Klik hier als u de onderstaande nieuwsbrief niet goed kunt lezen.

CompLions

2012-nr.03

NieuwsBrief

Inhoudsopgave

Geachte lezer,

Welkom bij deze derde nieuwsbrief van CompLions in 2012.

De afgelopen maanden zijn turbulent op economisch gebied, maar ook op het vlak van informatiebeveiliging is er het nodige voorgevallen. Steeds meer incidenten zorgen ervoor dat informatiebeveiliging op de agenda blijft staan. Zoals het lekken van vertrouwelijke dossiers, geslaagde hackpogingen met een criminele achtergrond, incidenten met de zogenaamde Bring Your Own Devices (BYOD) met bijvoorbeeld smartphones en virussen die processen platleggen bij gemeenten. De media hebben de nieuwswaarde van deze incidenten ook ontdekt en zijn zelf actief in het bloot leggen van lekken. Steeds vaker moeten organisaties aan de pers uitleggen hoe dit heeft kunnen gebeuren.

Al met al is de reputatieschade die optreedt bij dergelijke incidenten enorm toegenomen. In deze nieuwsbrief gaan we in op de oorzaken, de verantwoordelijkheden en de reikwijdte van het ISO 27001 certificaat. Daarnaast willen wij met onze nieuwe Outsourcingsdienst inspelen op de groeiende behoefte aan het beheersen van de kosten. Met onze outsourcingsdienst besteedt u het gehele ISMS-proces aan ons uit. Uw organisatie kan zich dan richten op de eigen kerntaken en core business. Ook onze Technische Kwetsbaarheden Analyse-diensten zijn aangepast op de groeiende behoefte deze kwetsbaarheden, en de hiermee gepaard gaande risico's, inzichtelijk te krijgen.

Op verzoek van meerdere klanten is ons cursusprogramma uitgebreid met een Security Management training om de Security staf meer inzicht te geven in algemene aspecten als In Control, de veelheid aan normen en standaarden en hoe efficiënt om te gaan met compliance en audit. Met al deze ontwikkelingen, nieuwe diensten en ons eigen behaalde ISO 27001 certificaat willen wij ons commitment onderstrepen door u nog beter van dienst te zijn en het niveau van onze dienstverlening en uw beveiliging te verhogen en te continueren.

Tevens willen wij u wijzen op de Infosecurity Beurs op 31 oktober en 1 november a.s. in de Jaarbeurs te Utrecht. Wij zijn hier aanwezig met een stand. Meer informatie over de beurs vindt u in deze nieuwsbrief.

Met vriendelijke groet,

CompLions

Directie CompLions B.V.

Nieuwe certificeringen

CompLions is per 1 augustus 2012 gecertificeerd voor ISO 27001:2005.

Verder mogen wij **'DCF, DataCenterFryslân'**, die wij recent hebben ondersteund bij de implementatie, feliciteren met het behalen van een certificaat voor ISO 27001.

Meer informatie over onze klanten en hun certificering is op onze website terug te vinden onder 'CompLions Nieuws'. Lees hier meer.

Klantencase: 'Amphia Ziekenhuis'

Timo Schipperen is werkzaam als Security Officer bij het Amphia Ziekenhuis binnen het onderdeel Kenniskern Informatie- en Medische Technologie (IMT). Als Security Officer is hij verantwoordelijk voor alle aspecten en activiteiten rondom het (continue) proces van informatiebeveiliging. Voor het Amphia Ziekenhuis is hij direct betrokken en verantwoordelijk voor het expliciteren van de risico's binnen het werkveld van informatiebeveiliging. Timo Schipperen richt zich op het beheersen en verbeteren van elementen uit de norm NEN 7510, zodat het ziekenhuis voldoet aan de landelijke eisen vanuit de Inspectie voor de Gezondheidszorg.

Via het netwerk Linkedin en bezoekjes aan beurzen is Timo Schipperen in contact gekomen met CompLions. Hierbij waren de uitgangspunten: de interesse en het aansluiten van het wederzijds gedachtenveld.

