Whitepaper
ISO 62443

AudITvision
IT-auditors

Uw partner
in ISO 62443

Inhoud

Introductie

AudITvision biedt voor uw IT-omgeving: van hardware, applicatiesystemen, infrastructuur en software tot producten, diensten en processen interne auditdiensten met betrekking tot ISO 62243.

Voor een interne auditdienst betekent dit dat u kunt vertrouwen op een gecertificeerde aanpak die door middel van internationaal erkende rapportages en het AudITvision-keurmerk aantoont dat uw processen betrouwbaar en veilig zijn. Dit geeft vertrouwen aan interne en externe stakeholders en dient als aantoonbaar bewijs van naleving van wet- en regelgeving, zoals de EU Cybersecurity Act.

Onze auditdiensten signaleren risico's voordat ze schade kunnen veroorzaken, en begeleiden uw organisatie doelgericht naar succes – een zekerheid waarop u kunt bouwen.

Tegelijkertijd beschermen we uw meest waardevolle bezit in dit digitale tijdperk: data. Nieuwe digitale businessmodellen draaien om data. Met AudITvision heeft u een betrouwbare en ervaren partner aan uw zijde – niet alleen op het gebied van informatiebeveiliging en IT-security, maar ook op het vlak van gegevensbescherming en privacy.

Hoofdstuk 1 **Belang van ISO 62443 voor organisaties**

De druk op organisaties om hun digitale weerbaarheid te versterken neemt snel toe. Niet alleen door toenemende cyberdreigingen, maar ook door de groeiende hoeveelheid Europese regelgeving op het gebied van cybersecurity. Wet- en regelgeving zoals de Cybersecurity Act, de NIS 2-richtlijn en de Cyber Resilience Act leggen steeds meer nadruk op aantoonbare beveiligingsmaatregelen. Certificering op basis van internationale normen, zoals ISO 62443, wordt daarmee niet alleen een kwaliteitskenmerk, maar ook een strategische noodzaak.

Deze regelgeving moedigt bedrijven aan om een cybersecuritycertificering te behalen en zo aan te tonen dat hun producten voldoen aan cybersecurity-normen en voorbereid zijn op de uitdagingen van Industrie 4.0. Certificering is nog vrijwillig, tenzij Europese of nationale wetgeving anders bepaalt. De Europese Commissie zal regelmatig evalueren of bepaalde procedures verplicht moeten worden. EU-lidstaten stellen regels op voor sancties bij overtreding van de vereisten of de certificeringsschema's. In sommige landen, zoals Duitsland, is al nationale wetgeving van kracht.

Andere voorbeelden van Europese regelgeving zijn de Cyber Resilience Act en de Radio Equipment Directive, die eisen stellen aan processen en/of producten met betrekking tot best practices op het gebied van beveiliging. Niet-naleving kan leiden tot boetes tot 2,5% van de jaarlijkse omzet.

Bescherming van investeringen in Industrie 4.0-systemen is een belangrijk aandachtspunt. Klanten willen zeker zijn dat zij investeren in veilige producten, oplossingen of diensten die in overeenstemming zijn met Europese of nationale wetgeving. Bedrijven doen er daarom goed aan om hun operaties, producten, oplossingen en diensten te laten toetsen aan een internationale cybersecuritynorm, zoals ISO 62443. Ook bij de selectie van leveranciers en onderaannemers wordt steeds vaker gekeken naar de implementatie van deze standaard.

De implementatie van NIS 2.0 zal vooral grotere organisaties (vanaf 250 medewerkers en een omzet boven de €50 miljoen) in kritieke of essentiële sectoren aanzetten tot het nemen van beveiligingsmaatregelen en het kunnen aantonen van conformiteit van producten,

diensten en processen. Deze eisen zullen ook doorwerken naar leverancierssketens. Volgens de Europese Commissie behoort IEC 62443 tot de relevante normen waarmee rekening moet worden gehouden.

Hoofdstuk 2 **Wat houdt de ISO 62443 in?**

De ISO 62443-norm is een internationale standaard gericht op de beveiliging van industriële automatiserings- en controlesystemen, ook wel bekend als Industrial Automation and Control Systems (IACS). Deze systemen worden gebruikt in uiteenlopende sectoren, zoals de technologie- en ontwikkelingssector. De norm heeft als doel om cybersecurity op een gestructureerde en risicogebaseerde manier te verankeren in het ontwerp, de implementatie en het beheer van industriële systemen.

De standaard is van toepassing op alle betrokken partijen binnen het IACS-ecosysteem: van product-leveranciers en systeemintegratoren tot asset owners. Hierbij ligt de nadruk niet alleen op technische beveiligingsmaatregelen, maar ook op processen, verantwoordelijkheden en beleidsvoering. Belangrijke uitgangspunten van de norm zijn de bescherming van mens en milieu, de beschikbaarheid van installaties, de efficiëntie van processen en de kwaliteit van de productie.

