Proaktiv riskhantering för sårbarheter inom öppna programvaruprojekt

Johan Linåker

Hållbarhet hos öppna programvaruprojekt

- Ett öppet programvaruprojekts förmåga att förbli underhållet över tid utan avbrott och till hög och bibehållen kvalitet

Photo by Jan Piatkowski | https://unsplash.com/photos/eopz9bkwROs

Hälsa hos öppna programvaruprojekt

- Ett öppet programvaruprojekts förmåga att förbli livskraftigt över tid
  - Produktivitet: projektets aktivitet avseende utveckling och underhåll
  - Robusthet: projektets förmåga att stå emot störningar, ex. att nyckelaktörer lämnar projektet
  - Öppenhet: projektets öppenhet för externt inflytande och bidrag

Öppen programvara – del av vår digitala infrastruktur

- Öppen programvara utgör ett centralt typ av byggblock i vår digitala infrastruktur
- Behöver kontinuerligt underhåll likt fysisk infrastruktur för att förbli säker och robust

Photo by Modestas Urbonas | https://unsplash.com/photos/vj_9l20fzj0

Öppen programvara – del av vår digitala infrastruktur

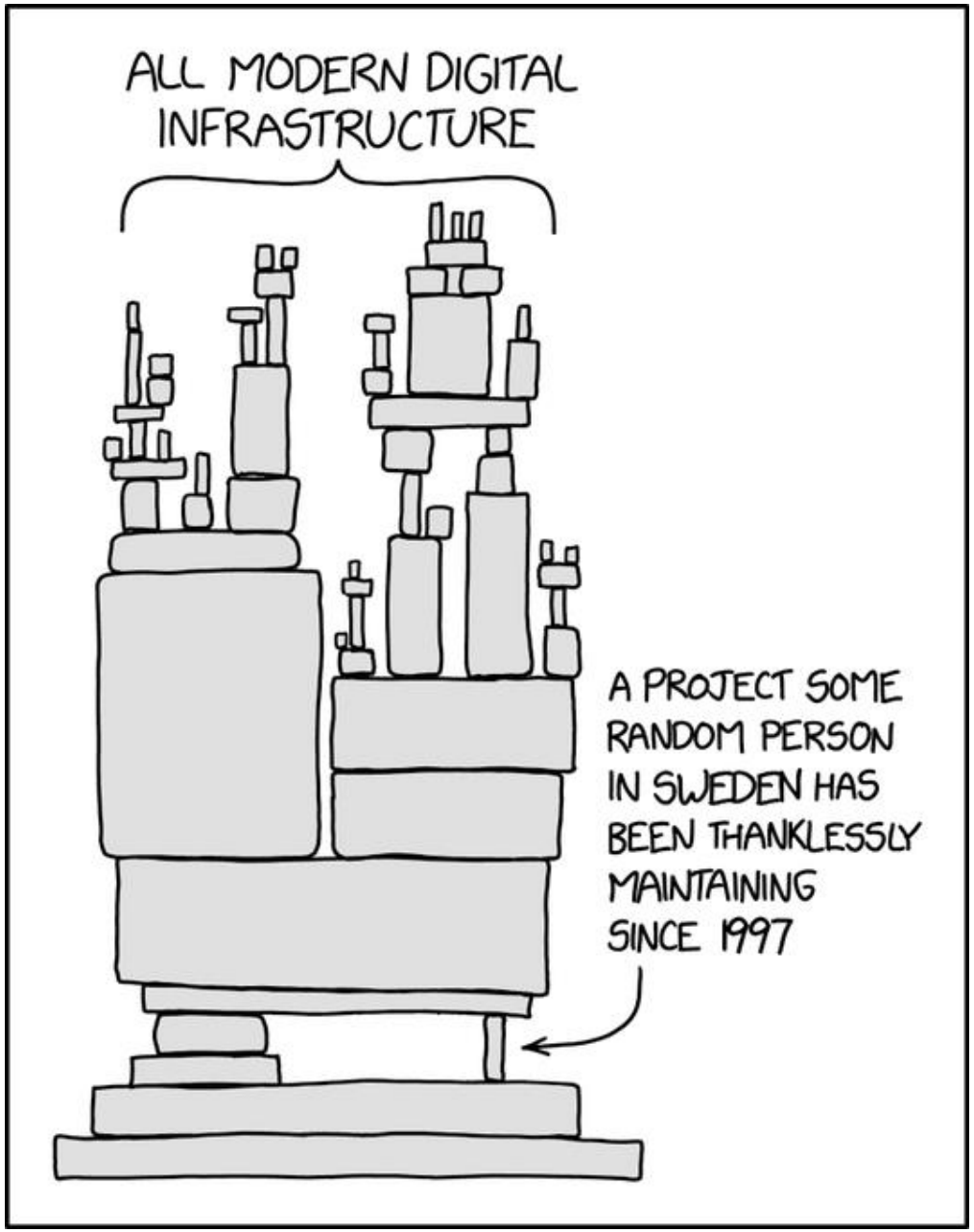
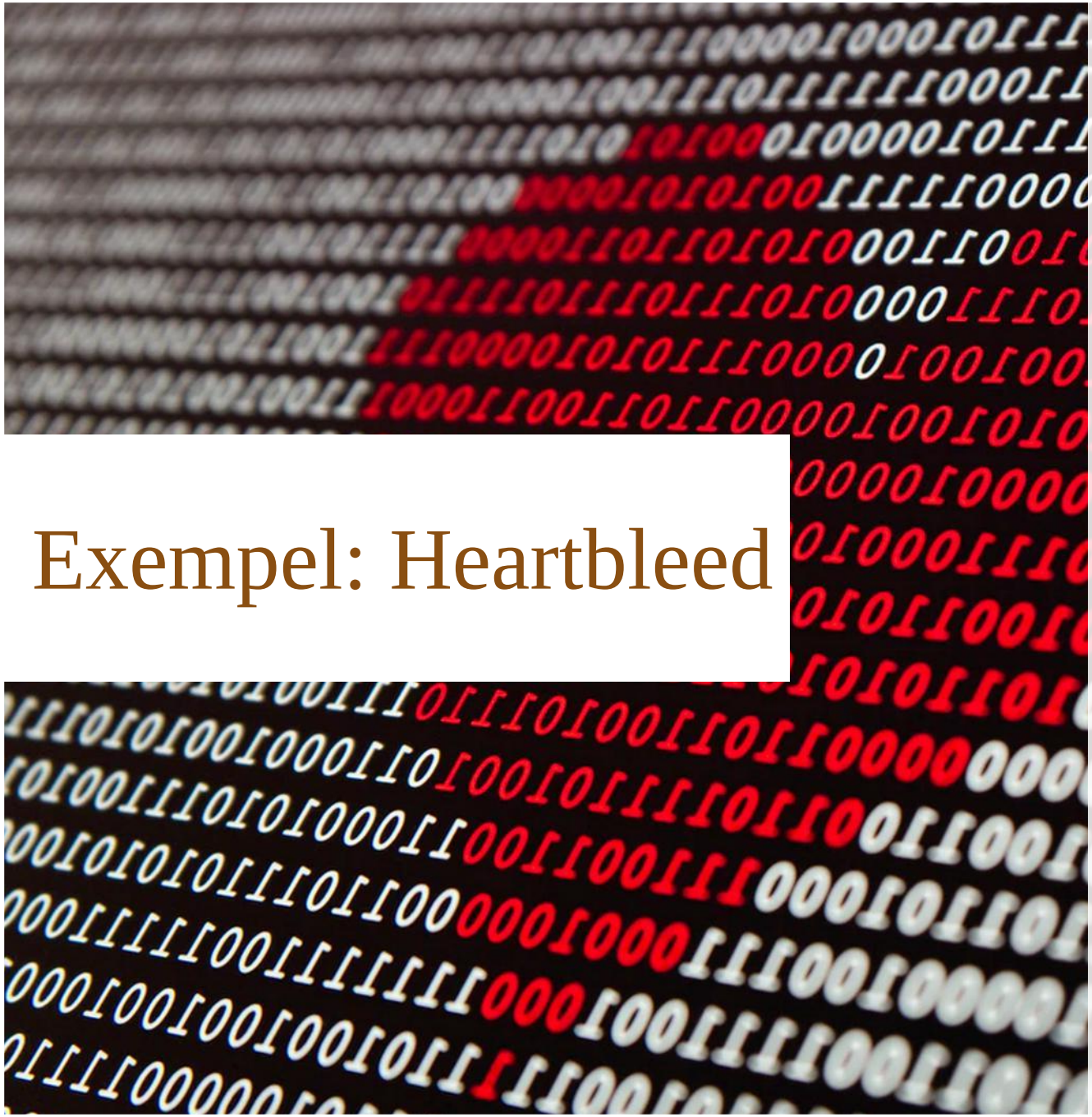


