



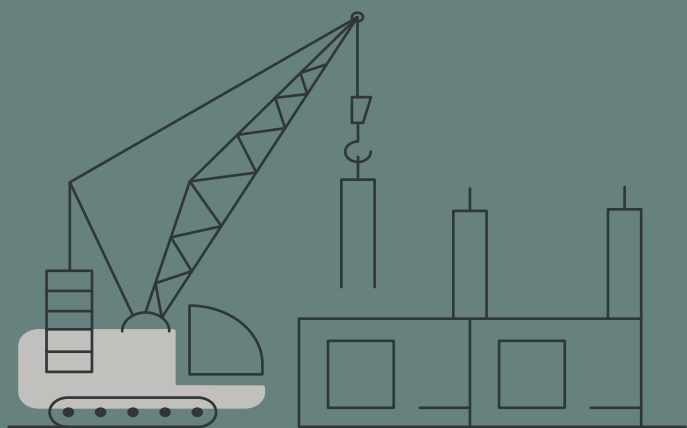
IM\_

# 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 af spionage i alle brancher - også i byggebranchen

## Udfordring

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

## Risiko

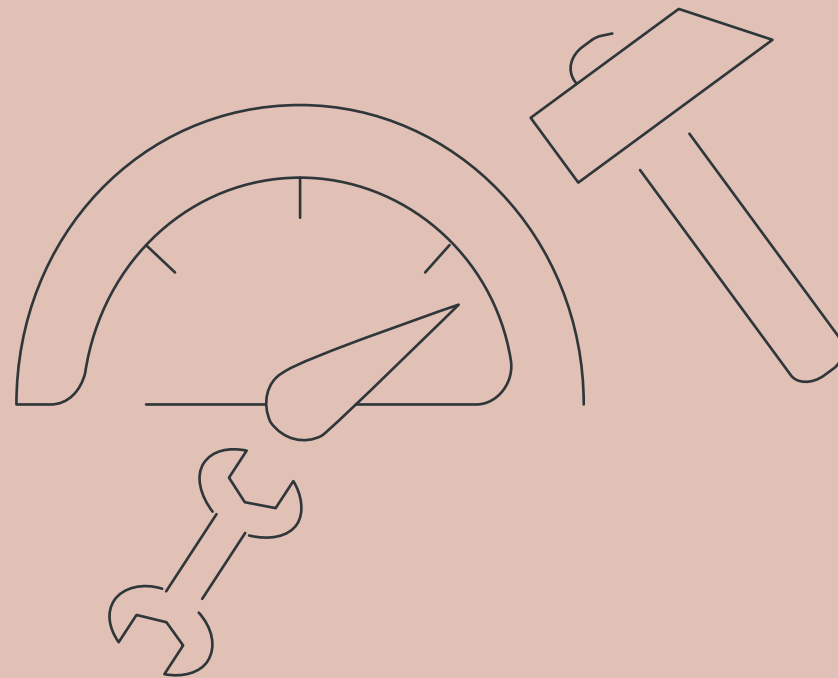
Angribere kan udnytte åbne Wi-Fi eller svage adgangskoder til at få adgang til projektdata

## Løsning

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



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



# Midlertidige netværk på byggepladser

## Udfordring

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

## Risiko

En kompromitteret aktør kan blive indgang til hele projektets data.

## Løsning

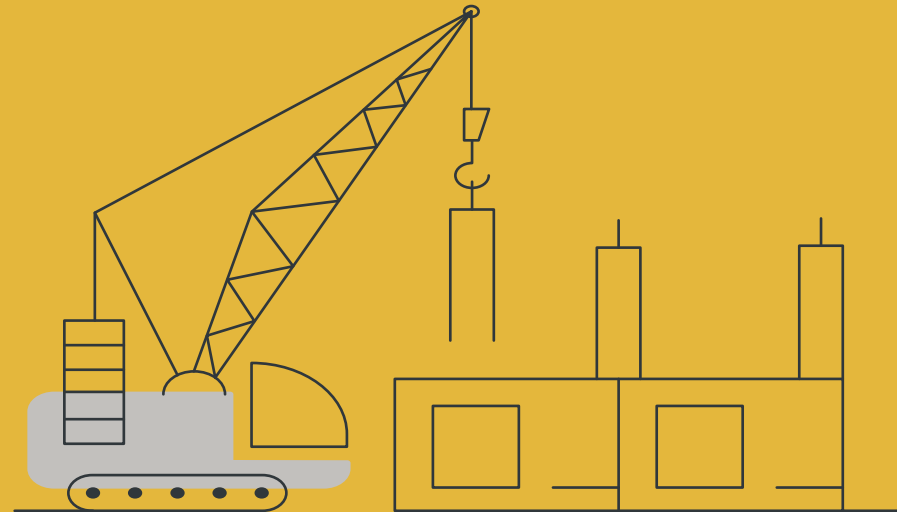
Implementér fælles sikkerhedsstandarder og krav til leverandører (fx NIS2 og ISO27001)