Opbouw van de norm

De ISO 62443 bestaat uit vier hoofddelen:

1. Algemene richtlijnen

Deze bieden basisprincipes en terminologie die gelden voor alle onderdelen van de standaard.

2. Beheersystemen (policies en procedures)

Richtlijnen voor het opzetten van een cybersecurity managementsysteem (CSMS) binnen industriële omgevingen. Dit deel is vooral van belang voor asset owners.

3. Systeemeisen (IACS)

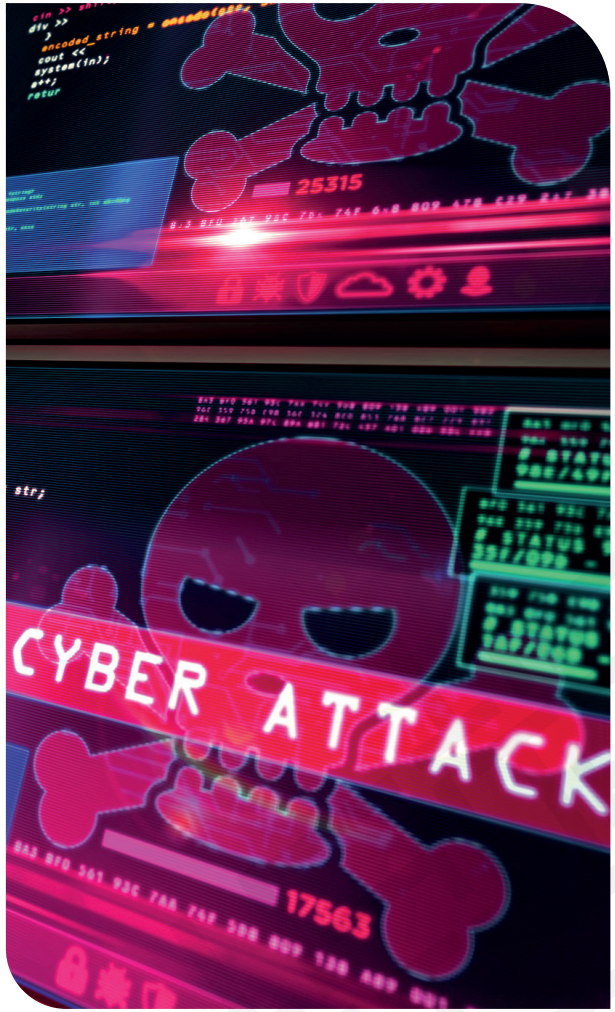
Technische eisen aan complete automatiserings-systemen, inclusief netwerkarchitectuur, risicobeoordeling, toegangsbeheer en monitoring.

4. Componentbeveiliging

Richtlijnen voor het beveiligen van individuele componenten zoals embedded devices, systeemcom-ponenten, werkstations en applicaties.

Elke laag binnen de standaard bouwt voort op het vorige niveau en draagt bij aan een geïntegreerde aanpak van industriële cybersecurity. Zo wordt bijvoorbeeld vereist dat componenten veilig ontworpen zijn, dat systemen correct worden geïntegreerd en dat het overkoepelende beleid en beheer op orde is.

ISO 62443 biedt daarmee een robuust en flexibel raamwerk waarmee organisaties hun cybersecurity kunnen verbeteren, compliance kunnen aantonen en risico's kunnen beheersen in een steeds complexer en digitaler industrieel landschap.



IEC 62443
Security fot Industrial Automation and Control Systems

General	Policies & Procedures	System	Component/ Product	Profiles	Evaluation
1-1 Terminoloy concept and models[1]	2-1 Security program requirements for IACS asset owners[2]	3-1 Security program technologies for IACS	4-1 Secure product development lifecycle requirements	5-x Profiles within the framework of part 1-5	6-1 Security evaluation methodology IEC 62443-2-4
1-2 Master glossary of terms and abbreviations	2-2 Security program rating	3-2 Security program risk assessment for system design	4-2 Technical security requirements for IACS comonents		6-2 Security evaluation methodology IEC 62443-4-2
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels			
1-4 IACS securtiy lifecycle and use-cases	2-4 Security program requirements for IACS providers[3]				
1-5 Scheme for IEC 62443 cyber-security profiles	2-5 Implementation quidance for IACS asset owners				
1-6 Application of IEC 62443 to the industrial internet of things					

Published

Published/next edition planned

1: Edition 2 planned for 2026
2: Edition 2 planned for 2024
3: Edition 2 planned for 12/2023
Edition 2 planned for 2026/27

In development /planned

Hoofdstuk 4 **Onze aanpak: interne audit conform ISO 62443**

Als extern bieden wij organisaties een interne auditdienst aan om hen voor te bereiden op een externe certificering volgens de ISO 62443-norm, die zich richt op cybersecurity voor industriële automatiserings- en controlesystemen (IACS). Onze aanpak bestaat uit vijf stappen:

1. Intake en scopedefinitie

De eerste stap is een grondige intake, waarbij we samen met de klant de scope van de audit vaststellen. Dit omvat het bepalen van de normdelen die relevant zijn voor de organisatie, bijvoorbeeld ISO 62443-2-1, die richtlijnen biedt voor het cybersecurity-managementsysteem. We identificeren ook de kritieke systemen en processen die onder de audit vallen.

