Universitetet i Sørøst-Norge

# Operasjonalisering av NIST SSDF til en sikkerhetsjekkliste

## Fra rammeverk til arbeidsflyt

*Samme krav — ulik fase — ulikt spørsmål*

**01 Analyser**
*«Gjelder dette kravet?*

**02 Design**
*«Hvordan løser vi det?»*

**03 Implementer**
*«Hvor i koden er det?»*

**04 Verifiser**
*«Er kravet oppfylt?»*

**05 Fullfør**
*«Klar for leveranse?»*

**06 Respondér**
*«Hvordan håndteres nye funn?»*

**Hver fase bygger sitt eget bevisspor → automatisk sporbarhet**

# Hensikt og mål

I dag mangler mange bedrifter gode, praktiske løsninger for å holde oversikt over regulatoriske krav og compliance. Kravene blir både flere og strengere, og omfanget gjør det krevende å sikre at alle krav er oppfylt for hvert enkelt produkt og prosjekt.

I dette prosjektet har vi utviklet og testet en sikkerhetssjekkliste som skal gi bedre oversikt over relevante krav, og gjøre det enklere å følge dem opp i praksis.

Målet med prosjektet var å:

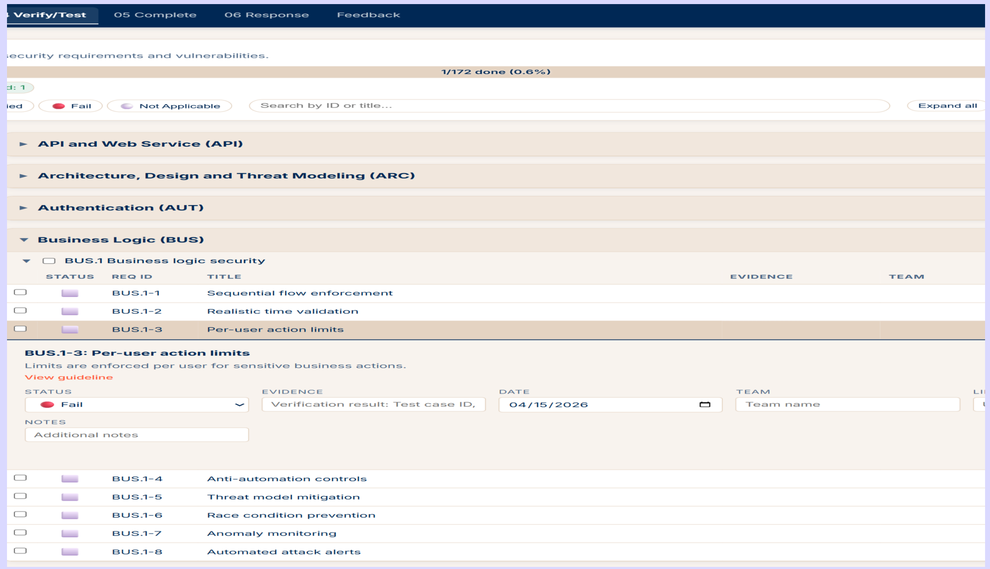
- Kartlegge relevante krav innenfor sikker programvareutvikling basert på NIST SSDF og regulatoriske krav.
- Utvikle en prototype på en sjekkliste som kobler krav til konkrete prosjekter/produkter.
- Teste løsningen i faktiske prosjekter i bedriften for å vurdere nytteverdi og brukervennlighet.

# Resultater og sentrale funn

Prosjektet resulterte i en fungerende prototype på en digital sikkerhetssjekkliste som gir bedre oversikt over hvilke krav som gjelder i ulike prosjekter, og hvordan status er på hvert enkelt krav.

De viktigste funnene er:

- Vi utviklet en prototype som gjør det mulig å oppdatere status på hvert krav fortløpende. Dette kan redusere behovet for omfattende sikkerhetsdokumentasjon i etterkant, samt antall gjentatte spørsmål fra kunder om de samme sikkerhetsforholdene.
- Brukertesting i to faktiske prosjekter viste at autonomi for utviklere er viktig – løsningen må oppleves som støtte, ikke som ekstra administrativt arbeid.
- Analysen vår tyder på at strukturen i sjekklisten må forbedres for å gjøre den enklere å bruke. En bedre struktur kan spare bedriften for betydelig manuelt arbeid senere i prosjektløpet.
- Løsningen kan videreutvikles ved å:
- fokusere mer på synkronisering av krav på tvers av prosjekter
- gruppere og kategorisere krav tydeligere etter type prosjekt og produkt





Tobias Melsom
247045@usn.no
Master i Cybersikkerhet og digitalisering

Robin Færaas
145428@usn.no
Master i Cybersikkerhet og digitalisering

Veileder: Geir M. Køien, Professor i Cybersikkerhet, USN (geir.koien@usn.no

Samarbeidspartner: Jotron AS – Anders Viken : Utvikler (anders.viken@jotron.com)