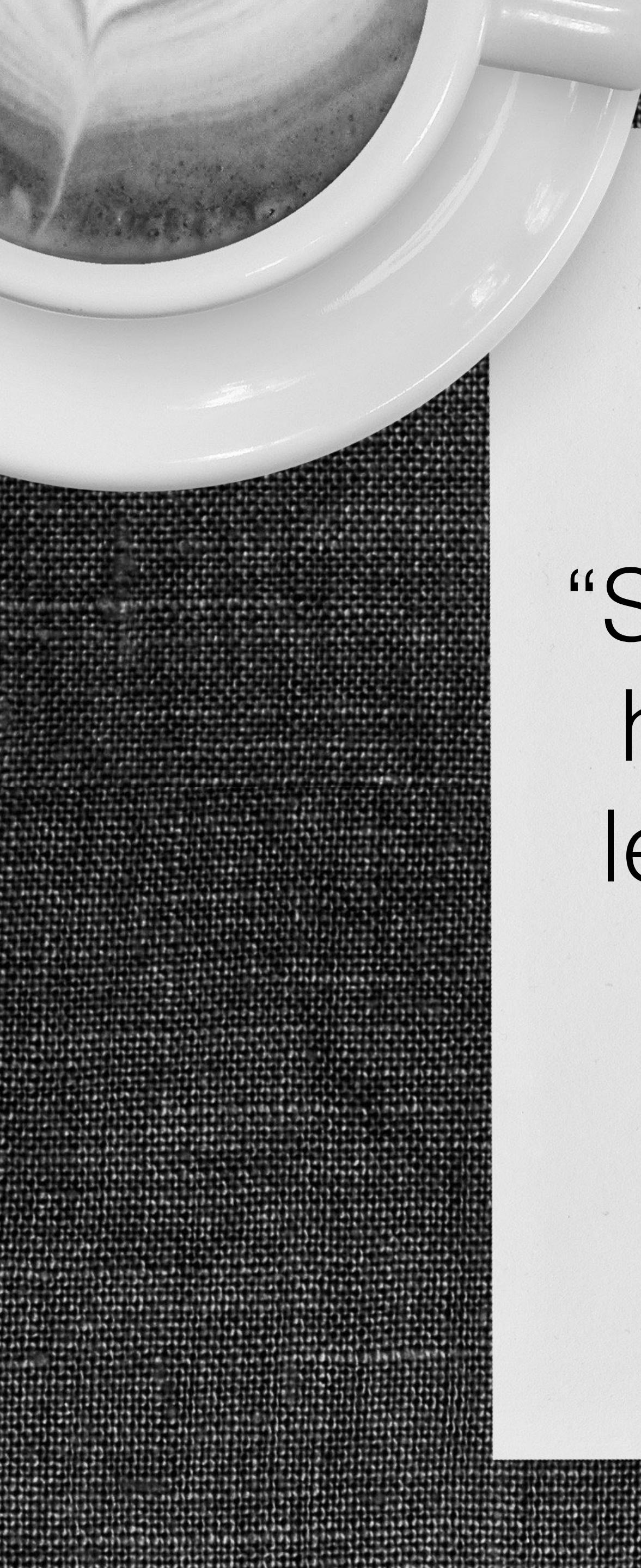
“de hadde ikke gjort [testing] på egenhånd, og det skremte meg egentlig ganske mye. (...) noen ting vi fant var ganske... guffene. ”

Anbefaling:

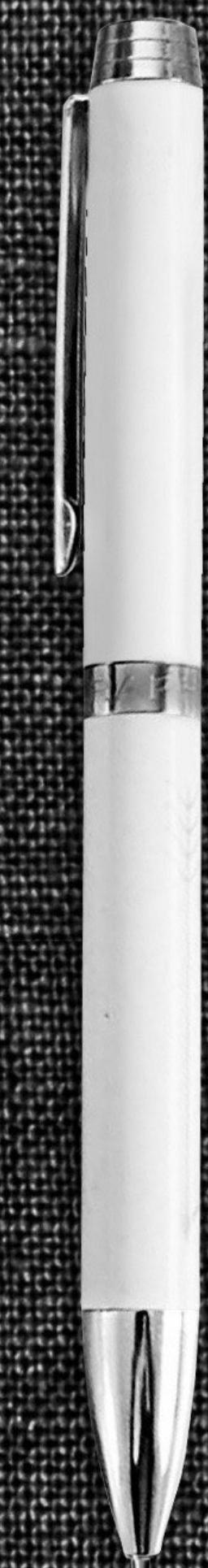
Behold eller anskaff intern
kompetanse på sikkerhet



Sikkerhetsfokus
i SSA



“SSAene har ødelagt mye ved at man har fått et enormt fokus på deler av leveranser, men ikke på totalitet. Og sikkerhet er jo ikke en påkk med.”



Anbefaling:

SSAene må oppdateres slik at
sikkerhet i større grad inkluderes

Sikkerhetskrav i offentlige anskaffelser

- Et sjærerende oppussingsobjekt med stort potensiale





Spørsmål?

hkh.io/master

master@hkh.io

Bilder

Alle bilder brukes under Creative Commons-lisens

Andrew Gibson - <https://www.flickr.com/photos/gibospics/9457851081>

Magdalena Reseller - <https://www.flickr.com/photos/magdaleneroeseler/14579860843/>

Butch Dalisay - <https://www.flickr.com/photos/penmanila/7459787712> (konvertert til s/h)

Herr Olsen - <https://www.flickr.com/photos/herrolsen/14890254298> (konvertert til s/h)

Ekin Arabacioglu - <https://www.flickr.com/photos/ekinarabaci/3476631499> (konvertert til s/h)

E_Bass - https://www.flickr.com/photos/e_bass/5042766520 (konvertert til s/h)

Yaffa Phillips - <https://www.flickr.com/photos/yaffamedia/2042195912> (konvertert til s/h)

Sebastien Wiertz - <https://www.flickr.com/photos/wiertz/5624281846> (konvertert til s/h)

Marcelo Campi - <https://www.flickr.com/photos/marcelocampi> (konvertert til s/h)

Kannan Muthuraman - <https://www.flickr.com/photos/wellbredkannanclicks/17251824375>

Ruud van Eck - <https://www.flickr.com/photos/blechdach/14387805316>

International Monetary Found - <https://www.flickr.com/photos/imfphoto/3612876572>

littlestar19 - <https://www.flickr.com/photos/littlestar19/6857110627> (konvertert til s/h)

Sebastien Wiertz - <https://www.flickr.com/photos/wiertz/6093566215>

Tina Vance - <https://www.flickr.com/photos/tina/16140496941> (konvertert til s/h)

Martin Grandjean - https://en.wikipedia.org/wiki/File:Social_Network_Analysis_Visualization.png (konvertert til s/h)

Sikkerhetskrav i offentlige anskaffelser

- Et sjærerende oppussingsobjekt med stort potensiale

