Steeds meer opdrachtgevers, aannemers, installateurs, toeleveranciers en vastgoedbeheerders die gebruik maken van Ibis applicaties en locatie en tijd onafhankelijk werken en geen omkijken meer willen hebben naar het installeren en beheren van software, gebruiken Ibis software applicaties via het internet. Door het toenemend gebruik van 'Software-as-a-Service' (Saas), verschuiven echter ook de verantwoordelijkheden voor de beschikbaarheid, vertrouwelijkheid en integriteit van de programmatuur en bijbehorende data. Ibis beseft het bedrijfskritische belang van deze verantwoordelijkheden en heeft daarom het afgelopen jaar de internationaal erkende ISO 27001-certificering voor het beveiligen van bedrijfsinformatie behaald. De ISO 27001 is een standaard die gaat over informatiebeveiliging. In deze standaard staat hoe je procesmatig met het beveiligen van informatie kan omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen een organisatie zeker te stellen.

Er zijn wel regels voor het bepalen wat er wordt geaudit

Als organisatie mag je bepaalde delen van je dienstverlening uitsluiten en ook bepaalde delen van je organisatie. Er zijn echter wel regels voor wat je wel en niet mag uitsluiten. De auditor controleert dat en samen met de organisatie wordt de scope bepaald. De scope is een tekstuele omschrijving van de diensten / producten die geleverd worden. Deze scope staat op het certificaat.

Wat is de scope van Software?

Het ontwikkelen, beheren en leveren van online applicaties en het aanbieden van support en consultancy diensten, zoals vastgesteld door de directie, en in overeenstemming met de Verklaring van toepasselijkheid.

Wat houdt de Verklaring van Toepasselijkheid in?

De ISO 27001 bestaat uit 2 delen. Een algemeen deel, in de norm terug te vinden in de hoofdstukken 4 tot en met 10. En een specifiek deel, in de norm terug te vinden in de Annex. In deze Annex staan de beheersmaatregelen met betrekking tot informatiebeveiliging, zoals bijvoorbeeld uitgifte van rechten, netwerkscheiding en de fysieke beveiliging. Van dit specifieke deel zijn beheersmaatregelen op 'niet van toepassing' te zetten. Dat betekent dan dat je dat deel van de norm niet hebt geïmplementeerd in jouw organisatie. De Verklaring van Toepasselijkheid is hier te downloaden.

Hoe meer je uitsluit hoe minder het certificaat waard is

Immers je hebt niks gedaan met dat deel van de norm dat je hebt uitgesloten. Hoe meer je uitsluit hoe minder je certificaat waard is. Nou kan het natuurlijk dat het logisch is om een deel uit te sluiten. Als je bijvoorbeeld software inkoopt en dus niet zelf ontwikkeld kan je, het deel dat gaat over ontwikkelen van software, uitsluiten. Jouw klanten zullen dat ook logisch vinden. Echter als je veel uitsluit zeg je daarmee dat je geen aandacht hebt voor dat deel uit de norm. Je hebt het immers niet geïmplementeerd in jouw organisatie. Het maakt dus geen deel uit van jouw managementsysteem voor informatiebeveiliging (het ISMS).

Wat heeft Aceve Nederland uitgesloten in de Verklaring van Toepasselijkheid?

Aceve Nederland heeft slechts één beheersmaatregel uitgesloten in de Verklaring van Toepasselijkheid. Dit is de beheersmaatregel: A14.2.7 Uitbestede softwareontwikkeling. De reden hiervoor is dat alle softwareontwikkeling intern plaatsvindt.

Wat is een ISMS

ISMS staat voor Information Security Management System en is de vastlegging van de complete set van maatregelen, processen en procedures. Deze complete set is dus de manier / methode hoe een organisatie met informatiebeveiliging omgaat. Deze methode moet ook rekening houden hoe de organisatie van zichzelf leert zodat ze zich continu kunnen verbeteren.

Voor wie is ISO 27001 bedoeld?

Voor alle organisatie die willen aantonen dat zij een set van maatregelen, processen en procedures hanteren om aan stakeholders te laten zien dat zij serieus met informatiebeveiliging omgaan. Dit kunnen ICT bedrijven (zoals Aceve Nederland) zijn, maar ook banken, verzekeraars, overheid, zorginstellingen en andere bedrijven die met vertrouwelijke informatie omgaan, bewerken of opslaan.

Waaruit bestaat de ISO 27000 familie?

De ISO 27001 norm staat niet op zichzelf, maar is onderdeel van de ISO 27000 familie. Hierin zijn bijvoorbeeld ook implementatie richtlijnen opgenomen (zie ISO 27002) en wordt er uitleg gegeven over hoe de ISO 27001 geaudit kan worden (zie ISO 27007 en ISO 27008).

Wat is een norm of standaard?

Een norm of standaard is een document met erkende afspraken, specificaties of criteria over een product, een dienst of een methode. Standaarden kunnen vastgelegd worden binnen een bedrijf of organisatie, binnen een consortium van organisaties of door erkende standaardisatieorganisaties. Erkende standaardisatieorganisaties (zowel nationale als internationale) werken volgens een bepaald proces en controleerbare regels.

Wat is informatiebeveiliging?

Dit is het geheel van preventieve, detective, repressieve en correctieve maatregelen alsmede procedures en processen die de vertrouwelijkheid, beschikbaarheid en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.

Wat is ISO 27001?

ISO 27001 is een standaard die gaat over informatiebeveiliging. In deze standaard staat hoe je procesmatig met het beveiligen van informatie kan omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen een organisatie zeker te stellen. Een organisatie die voldoet aan de ISO 27001 eisen kan zich door een certificerende instantie laten auditen. Bij voldoende niveau krijgt een organisatie dan een certificaat. De certificerende instantie doet dit volgens richtlijnen zodat er zeker gesteld wordt dat iedereen die zo'n certificaat krijgt ook aan bepaalde voorwaarden voldoet. Het belangrijkste is om een certificaat te krijgen met een stempel van de RvA erop. Dit is de Raad van Accreditatie, zij controleren de certificerende instantie op kwaliteit. Dit heet een "geaccrediteerde certificering" en geeft meerwaarde aan een ISO certificaat.

Waarom wilt Aceve Nederland Software ISO 27001 gecertificeerd zijn?

Dit is nodig om ons bedrijf doorlopend veilig te houden. Dit zijn zowel organisatorische als technische stappen. Hierbij nemen we het volgende standpunt in; we nemen maatregelen: Die nodig zijn om de beveiliging van klantdata, bedrijfsgegevens, personeelsgegevens, bedrijfsmiddelen en collega's te garanderen. Om te voldoen aan wet- en regelgeving. Om de continuïteit van de bedrijfsvoering te garanderen. Om onze reputatie, en die van onze klanten te beschermen. Waarvan de baten opwegen tegen de kosten.