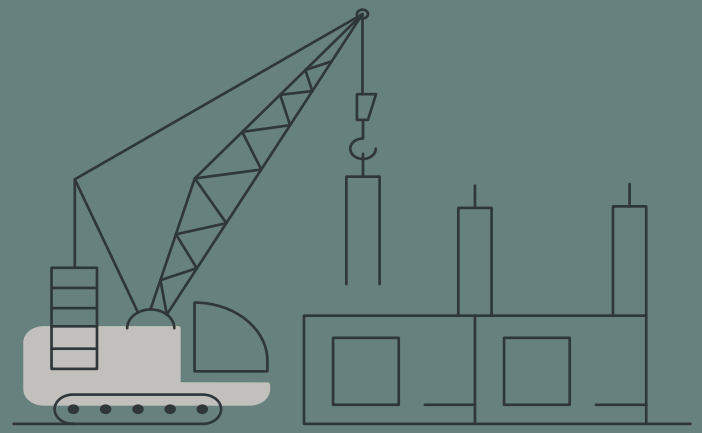
IM_

Sikre digitale samarbejder i byggeriet

Cyber-teknologiske løsninger

Implement Consulting Group • Anders Balslev, Partner

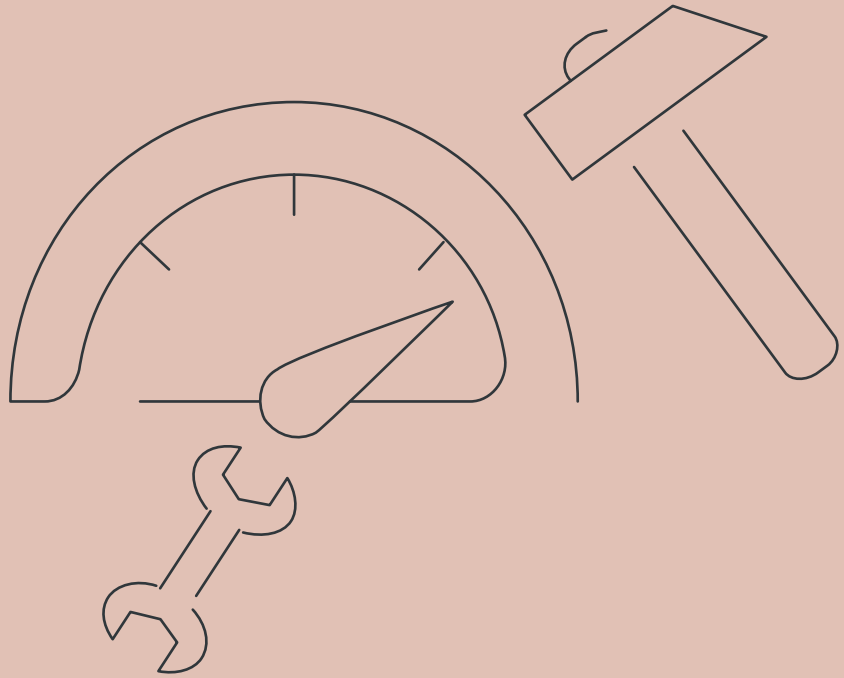
Byggebranchen er i stigende grad digitaliseret med BIM-modeller, IoT-sensorer og cloud-baserede samarbejdsplatforme. Det betyder:



Midlertidige netværk på byggepladser:	Ofte uden stærk segmentering, hvilket gør dem sårbare.
Mange aktører og systemer	Entreprenører, rådgivere og leverandører med forskellige sikkerhedsniveauer skaber en kompleks angrebsflade
Lovkrav som NIS2	Byggeriet bliver omfattet af EU's krav til kritisk infrastruktur, hvilket betyder dokumenteret risikostyring og incident response.
Høj afhængighed af tredjepartsleverandører	Underleverandører har ofte lavere sikkerhedsniveau, hvilket gør dem til svage led i værdikæden
Lav awareness hos medarbejdere	Mange i branchen har begrænset viden om cybertrusler, hvilket gør phishing og social engineering til en stor risiko.
Hvem er det reelt der arbejder på pladsen?	Danmark oplever en stigende grad ad spionage i alle brancher - også i byggebrancen

IM_

Midlertidige netværk på byggepladser



Udfordring

Midlertidige netværk er ofte sat op hurtigt uden stærk segmentering eller sikkerhedspolitikker.

