Bureau Veritas – IT-Security

Bureau Veritas er en af verdens største virksomheder inden for inspektion, klassificering, rådgivning og certificering. Virksomhedens kernekompetence er kvalitet, miljø, arbejdsmiljø, sikkerhed og social ansvarlighed. Projektet vil være forankret i IT-Security afdelingen. Her arbejder man bl.a. med den kommende lovgivning NIS2, der kommer til at rumme en del nye krav til Kritisk infrastruktur hos virksomheder. NIS2 er et EU-direktiv, som skal sikre infrastrukturen- og samfundskritiske tjenester med nedbrud og cybertrusler gennem et ensartet niveau af cyber- og informationssikkerhed i EU.
Der er i dag kun ganske få virksomheder, der er underlagt nuværende NIS fra Staten. Iht. NIS2 vil en langt større andel på tværs af sektorer og brancher blive underlagt dette af staten, hvilket vil komme bag på flere virksomheder. Kravene er primært udformede som evnen til at risikovurdere og evnen til at reagere/rapportere en evt. IT-hændelse indenfor 24 timer. Lovgivningen forventes gældende i dansk lov med udgangen af 2024.

CASE: Gennem strategisk analyse og udvikling skal der udarbejdes værktøjer til risikovurdering/GAP-analyse i flere niveauer afhængigt af virksomhedsstørrelse og kompleksitet/branche. Indsigterne benyttes til at udvikle produkter/business support-ydelser med henblik på at sikre virksomhedernes gevinst af deres investeringer gennem Bureau Veritas' ydelser og rådgivning. Hertil skal teamet indtænke forankring og kommercialisering gennem marketingskampanger og Auditor træning til medarbejderne. Projektet skal i sidste ende understøtte en øget andel af IEC62443 og ISO27001 certificeringer hos Bureau Veritas.

OVERBLIK

Virksomhed	Bureau Veritas Danmark – IT-Security
Lokation	Oldenborggade 25-31, 7000 Fredericia
Kontaktperson	Jens Bertelsen, Business Developer & ISO27001 Lead Auditor

VIRKSOMHEDSPROFIL

Bureau Veritas er en af verdens førende- og største virksomheder inden for inspektion, klassificering, rådgivning og certificering, med kernekompetencer inden for kvalitet, miljø, arbejdsmiljø, sikkerhed og social ansvarlighed. De hjælper virksomheder med at fastholde og udvikle deres brands, værdier og forretning.

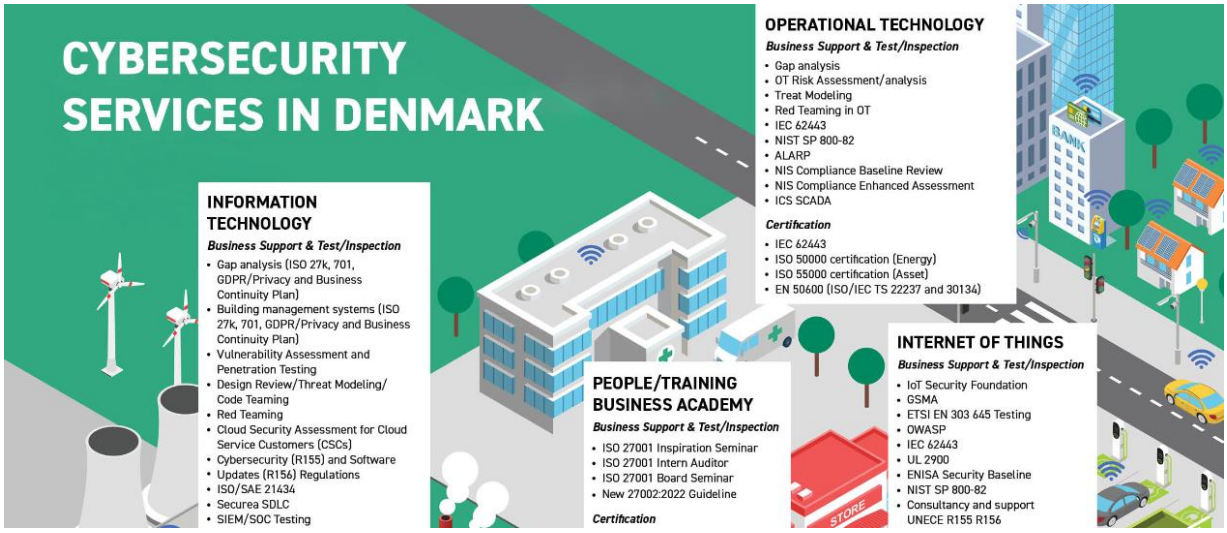
Det kommende projekt er lokaliseret i Bureau Veritas' forretningsområde 'IT-Security', hvorfor omdrejningspunktet i casen vil omhandle Cybersecurity, mere specifikt hvordan Bureau Veritas kan understøtte virksomheder med deres opretholdelse af IT-sikkerhed iht. standarter og lovgivning, gennem rådgivning med henblik på at kunne øget antallet af IEC62443 og ISO 27001-certificeringer på sigt.