Photo by @tsjost and XKCD | https://twitter.com/tsjost/status/1295662118113619968



Exempel: Heartbleed

- Bugg i krypteringsbilioteket OpenSSL
- Biblioteket används i ett stort antal internetuppkopplade maskiner i världen
- Introducerad 2012, åtgärdad 2014
- Möjliggjorde åtkomst till privata krypteringsnycklar
- Problem: underhölls vid tidpunkten av två personer, användes av i princip alla, väldigt få bidrog till underhållet

Öppen programvaras kvalitet – två sidor av samma mynt

- Öppen programvara är...
  - full av, eller mottaglig för, sårbarheter redo att utnyttjas
  - alltid säkrare än stängda och proprietära alternativ
- Ej så svart och vitt...

Photo by Elena Rouame | https://unsplash.com/photos/9JU2CKqtw0M

The ”Many-Eyes” effect

- Även känd som Linus’ lag →
- ”Given enough eyeballs, all bugs are shallow”
- Kräver att tillräckligt antal ögon faktiskt når källkoden

Utvecklingsresurser är begränsade

- En överhängande majoritet av öppna programvaruprojekt underhålls av en eller ett fåtal individer
- Begränsad kapacitet, ofta med mycket fokus på support och besvara frågor
- Kan lätt falla från, ex. pga. bristande intresse, förändrade familjeförhållanden eller utbrändhet
- Få som faktiskt bidrar tillbaka, tar underhållet för givet

Vem är ansvarig för kvalitén hos programvaran?

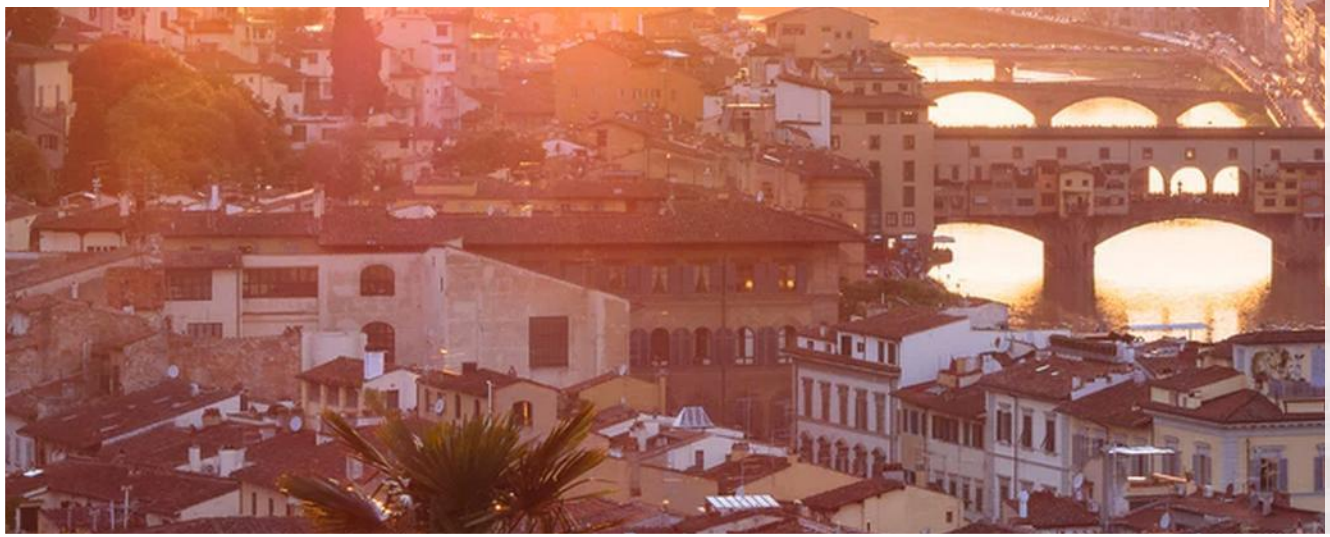
- Förvaltarna?
- Användarna?
- Staten?
- Annan? Alla?