Risiko

Angribere kan udnytte åbne Wi-Fi eller svage adgangskoder til at få adgang til projektdata

Løsning

Brug VPN, segmentering og Zero Trust-principper for at sikre netværket

Qualys®

Scanningsværktøj til brug for identificering af sårbarheder i netværk, miskonfiguration samt asset management

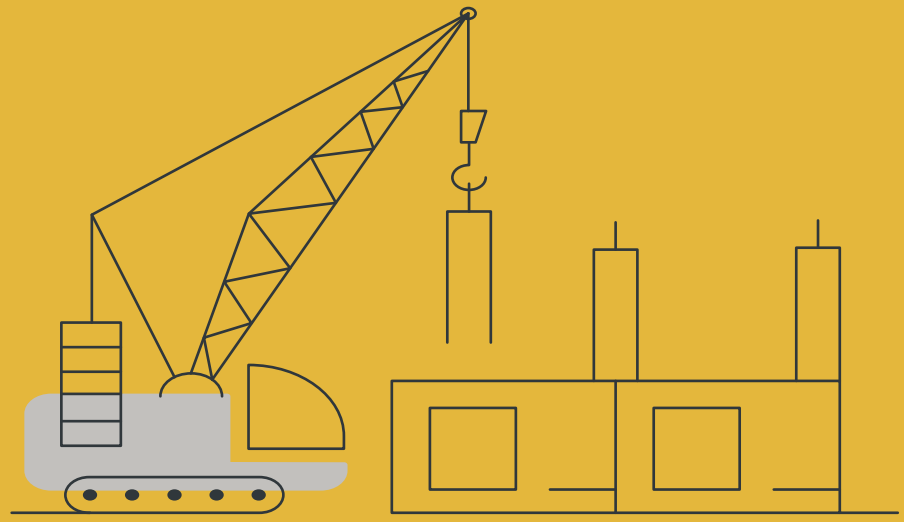
IM_

Mange aktører og systemer

Udfordring
Entreprenører, rådgivere og leverandører arbejder på forskellige platforme med varierende sikkerhedsniveau.

Risiko
En kompromitteret aktør kan blive indgang til hele projektets data.

Løsning
Implementér fælles sikkerhedsstandarder og krav til leverandører (fx NIS2 og ISO27001)



pwc

Deloitte.

DOKUMENTATIONSKRAV
- ISA3000
- Maturity Assesment
- Compliance dokumentation

IM_

Udfordring
Byggeriet bliver omfattet af EU's NIS2-direktiv, som kræver dokumenteret risikostyring og incident response.

Risiko

Manglende compliance kan føre til bøder og tab af kontrakter.

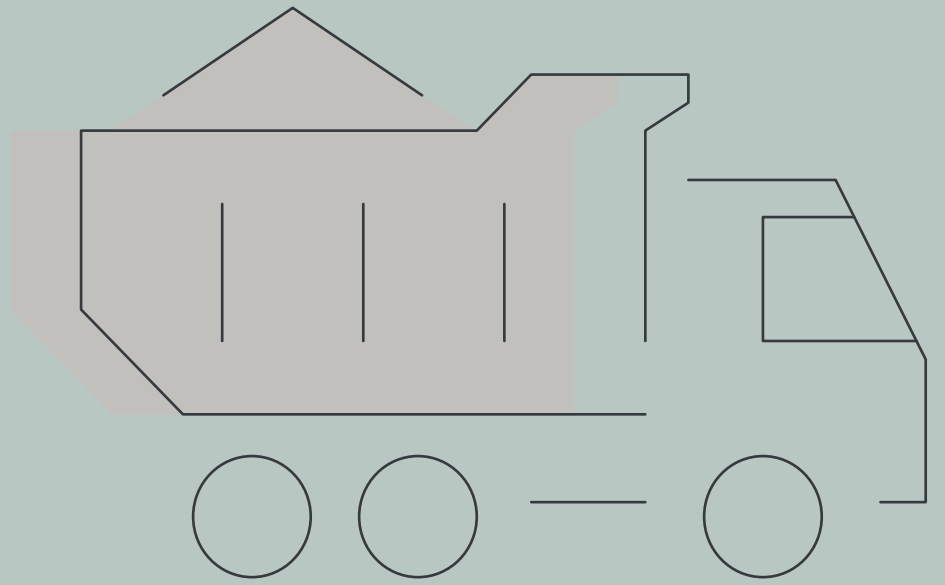
Løsning

Etabler governance, beredskabsplaner og regelmæssige audits.

pwc

Deloitte.