**pwc**

**Deloitte.**



DOKUMENTATIONSKRAV  
- ISA3000  
- Maturity Assessment  
- Compliance dokumentation



# Mange aktører og systemer

## 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

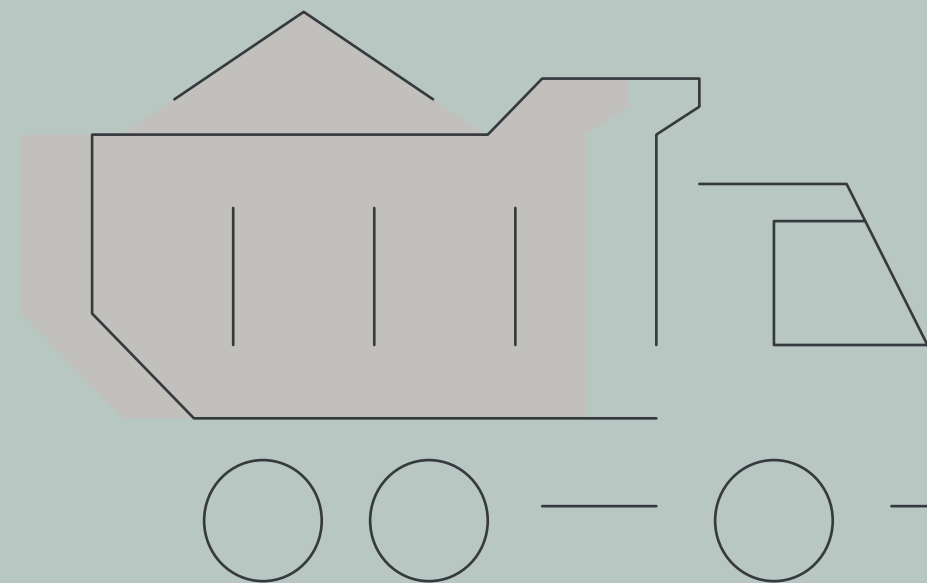
Etabler governance, beredskabsplaner og regelmæssige audits.

**pwc**

**Deloitte.**



DOKUMENTATIONSKRAV  
- ISA3000  
- Maturity Assessment  
- Compliance dokumentation



# Lovkrav som NIS2

## Udfordring

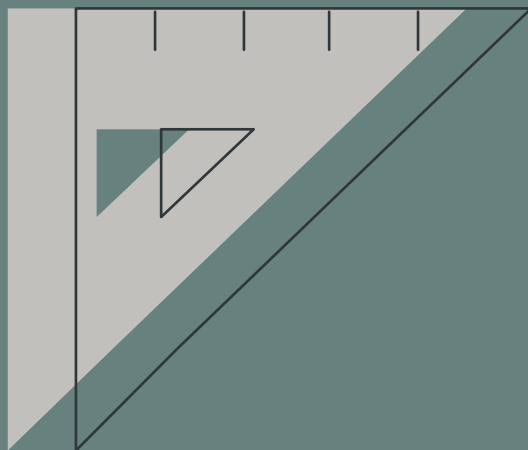
Underleverandører har ofte lavere sikkerhedsniveau.

## Risiko

Supply chain-angreb kan ramme hele projektet.

## Løsning

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



DOKUMENTATIONSKRAV  
- ISA3000  
- Maturity Assessment  
- Compliance dokumentation