Photo by Scott Blake | https://unsplash.com/photos/x-ghf9LjrVg

Öppen programvara inom offentlig sektor

- Utmaningar kring bristande kultur, kunskap och tillgång av resurser
- Anskaffning nyckel till användning och utveckling av öppen programvara
- Behov av stöd och vägledning

Nationellt kompetenscenter: Exempel från Italien



- Nationellt och regionala kompetenscenter → Motsvarande industrins Programkontor för Öppen programvara (Open Source Program Offices)
- Lagar som föreskriver hur öppna alternativs bör prioriteras, och egenutvecklad programvara tillgängliggöras öppet
- Beslutsmodell och vägledning kring hur öppen programvara kan utvärderas och jämföras, inklusive dess hälsa:
  - ”*the viability of the open source project, through the assessment of visible indicators on the repository, such as code activity, release history, user community, longevity of the project, number of unique developers.*”
- Se: https://docs.italia.it/italia/developers-italia/gl-acquisition-and-reuse-software-for-pa-docs/en/stabile/index.html

Photo by Mark Tegethoff | https://unsplash.com/photos/l-GmdF7Md0o

Samverkansförbund: Exempel från Danmark

- OS2 – formellt samarbete mellan majoritet av danska kommuner men även regioner och myndigheter i växande skala
- Projekt initieras av en eller flera medlemmar, utvecklas genom anskaffade resurser
- Tillhörande ekosystem om 60+ tjänsteleverantörer
- Etablerade processer för styrning, anskaffning och förvaltning som säkerställer hälsan för nya öppna programvaruprojekt
- Se: https://os2.eu/

Photo by Nick Karvounis | https://unsplash.com/photos/3_ZGrsirryY

Proaktivt riskarbete nödvändigt

- Identifiera vilka projekt organisationen är beroende av
- Analysera och bilda sig en uppfattning om hur hälsan ser ut för aktuella projekt
- Överväga att bidra tillbaka egna ändringar alt. utifrån projektet behov
- Även av vikt att beakta vid nyanskaffning av öppen programvara till verksamhet

Hur mäter vi hälsan?

- Community Health Analytics for Open Source Software (CHAOSS)
  - Ramverk av mått för att analysera hälsan hos ett projekt
- En verktygslåda av mått att välja utifrån behov
- Kan besvaras kvalitativt och genom analysverktyg
- Pågående forskning kring att ta fram ramverk för svensk industri och offentlig sektor:
  - https://www.ri.se/sv/vad-vi-gor/projekt/health-and-security-management-in-open-source-software