DOKUMENTATIONSKRAV
- ISA3000
- Maturity Assesment
- Compliance dokumentation



Lovkrav som NIS2

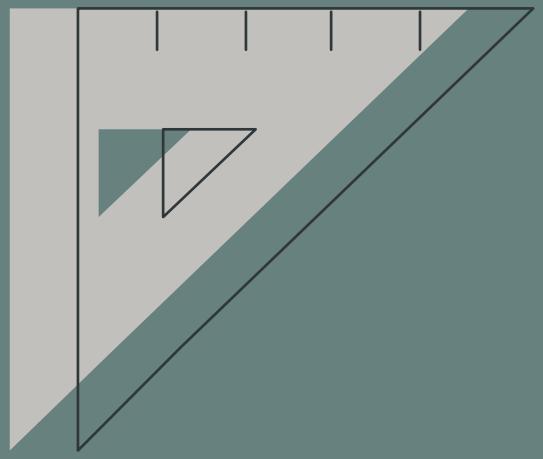
IM_

Høj afhængighed af tredjepartsleverandører

Udfordring
Underleverandører har ofte lavere sikkerhedsniveau.

Risiko
Supply chain-angreb kan ramme hele projektet.

Løsning
Brug leverandørstyring med krav til sikkerhed - f.eks. blockchain til sporbarhed og smart contracts.



pwc

Deloitte.

DOKUMENTATIONSKRAV
- ISA3000
- Maturity Assesment
- Compliance dokumentation

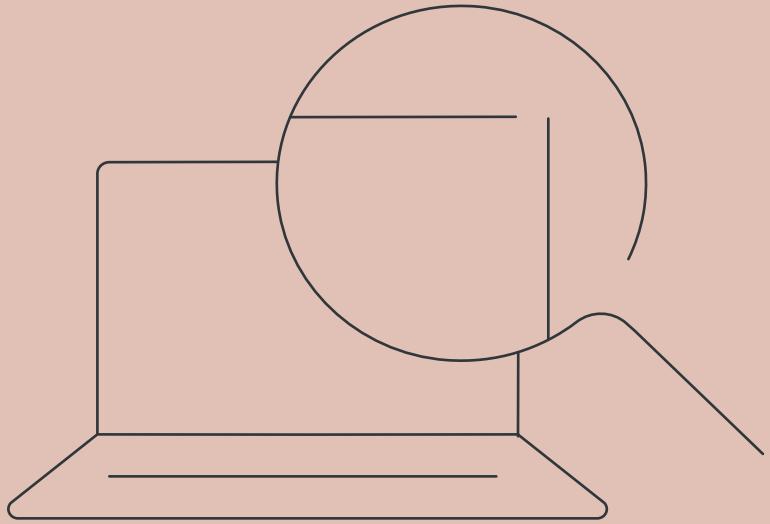
Udfordring
Gammel dokumentation.

