Hoe houdt uw organisatie informatie veilig?

VERBETER INFORMATIEBEVEILIGING MET ISO/IEC 27001

SGS

ISO 27001-certificering

Investeer in informatiebeveiliging

Veel organisatie zijn zich onvoldoende bewust van het belang van informatie-beveiliging. Echter zijn de gevolgen groot, als er bijvoorbeeld door een hack of een datalek persoonsgegevens in de verkeerde handen terechtkomen.

Daarnaast is de waarde van data de laatste jaren gestegen. Door de komst van internet, big data en mobile devices is data steeds makkelijker beschikbaar. Als organisatie moet u zichzelf vragen stellen als:

- Hoe zorgen wij ervoor dat we verantwoord en veilig omgaan met informatie?
- Hoe verminderen wij de kans op cyberaanvallen en ransomware?
- Wat kunnen de gevolgen zijn als vertrouwelijke gegevens in de verkeerde handen terechtkomen?

BESCHERM BELANGRIJKE INFORMATIE MET EEN INFORMATIEBEVEILIGING MANAGEMENTSYSTEEM

Organisaties krijgen steeds vaker te maken met cyberaanvallen en ransomware. Daarmee zijn organisaties zich er steeds bewuster van, dat het beveiligen van informatie ook onderdeel is van de bedrijfsvoering. Ook klanten en werknemers willen zeker zijn dat de organisatie waar ze zaken mee doen, veilig omgaat met hun (privé)gegevens.

Informatiebeveiliging is van toepassing op allerlei organisaties en nuttig voor alle organisaties die omgaan met het opslaan en verwerken van vertrouwelijke informatie. Met ISO 27001 kunnen organisaties aan hun stakeholders aantonen dat zij de informatiebeveiliging zeker gesteld hebben in hun bedrijfsvoering. In de ISO 27001-norm wordt beschreven hoe informatiebeveiliging procesmatig ingericht zou kunnen worden. Doordat deze informatiebeveiligingsnorm opgesteld is volgens de High Level Structure (HLS), kan hij goed geïntegreerd worden in uw bestaande managementsysteem.

Een managementsysteem voor informatiebeveiliging (ISMS) ondersteunt uw organisatie met het opstellen van richtlijnen rondom informatiebeveiliging. In het managementsysteem maakt uw organisatie duidelijk hoe informatie verwerkt en beschermd wordt. Met ISO/IEC 27001 certificering toont u de inzet van uw organisatie voor informatiebeveiliging. Het helpt tevens bij het voldoen aan privacywetgeving.

ISO/IEC 27001 CERTIFICERINGSVOORDELEN

- U toont aan dat informatiebeveiliging op alle niveaus binnen uw organisatie belangrijk wordt gevonden.
- U geeft zekerheid naar klanten en werknemers dat u veilig omgaat met hun (privé)gegevens.
- U draagt bij aan het voldoen aan relevante wet- en regelgeving.
- U vermindert risico's en de kans op incidenten op gebied van gegevensbeveiliging.
- U brengt risico's in kaart en implementeert controlemaatregelen om deze risico's te beheren of uit te bannen.
- U beschermt zich met ISO 27001 tegen externe bedreigingen en minimaliseert de eventuele impact.

ISO 27001 CERTIFICERING HELPT BIJ INFORMATIEBEVEILIGING

ISO/IEC 27001 is een managementsysteem voor informatiebeveiliging. Hiermee kunt u informatie binnen uw organisatie beveiligen. Dit gebeurt door het in kaart brengen van risico's. Door middel van het implementeren van controlemaatregelen, neemt de kans op incidenten af. Met ISO/IEC 27001 certificering maakt u aantoonbaar dat uw organisatie op een verantwoordelijke manier omgaat met informatie. Dit geeft interne en externe partijen geruststelling.

Informatiebeveiliging gaat over het beschermen van alle informatie die een belangrijke waarde vertegenwoordigt voor uw organisatie.