2. Audit op locatie en documentanalyse

Onze auditors voeren een gedetailleerde beoordeling uit op locatie. Dit omvat interviews met medewerkers, het observeren van processen en het evalueren van technische systemen. Daarnaast analyseren we de bestaande documenten, zoals risicobeoordelingen, beleidsdocumenten en systeemconfiguraties, om te bepalen in hoeverre deze voldoen aan de eisen van de norm.

3. Gap-analyse

Na de audit stellen we een gap-analyse op, waarin we per normvereiste de bevindingen, risico's en verbeterpunten documenteren. Dit biedt de organisatie inzicht in de tekortkomingen en geeft concrete aanbevelingen voor het sluiten van de gaps, zodat de organisatie zich volledig kan voorbereiden op certificering.

4. Advies en opvolging

Op basis van de bevindingen begeleiden wij de organisatie bij het implementeren van corrigerende maatregelen. We bieden advies over zowel organisatorische als technische verbeteringen, rekening houdend met de specifieke behoeften en risico's van de organisatie.

5. Herbeoordeling (optioneel)

Na de implementatie van de verbetermaatregelen voeren we een herbeoordeling uit om te verifiëren of alle tekortkomingen zijn verholpen en of de organisatie volledig voldoet aan de eisen van ISO 62443. Dit zorgt ervoor dat de organisatie klaar is voor de externe certificeringsaudit.

Hoofdstuk 5 **Waarom AudITvision?**

Bij het uitvoeren van een interne ISO 62443-audit is vertrouwen cruciaal. U zoekt een partner die inhoudelijk sterk is, duidelijk communiceert en praktische oplossingen biedt. AudITvision onderscheidt zich op vijf fronten:

1. Diepgaande expertise in ISO 62443

Onze auditors zijn gespecialiseerd in industriële cybersecurity en beschikken over diepgaande en actuele kennis van de ISO 62443-standaard. Wij begrijpen niet alleen de technische vereisten, maar hebben ook inzicht in operationele processen, systeemarchitecturen en de impact van regelgeving binnen industriële automatiseringsomgevingen. Onze ervaring strekt zich uit over complexe omgevingen zoals productie-installaties, OT-netwerken, kritieke infrastructuren en geïntegreerde IT/OT-platformen.

2. Heldere, actiegerichte rapportages

Onze auditrapporten zijn geen ondoorgrondelijke technische documenten, maar gestructureerde en bruikbare rapporten. Bevindingen worden overzichtelijk gepresenteerd per relevante ISO 62443-eis (bijvoorbeeld 62443-2-1 voor beleidsmaatregelen of 62443-3-3 voor systeembeveiliging), voorzien van context, impactanalyse, praktijkvoorbeelden en concrete verbeteradviezen. Zo kunnen technische teams, beleidsmakers en operationele verantwoordelijken direct aan de slag met gerichte maatregelen die aantoonbaar bijdragen aan compliance én risicoreductie.

3. Gestructureerde en bewezen aanpak

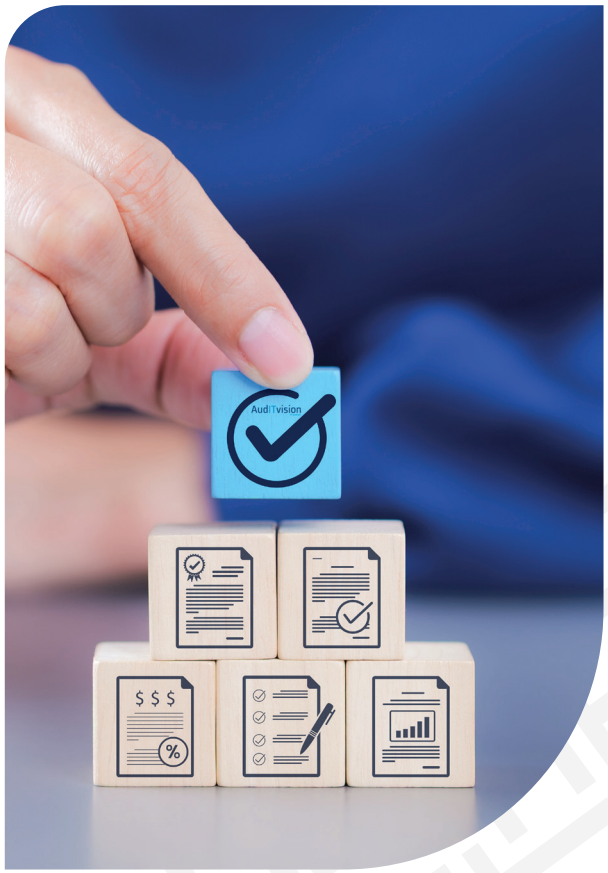
Onze interne audit aanpak is ontwikkeld op basis van honderden audits. Elke stap is transparant en herhaalbaar. U weet waar u aan toe bent qua planning, resultaat en verwachte inzet. Geen onverwachte kosten met een prijsafspraak vooraf.