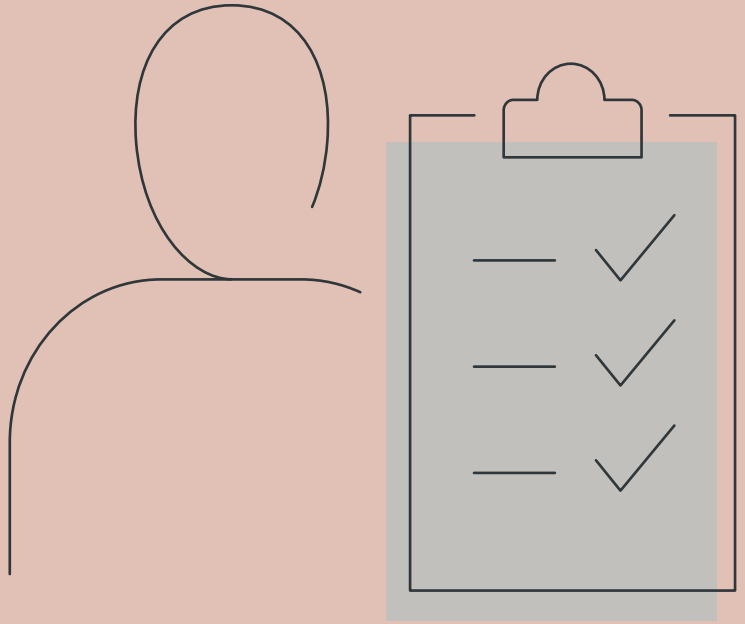
Risiko

Ændringer eller system arv fra udførsel til virkelighed

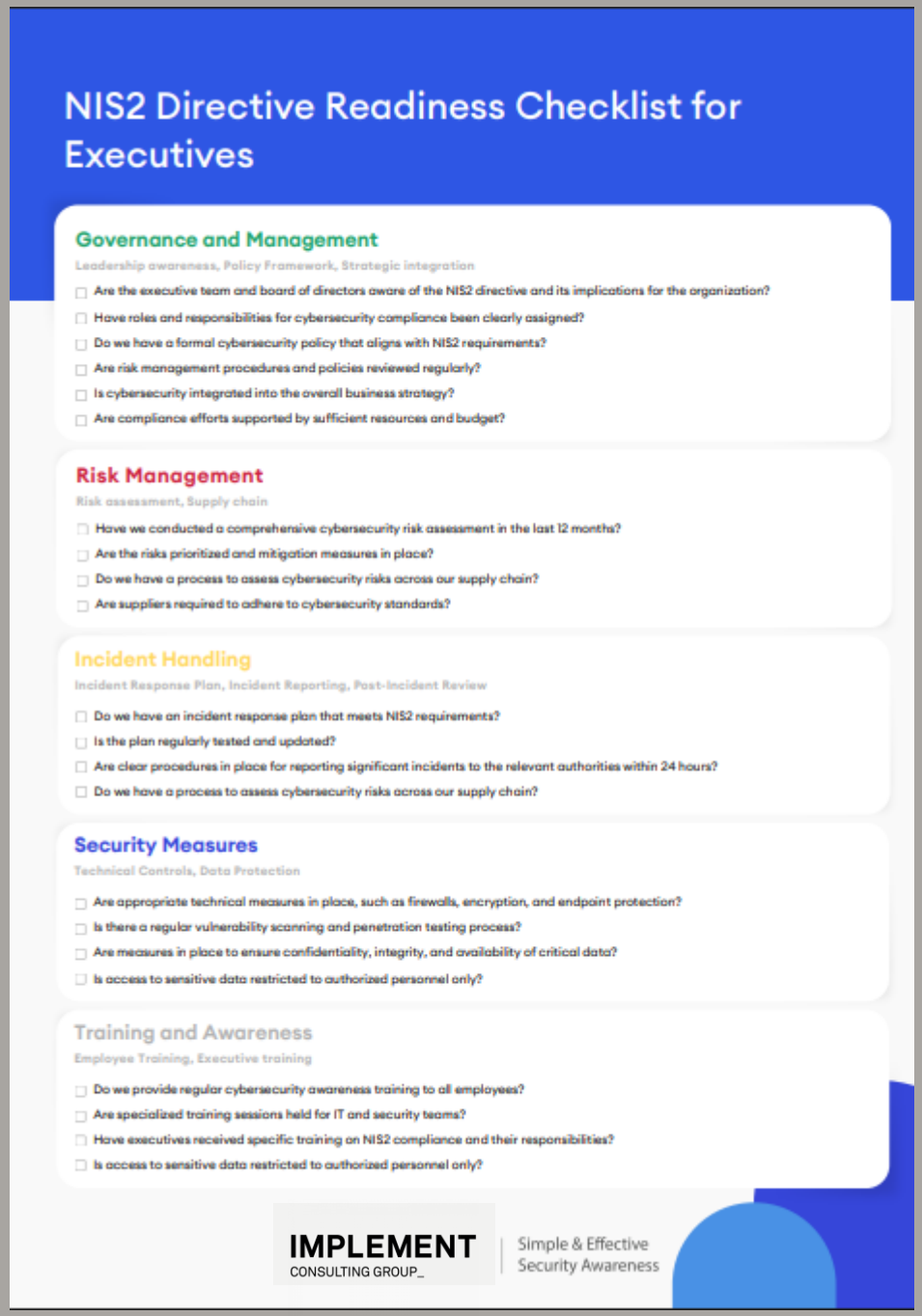
Løsning

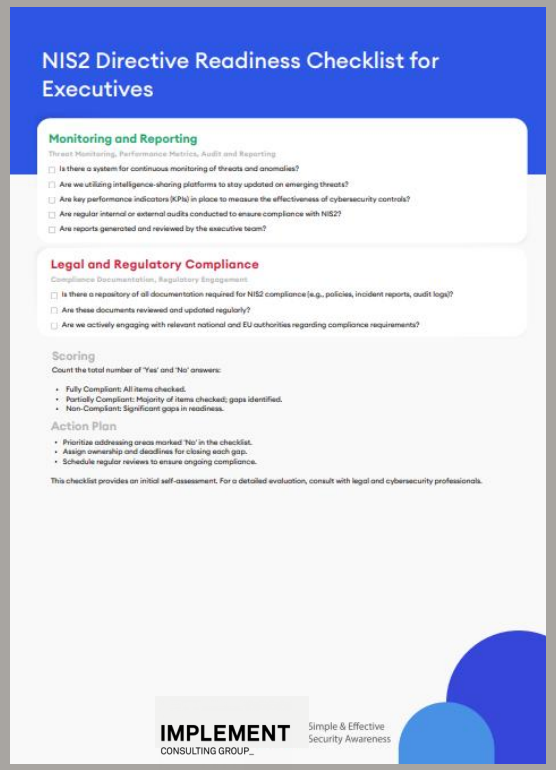
Kontroller ved test at sikkerhedskrav opretholdes løbende ved at stikprøve teste