Bureau Veritas tilbyder en række specifikke serviceydelser, som illustreret nedenfor. IT-Security hjælper med at imødekomme virksomheders behov gennem ledelse, rådgivning og konsultering til inspektion/audit og træning for at opnå klassificering og certificeringer.

Kilde:https://bureauveritas.dk/da/cybersecurity

Bureau Veritas arbejder med Cybersecurity set ud fra de tre søjler og persektiver; mennesker, proces og teknologi. De 3 søjler sigter mod at adressere, at IT-løsninger ikke kan implementeres alene uden en stærk bevidsthed om menneskers evne til at forstå risici og trusler ifm. Cybersecurity, for at kunne skabe den nødvendige motivation mod adfærdsmæssig ændring og forankring.

Søjlerne afspejles i den brede portefølje, som IT-Security leverer i dag på tværs af brancher og sektorer, bl.a. gennem Industriel Cybersecurity (OT), tilsluttede produkter (IOT) og informationsteknologi (IT), hvor de rådgiver og auditerer virksomheder med at sætte akkrediteringer og licenser i drift, bl.a. gennem IEC 62443-certificering (OT) og ISO 27001-certificering (IT).



Kilde:https://bureauveritas.dk/da/cybersecurity

Cybersecurity bliver generelt en større prioritet for virksomheder, men i dag er kun ganske få virksomheder underlagt nuværende NIS-lovgivning (net- og informationssikkerhed). Med den kommende NIS2 lovgivning vil en langt større andel virksomheder (minimum 250 ansatte) på tværs af sektorer og brancher blive underlagt dette af staten, hvilket vil komme bag på flere virksomheder.
NIS2 er et EU-direktiv, som skal sikre infrastrukturen- og samfundskritiske tjenester mod nedbrud og cybertrusler gennem et ensartet niveau af cyber- og informationssikkerhed i EU. Kravene iht. NIS2 er primært udformede som evnen til at risikovurdere og evnen til at reagere/rapportere en evt. IT-hændelse indenfor 24 timer. Lovgivningen forventes gældende i dansk lov med udgangen af 2024.
Dette vil være gældende for industrielle organisationer, hvor den kritiske infrastruktur styres gennem operationel teknologi (OT), herunder energi og forsyning, olie og gas, marine og offshore, vand, fødevare, kemi og landbrug, som alle tilhører kritiske forsyningskæder for samfundet.
Bureau Veritas vision for OT er, at der ingen sikkerhed, pålidelighed og tilgængelighed er uden cybersikkerhed.
Digital sikkerhed er af stigende betydning, fordi flere og flere OT/IT-systemer (PLC'er, ICS/SCADA-enheder og understøttende komponenter) er forbundet til IP-netværk. For eksempel til at overvåge og kontrollere processer, (forudsigende) vedligeholdelse eller fakturering.

I forbindelse med de kommende NIS2 regler og industrielle krav er behovet for uafhængige tredjepartsorganisationer intensiveret, da mange virksomheder ikke er forberedte og klar over, at dette er på vej.
Bureau Veritas ønsker at være på forkant- og levere serviceydelser, der understøtter virksomheder i processen. Bureau Veritas har endnu ikke fuldt ud identificeret, hvilke produkter/business support ydelser de bør udbyde, for at sikre virksomhedernes gevinst af deres investeringer gennem Bureau Veritas ydelser og rådgivning.