Photo by Luke Chesser | https://unsplash.com/photos/JKUTrJ4vK00

Behov för systematisk process

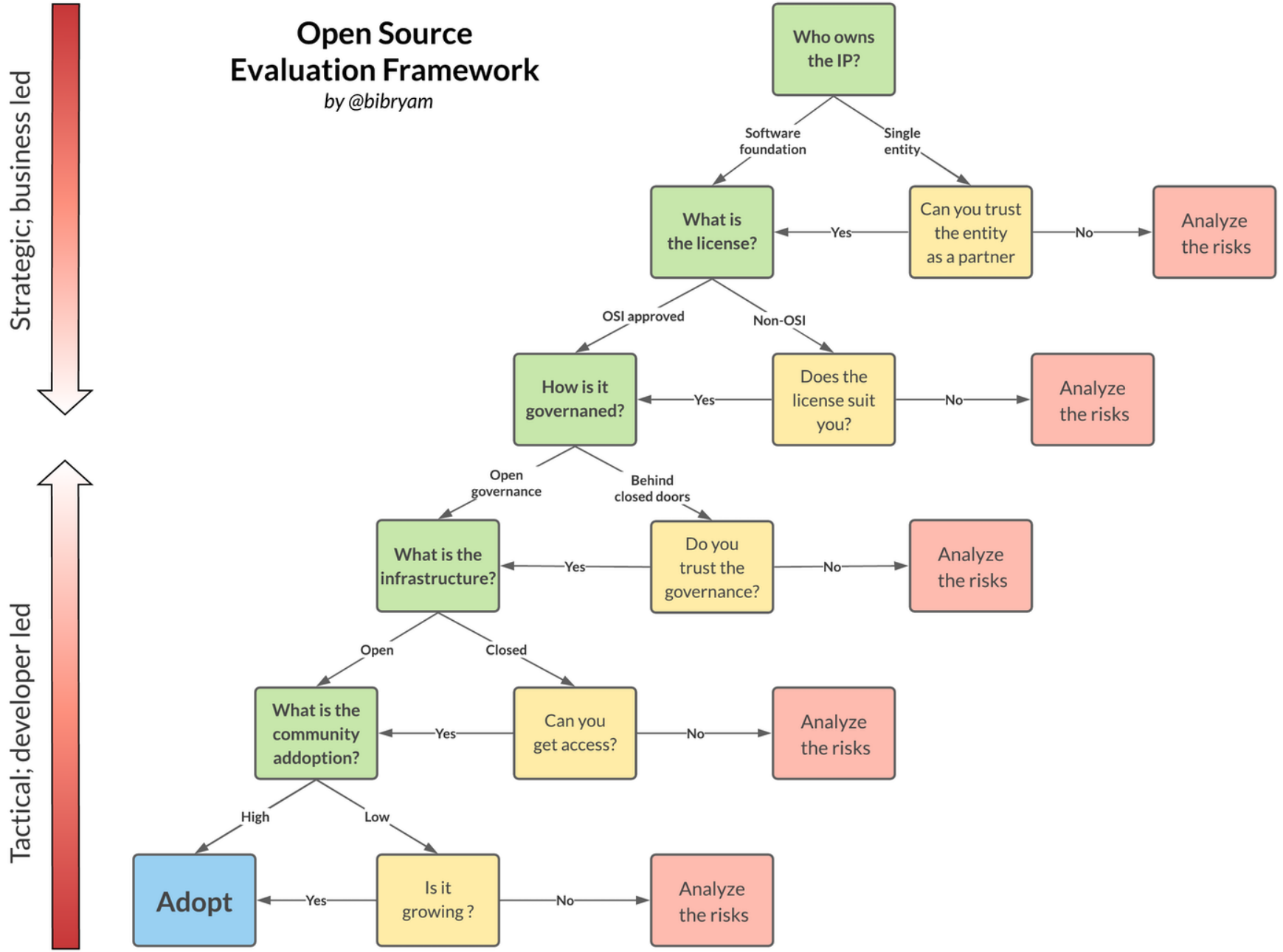


Photo by Bilgin Ibryam | https://monetize.substack.com/p/a-framework-for-open-source-evaluation

Hur kan vi mäta hälsan?

- Legalt – Ägarskap av upphovsrätt, typ av licens
- Styrning – Öppenhet för påverkan och tillsättning
- Tillgänglighet – Kommunikation och utveckling
- Diversitet – Användare och utvecklare
- Professionell support – utbud av leverantörer
- Social aktivitet – Kommunikation och utveckling
- Utvecklingsaktivitet – Teknisk och icke-teknisk
- Kvalitet – Testfall, dokumentation, process mm.
- *Baserat på https://CHAOSS.community*

Exempel från praktisk tillämpning

- Arbetsförmedlingen i val mellan två öppna e-arkivslösningar, RODA och ESSArch
- Hälsoanalys, del av av övergripande analys som även innefattar risk och konsekvensanalys, nyttorealisering, kravuppfyllnad osv.
- Datainhämtning från onlinekällor och tidigare utvärderingar, ex. från Tullverket
- Genomgång av inhämtad data utifrån checklista
- En leverantör bakom respektive lösning, den ena mer aktiv än den andre avseende extern utveckling
- Frågetecken avseende inlåsning och nyttohemtagning
- För rapport, begär ut: Af-2021 /0001 1174

Lärdomar från tillämpning

- Vid anskaffning av strategisk eller central programvara behövs
  - Omfattande och noggranna utvärderingsprocesser
  - Enkelt att skapa överblick och jämföra alternativ
  - Kvalitativt fokus
  - Stöd och hjälp för utvärdering behövs