VOORKOM PROBLEMEN MET RISICOMANAGEMENT

Elke organisatie wordt geconfronteerd met interne en externe factoren die invloed hebben op de doelstellingen van uw organisatie. Door het in kaart brengen van de risico's, de impact ervan vast te stellen en de risico's te beheersen zorgt uw organisatie dat ze succesvol blijft. Adequate risicomanagementprocedures zijn essentieel om risico's te beoordelen en in de hand te houden, ongeacht de aard van uw organisatie. Risico's doen zich in allerlei vormen voor. Met welke risico's u te maken krijgt hangt af van de aard en de complexiteit van uw organisatie. In alle gevallen is het zaak de specifieke risico's waarmee uw organisatie te maken kan krijgen te identificeren en te kwantificeren. Vervolgens moet u beslissen hoe uw organisatie deze risico's het best beheerst en beperkt.

QUICKSCAN

Om te onderzoeken of er voldoende maatregelen zijn genomen, om de informatie binnen uw organisatie veilig te stellen, kunt u een quickscan uit laten voeren. Met de quickscan kunt u vast stellen of het beschermingsniveau voldoende is. Als er wijzigingen in de systemen plaatsvinden of als er een initiatief van een nieuw project is, kan het goed zijn om een quickscan uit te laten voeren.

RISICOANALYSE

Aanvullend kunt u met een diepgaandere risicoanalyse in kaart te brengen welke maatregelen moeten worden getroffen om het juiste beveiligingsniveau te realiseren. Naast het in kaart brengen van de bedreigingen, wordt in een risicoanalyse bepaald wat de kans van het optreden van de bedreiging is. Daarbij wordt ook berekend wat het gevolg zou zijn als de bedreiging daadwerkelijk optreedt.

Met risicomanagement inventariseert u waar de kansen en risico's in uw organisatie liggen. Hiermee verkleind u de kans op datalekken of hacks.

ZORG VOOR BEDRIJFSCONTINUÏTEIT

De meeste organisaties krijgen vroeg of laat te maken met een incident dat de dagelijkse activiteiten van hun organisatie verstoord of bedreigd. Door het uitvoeren van oefeningen en regelmatige controles, behoudt uw organisatie grip op deze incidenten. Tevens zorgt het ervoor, dat iedereen in de organisatie weet wat verwacht wordt als er een incident plaatsvindt. Een bedrijfscontinuïteitbeheersysteem (BCM) helpt vervolgens om de impact van verstoringen te verkleinen.

ISO 22301-CERTIFICERING

Met het invoeren van een BCM inventariseert en definieert uw organisatie de belangrijkste bedrijfsprocessen. Dit helpt u om de kritieke bedrijfsprocessen en de impact van eventuele verstoring te begrijpen. Het is daarbij belangrijk om te begrijpen hoe u de veerkracht van uw organisatie kunt verbeteren. Met herstelprocessen kunt u het voortbestaan van uw organisatie waarborgen. Maak de inzet van uw organisatie aantoonbaar met ISO 22301-certificering.

INVENSTEER IN CONTINUE ONTWIKKELING MET TRAININGEN

In België en Nederland bieden wij diverse trainingen aan die uw organisatie helpt bij het voldoen aan de continue veranderingen van technische normen en wet- en regelgeving. Zo ook op gebied van informatiebeveiliging, risicomanagement en bedrijfscontinuïteit. Zo bieden wij de onder andere:

- klassikale training ISO 27001 informatiebeveiliging;
- e-learning inleiding tot risicobeheer en risicogebaseerd denken;
- klassikale training risicomanagement;
- klassikale training ISO 22301 bedrijfscontinuïteit.

Wilt u meer te weten komen over de trainingsmogelijkheden? Neem dan contact met ons op, wij bespreken het graag met u.

CONTACTINFORMATIE

www.sgs.be
www.sgs.nl

t +32 (0)3 545 48 48
t +31 (0)88 214 37 88

be.ssc.sales@sgs.com
nl.certificatie@sgs.com

www.sgs.com/linkedin

WHEN YOU NEED TO BE SURE