CASEBESKRIVELSE

Bureau Veritas håber derfor at finde et team, der gennem strategisk analyse og udvikling kan hjælpe IT-Security afdelingen med at finde og udvikle gode værktøjer og hjælpemidler til risikovurdering og GAP-analyser i flere niveauer afhængig af virksomhedsstørrelse og kompleksitet/branche. Herefter udvikles Bureau Veritas produkter/business support ydelser så virksomhederne går til Bureau Veritas og henter gevinsten af deres investeringer.

Der er ganske mange OT virksomheder med over 250 ansatte der rammes, men som slet ikke er oplyst eller har energi til at tænke i disse retninger. Virksomheden ønsker derfor at teamet med sparring fra salgsafdelingen, og andre afdelinger som fx marketing, udarbejder kommercielt materiale f.eks. white papers med gode argumenter og illustrationer for, hvorfor det er vigtigt for pålagte markeder og virksomheder.
Endeligt skal teamet udarbejde og fastlægge et træningsforløb for auditorerne med henblik på tilegnelse af viden og kompetencer, så virksomhedens frontpersonale kan tage snakken i marken. Det samlede projekt skal på sigt understøtter en øget andel af IEC 62443 og ISO 27001-certificeringer hos Bureau Veritas.
Qua begrænset ressourcer i IT-Security afdelingen må teamet gerne inddrage muligheden for udvikling af selvhjælpsværktøjer, der kan uddelegeres til virksomhederne, så alle ydelser og opgaver ikke drives og bor hos Bureau Veritas. Marketingsafdelingen arbejder pt på en kundeportal løsning, hvor Cybersecurity er et af emnerne.

KONKRETE OPGAVER

De konkrete opgaver for casen er inddelt i følgende faser:

0. **Fase: Onboarding og fastlæggelse af overordnet målsætninger.**
   - 0.1. Onboarding til Bureau Veritas og IT-Security afdelingen, værdier, strategier, kultur og det marked, de operer i.
   - 0.2. Forventningsafstemning: Frekvens af feedback og løbende sparring.
   - 0.3. Dybdegående introduktion af udfordringer og ønsket resultater.
   - 0.4. Diskuter de forskellige faser og vægtning/prioritering af opgaver, så tiden bliver brugt optimalt.
   - 0.5. Fastlæg arbejdsfordeling, kalenderstyring, mødetider mv.

1. **Fase: Gennemfør strategiske analyser med henblik på at udvikle værktøjer og hjælpemidler til risikovurdering/GAP-analyse til OT-markederne.**

1.1 Kortlæg kommende krav og standarter der vil medfølge den nye NIS2 lovgivning med henblik på at identificere, hvilke behov pålagte virksomheder vil have for hjælpeværktøjer og support.
1.2 Gennem analyse inddeles markederne i forskellige modenhedsklasser ud fra kriterierne, som f.eks.:
1.2.1 Virksomhedsstørrelse
1.2.2 Kompleksitet i branchen
1.2.3 Mfl.
1.3 Analyser hvilke gode værktøjer der kan udarbejdes til GAP-analyse og risikovurdering. Hertil er de vigtigt, at de udarbejdes de forskellige modenhedsklasser (gerne som selvhjælpsværktøjer). I bør derfor udvikle:
1.3.1 Værktøjer
1.3.2 Hjælpemidler
1.3.3 Selvhjælpsværktøjer

2. **Fase: Framing og udvikling af produkter og business support ydelser med henblik på at sikre, at virksomhederne går til Bureau Veritas og henter gevinsten af deres investeringer.**
2.1 Ud fra en åben udviklingsproces udarbejdes framework for nye produkter og business support ydelser. Det er vigtigt, at disse er alignmet med NIS2 lovgivningens krav og standarter. Det er hertil vigtigt at:
2.1.1 Der udarbejdes forskellige frameworks til de respektive modenhedsklasser.
2.2 Udvikling af de forskellige produkter og business support ydelser, der skal indgå i de forskellige frameworks. Hertil er det vigtigt at:
2.2.1 At de forskellige produkter og business support ydelser tilpasses de forskellige modenhedsklasser og ledelsesniveauer.