Photo by Belinda Fewings | https://unsplash.com/photos/LtNvQHdKkmw

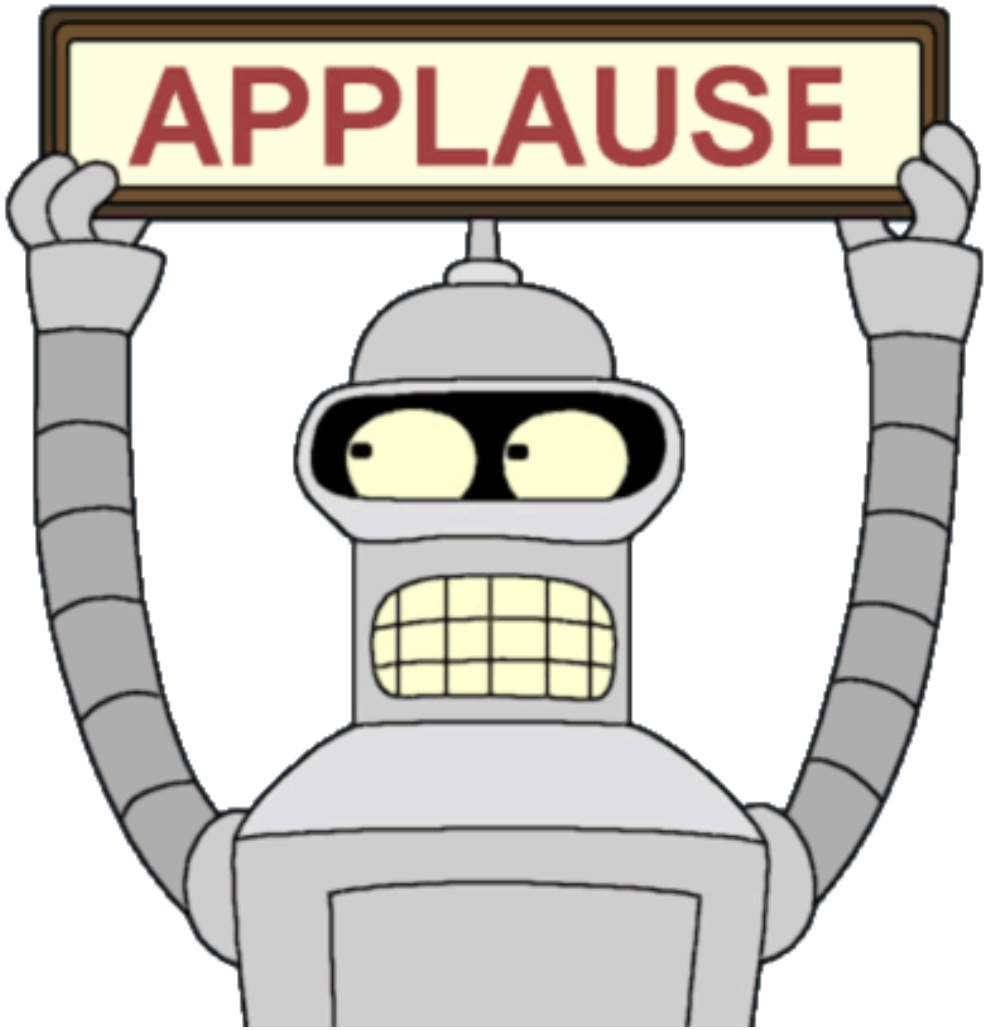
Sätt att förbättra hälsan

- Upphandla support och utveckling
- Kravställ att upphandlad utveckling ska planeras i dialog med huvudprojekt och delas tillbaka
- Kravställ nivå gällande delleverabler som dokumentation och testfall
- Dela vilka öppna programvaror som används inom er organisation
- Identifiera kritiska programvaruprojekt och bidra tillbaka
- Främja att andra att bidra tillbaka
  - EC ska ex. lansera ett bug bounty-program för kritiska projekt

Slutsatser och medskick

- Hälsa och hållbarhet hos öppen programvara är centralt för en säker och robust digital infrastruktur
- Offentlig sektor mfl. behöver se över hur de kan bidra till att hälsan kan förbättras för att minimera risker för sårbarheter
- Stöd och vägledning behövs kring hur hälsan kan beaktas i en anskaffningsprocess

Photo by Omer Sonido | https://unsplash.com/photos/LEMtekMLW4o


APPLAUSE