4. Praktisch én nauwkeurig

We hanteren een grondige methodiek, maar houden het werkbaar. Geen over-auditing of theoretische kaders, maar realistische adviezen afgestemd op uw situatie. We kijken niet alleen naar wat moet, maar ook naar wat wérkt.

5. Onafhankelijk en betrouwbaar

AudITvision is volledig onafhankelijk. Wij ontwikkelen geen systemen, beheren geen OT/IT-infrastructuren en leveren geen technische oplossingen – wij auditen en adviseren. Daardoor zijn onze beoordelingen objectief, onze aanbevelingen eerlijk en onze belangen volledig gericht op uw succes. Organisaties uit overheid, zorg, onderwijs en bedrijfsleven vertrouwen op onze aanpak. AudITvision helpt u van bewustwording naar borging – met een rapport waar u écht verder mee kunt.



Hoofdstuk 6 **Succesvolle certificering ISO 62443 dankzij interne audit AudITvision**

Klantprofiel

Een toonaangevend technologiebedrijf in de Randstad dat industriële automatiseringsoplossingen ontwikkelt en levert aan klanten in kritieke infrastructuren, stond voor de uitdaging om te voldoen aan de eisen van de ISO 62443-norm. De certificering was een vereiste vanuit de klantketen en tevens een strategisch middel om concurrentievoordeel te behalen.

Uitdaging

Hoewel het bedrijf al beschikte over diverse IT-beveiligingsmaatregelen, was de organisatie niet volledig zeker of deze voldeden aan de specifieke eisen van de ISO 62443-serie, in het bijzonder 62443-2-1 (beheerprocessen). Er bestond onzekerheid over de volwassenheid van processen, het risicobeheer en de technische implementatie in OT-omgevingen.

Aanpak: interne audit conform ISO 62443

Onze interne auditdienst werd ingeschakeld om de organisatie voor te bereiden op een externe certificering. De aanpak bestond uit:

Intake en scopedefinitie

Vaststellen van scope en normdelen (o.a. 62443-2-1).

Audit op locatie en documentanalyse

Beoordelen van processen, systemen, risicobeoordelingen en technische implementaties.

Gap-analyse

Opstellen van bevindingen, risico's en verbetervoorstellen, gestructureerd per eis uit de norm.

Advies en opvolging

Begeleiding bij het implementeren van corrigerende maatregelen.

Herbeoordeling

Controle of alle tekortkomingen zijn verholpen.

Resultaat

De interne audit bracht diverse knelpunten aan het licht, waaronder:

- Onvoldoende formele vastlegging van security policies en procedures.
- Onvolledige netwerksegmentatie binnen OT-omgevingen.
- Beperkt patchbeheer voor industriële apparatuur.

Binnen een periode van vier maanden heeft de organisatie, met ondersteuning van onze auditdienst, deze punten opgevolgd en verholpen. Tijdens de daaropvolgende externe certificeringsaudit door een geaccrediteerde instantie zijn geen kritieke afwijkingen geconstateerd. De organisatie behaalde met succes de ISO 62443-certificering.

Voordelen voor de klant

Dankzij onze aanpak realiseren organisaties aantoonbare conformiteit met de ISO 62443-norm, wat leidt tot verhoogd vertrouwen bij opdrachtgevers en ketenpartners. Tegelijkertijd worden interne cybersecurityprocessen en governance versterkt, waardoor de organisatie beter bestand is tegen verstoringen, cyberaanvallen en complianceproblemen. Door grondige voorbereiding verloopt het certificeringstraject bovendien efficiënter en soepeler, met minder verrassingen tijdens de externe audit.

audITvision b.v.

Van der Houven van Oordtlaan 2
7316 AH Apeldoorn

t. 088-2028700

info@auditvision.nl
www.auditvision.nl

AudITvision
IT-auditors

Uw partner
in ISO 62443