3. **Fase: Udvikling af kommercielle argumenter og marketingskampanger.**
3.1 Ud fra udarbejdet produkter og business support ydelser og dertilhørende værktøjer udarbejdes der idéer til kommercielle salgsargumenter, der kan sikre en større efterspørgsel i markedet. Disse skal understøtte et øget antal certificeringer hos Bureau Veritas.
3.2 I samarbejde med salgsafdelingen og marketingsafdelingen udarbejdes materiale i form af:
3.2.1 Argumenter
3.2.2 Marketing/kampagner med gode argumenter for at se på dette område.
3.2.3 White papers der illustrer fordele og gevinster ved dette.
3.2.4 Mfl.

4. **Planlæg auditor træning og kompetenceudvikling ud fra de nyudviklede værktøjer og indsigter med henblik på forankring.**
4.1 Afdæk hvordan et træningsforløb af overstående bør foregå. Det er vigtigt, at I planlægningen af dette tager højde for, at auditorerne tilføres viden og kompetencer iht. at frontpersonale kan tage snakken i marken.
4.2 Påbegynd træningsforløbene med henblik på forankring og kvalitetssikring.

ØNSKET UDBYTTE FOR VIRKSOMHEDEN

Efter forløbet vil virksomheden gerne stå i hånden med:

- ✓ Udarbejdet værktøjer og hjælpemidler til risikovurdering / GAP-analyse til de forskellige modenhedsklasser.
- ✓ Framing og udvikling af Bureau Veritas' produkter og business support ydelser til de forskellige ledelsesniveauer.
- ✓ Kommercielle argumenter og marketingskampanger.
- ✓ Udviklet- og påbegyndt træningsforløb af auditorerne.

RELEVANTE FAGLIGHEDER TIL CASEN

- Informationsteknologi, Cybersecurity og informationssikkerhed.
- IT-behandling, -implementering og -forankring.
- Security Awareness, træning, digitale værktøjer, e-learning og blended learning.
- Kulturændringer, adfærdsdesign, forandringsledelse og psykologi.
- GAP- og risikoanalyser.
- Compliance, standarter, certificeringer, lovgivning og jura.

TALENTPROFIL

Gennem forløbet har du en mulighed for at starte en karriere hos Bureau Veritas, som ikke bare er et job, men en mulighed for at være med til at skabe en fremtid, hvor der er fokus på sikkerhed og en grønnere retning i samfundet. Koncernen er ca. 82.000 medarbejdere på globalt plan og ca. 200 I Danmark. Bureau Veritas bestræber sig på at skabe et sundt arbejdsmiljø og -liv, hvor forståelse, personlig udvikling og ikke mindst professionel fremgang spiller en afgørende rolle.

Virksomheden arbejder med Cybersecurity set ud fra tre søjler og perspektiver; mennesker, proces og teknologi. De 3 søjler sigter mod at adressere, at IT-løsninger ikke kan implementeres uden en stærk bevidsthed om, menneskers evne til at forstå risici og trusler ifm. Cybersecurity, og kunne skabe den nødvendige motivation mod adfærdsmæssig ændring og forankring.

Bureau Veritas ønsker derfor ikke kun at sammensætte et team af tekniske fagligheder, men et team der afspejler deres måde at tænke- og arbejde med Cybersecurity på. De håber derfor at kunne sammensætte et mangfoldigt team med forskellige fagligheder inden for de 3 søjler.

Virksomheden forventer samtidigt at finde profiler, der grundlæggende er struktureret, udadvendte, nysgerrige, gode til at lytte og skabe refleksion. Projektet berører mange snitflader og niveauer, hvorfor det forventes at du kan begå dig og kommunikere på tværs af samme.

Teamet vil komme til at arbejde under Jens, der arbejder med frihed under ansvar. I vil derfor få stor medindflydelse og frihed i udviklingsprocessen, hvorfor det forventes at du trives med at arbejde selvstændigt, men også kan indgå i teams.