Tillid er godt



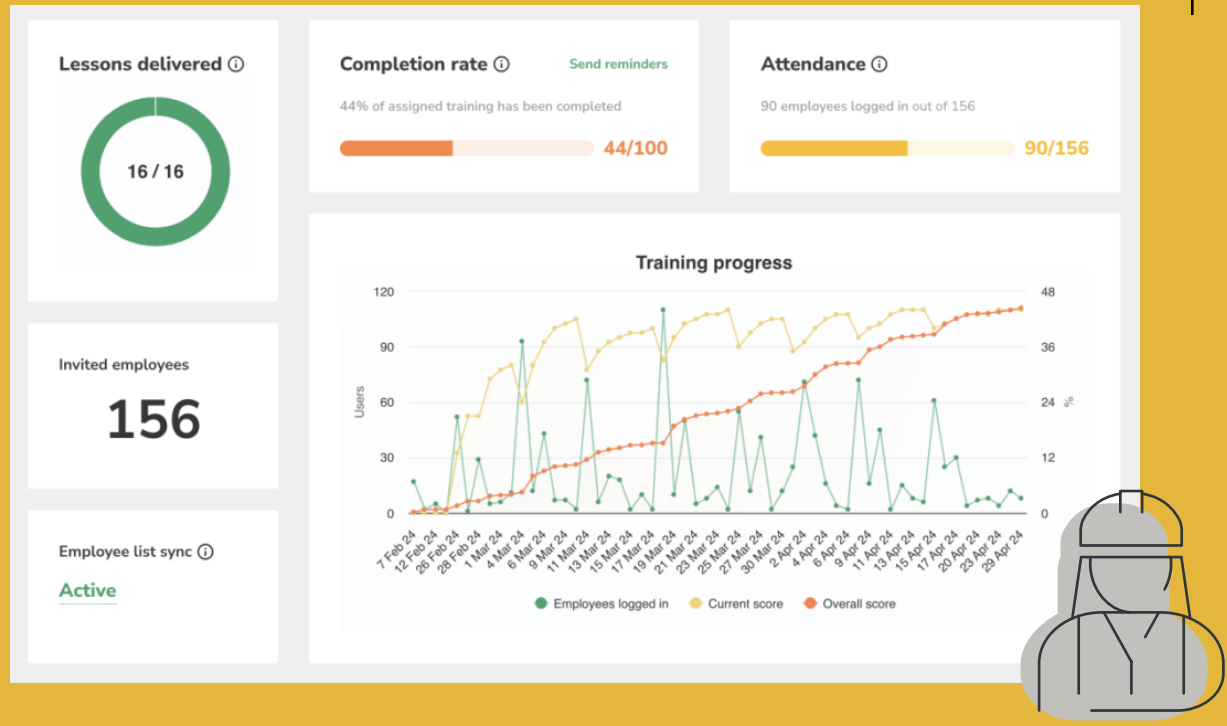


Compliance krav testes

Udfordring
Mange i branchen har begrænset viden om cybertrusler.

Risiko
Phishing og social engineering er en stor trussel.

Løsning
Awareness-træning og simuleringer (fx AwareGO) for alle projektteams



aware GO

Risikobaseret nano-læring til medarbejdere

Lav awareness hos medarbejdere

IM_

Udfordring
Identitetssikring af personer på byggepladsen er ofte svag.

Risiko

Insidertrusler og spionage – Danmark oplever stigende industrispionage i alle sektore

Løsning

Brug digitale ID-løsninger, adgangskontrol og biometriske systemer OG BAGGRUNDSTJEK.

Hvem er det reelt der arbejder på pladsen?

P-Secure

Kontinuerligt baggrundstjek af medarbjdere afhængig af risiko

Thank you.

Anders Balslev

Partner, Implement Consulting Group / .the Tech Collective

Tlf.: +45 52 21 53 55

E-mail: anev@thetechcollective.eu