# Høj afhængighed af tredjepartslevera ndører

## Udfordring

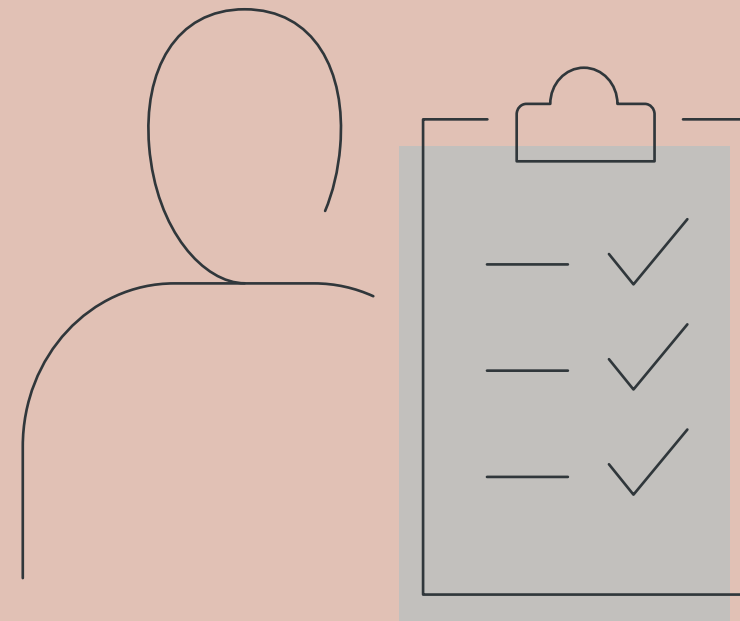
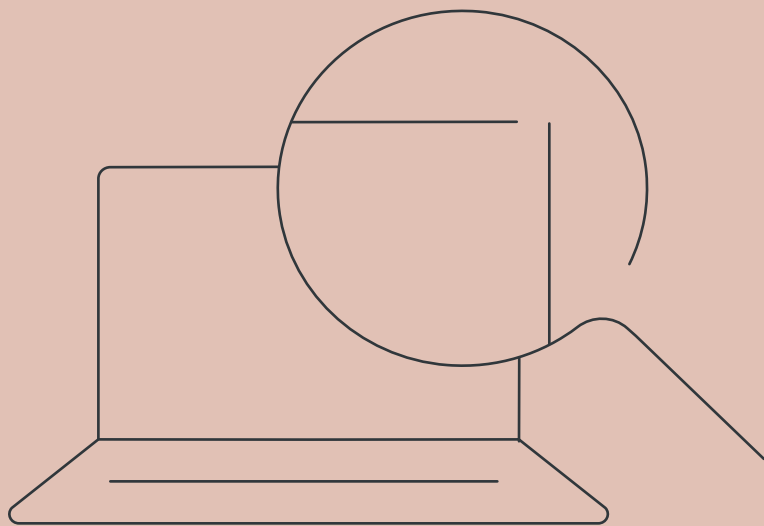
Gammel dokumentation.

## Risiko

Ændringer eller system arv fra udførsel til virkelighed

## Løsning

Kontroller ved test at sikkerhedskrav opretholdes løbende ved at stikprøve teste



# Tillid er godt

# NIS2 Directive Readiness Checklist for Executives

## Governance and Management

Leadership awareness, Policy Framework, Strategic Integration

- ☐ Are the executive team and board of directors aware of the NIS2 directive and its implications for the organization?
- ☐ Have roles and responsibilities for cybersecurity compliance been clearly assigned?
- ☐ Do we have a formal cybersecurity policy that aligns with NIS2 requirements?
- ☐ Are risk management procedures and policies reviewed regularly?
- ☐ Is cybersecurity integrated into the overall business strategy?
- ☐ Are compliance efforts supported by sufficient resources and budget?

## Risk Management

Risk assessment, Supply chain

- ☐ Have we conducted a comprehensive cybersecurity risk assessment in the last 12 months?
- ☐ Are the risks prioritized and mitigation measures in place?
- ☐ Do we have a process to assess cybersecurity risks across our supply chain?
- ☐ Are suppliers required to adhere to cybersecurity standards?

## Incident Handling

Incident Response Plan, Incident Reporting, Post-Incident Review

- ☐ Do we have an incident response plan that meets NIS2 requirements?
- ☐ Is the plan regularly tested and updated?
- ☐ Are clear procedures in place for reporting significant incidents to the relevant authorities within 24 hours?
- ☐ Do we have a process to assess cybersecurity risks across our supply chain?

## Security Measures

Technical Controls, Data Protection

- ☐ Are appropriate technical measures in place, such as firewalls, encryption, and endpoint protection?
- ☐ Is there a regular vulnerability scanning and penetration testing process?
- ☐ Are measures in place to ensure confidentiality, integrity, and availability of critical data?
- ☐ Is access to sensitive data restricted to authorized personnel only?

## Training and Awareness

Employee Training, Executive training

- ☐ Do we provide regular cybersecurity awareness training to all employees?
- ☐ Are specialized training sessions held for IT and security teams?
- ☐ Have executives received specific training on NIS2 compliance and their responsibilities?
- ☐ Is access to sensitive data restricted to authorized personnel only?

**IMPLEMENT**  
CONSULTING GROUP\_

Simple & Effective  
Security Awareness

# NIS2 Directive Readiness Checklist for Executives

## Monitoring and Reporting

Threat Monitoring, Performance Metrics, Audit and Reporting

- ☐ Is there a system for continuous monitoring of threats and anomalies?
- ☐ Are we utilizing intelligence-sharing platforms to stay updated on emerging threats?
- ☐ Are key performance indicators (KPIs) in place to measure the effectiveness of cybersecurity controls?
- ☐ Are regular internal or external audits conducted to ensure compliance with NIS2?
- ☐ Are reports generated and reviewed by the executive team?

## Legal and Regulatory Compliance

Compliance Documentation, Regulatory Engagement

- ☐ Is there a repository of all documentation required for NIS2 compliance (e.g., policies, incident reports, audit logs)?
- ☐ Are these documents reviewed and updated regularly?
- ☐ Are we actively engaging with relevant national and EU authorities regarding compliance requirements?

## Scoring

Count the total number of 'Yes' and 'No' answers:

- Fully Compliant: All items checked.
- Partially Compliant: Majority of items checked; gaps identified.
- Non-Compliant: Significant gaps in readiness.

## Action Plan

- Prioritize addressing areas marked 'No' in the checklist.
- Assign ownership and deadlines for closing each gap.
- Schedule regular reviews to ensure ongoing compliance.

This checklist provides an initial self-assessment. For a detailed evaluation, consult with legal and cybersecurity professionals.

**IMPLEMENT**  
CONSULTING GROUP\_

Simple & Effective  
Security Awareness

# Compliance krav testes

## Udfordring

Mange i branchen har begrænset viden om cybertrusler.

## Risiko

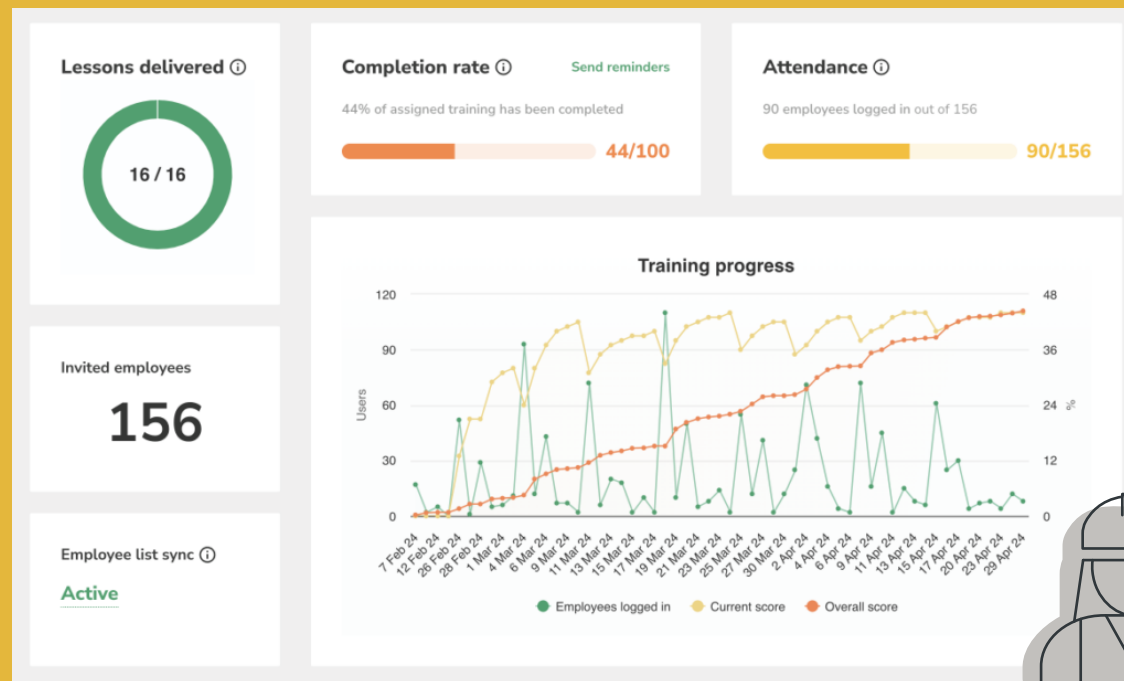
Phishing og social engineering er en stor trussel.

## Løsning

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

aware  
**GO**

Risikobaseret nano-læring til medarbejdere



# Lav awareness hos medarbejdere

## 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.



# P-Secure

Kontinuerligt baggrundstjek af medarbejdere  
afhængig af risiko

# Hvem er det reelt der arbejder på pladsen?

# Thank you.

**Anders Balslev**

**Partner, Implement Consulting Group /  
.the Tech Collective**

**Tlf.: +45 52 21 53 55**

**E-mail: [anev@thetechcollective.eu](mailto:anev@thetechcollective.eu)**