In navolging van de externe audit Informatiebeveiliging voor Ziekenhuizen in 2010 was het Amphia Ziekenhuis van plan om een zogenaamde Business Impact Analyse (BIA) te laten uitvoeren. Deze BIA had als doel meer inzicht te geven in de betrouwbaarheidseisen die de proceseigenaren van (kritische) zorgprocessen stelden aan de ICT-middelen. Classificatie van gegevens en systemen hoort daar een onderdeel van te zijn. Dit alles om aan de juiste beschikbaarheidseis van de zorgprofessional te kunnen voldoen. De uitkomst van de BIA zal vervolgens gebruikt worden om de juiste (ICT-) maatregelen in te voeren en daarmee ook de bedrijfscontinuïteit te onderbouwen of zelfs te verbeteren. Eén van de eisen was dat het eindresultaat van de opdracht voor het Amphia Ziekenhuis een actief onderdeel blijft binnen de organisatie. Dus niet een Excel bestand dat je per proces in de organisatie uit zet en dat vervolgens bewaakt moet worden door de Security Officer. De BIA moest ook aandacht hebben voor de volgende gerelateerde onderdelen van de (kritische) zorgprocessen: Fysieke beveiliging, Informatiebeveiliging, ICT en ondersteuning door Facilities.

Het Amphia Ziekenhuis heeft vervolgens gekozen voor consultancy en de ISMScontrol-tooling van CompLions. Om samen de BIA's uit te voeren en deze te verwerken in de meegeleverde tooling. De inrichting van ISMScontrol is opgepakt door het Amphia Ziekenhuis na het doorlopen van de 2-daagse Expert training

ISMScontrol bij CompLions.
De implementatie in ISMScontrol, in samenwerking met een consultant van CompLions, en de opgedane kennis van de gevolgde Expert training, resulteerde in een implementatie van een paar weken. Daarna volgde het uitvoeren van de BIA's en de risicoanalyses. De verkregen informatie werd verwerkt in ISMScontrol. Daarna volgde de eindpresentatie aan het management en de betrokken procesmanagers.

"Het spiegelen van de werkwijze en de gemaakte keuzes zijn logisch en verklaarbaar. Dat geldt ook voor de werking van ISMScontrol, het toepassen van activiteiten en de te nemen stappen bij de implementatie. CompLions is in mijn ogen een organisatie die openstaat voor eisen en wensen die uit het specifieke werkveld van kwaliteitsverbetering voortkomen. En informatiebeveiliging is toch ook wel te bestempelen als een kwaliteitsproces. De zaken die in het gebruik en in dagelijkse voorbeelden naar boven komen zijn bespreekbaar en indien niet direct oplosbaar, worden ze meegenomen en zie je oplossingen terug in een nieuwe release van het product. Ook het meedenken over het beter gebruiken en verder verspreiden van ISMScontrol is een aandachtspunt waarbij men binnen CompLions graag meedenkt en mee helpt. Daarmee helpt CompLions mee aan het goed wegzetten van informatiebeveiliging en het inzicht in het proces informatiebeveiliging binnen instellingen. Het mooiste voorbeeld was voor mij de vraag van het merendeel van de procesmanagers: "Wanneer krijgen wij deze tool, want dan kunnen we daarmee ook op de risico's gaan sturen?" Nou een groter compliment kun je niet krijgen" aldus Timo Schipperen.

Infosecurity beurs 2012

CompLions op Infosecurity beurs 2012

Op 31 oktober en 1 november a.s. staat CompLions op de Infosecurity beurs in de Jaarbeurs in Utrecht. Het thema van dit jaar is Social IT.

Zonder goed beleid en regels kan het gebruik van sociale netwerken zoals Facebook, Hyves en Linkedin tot ongewenste risico's leiden. Smartphone fabrikanten voorzien steeds meer in sociale netwerkintegraties op toestellen, waardoor de grens tussen werk en privé erg dun is geworden.
CompLions helpt u bij het opstellen van richtlijnen, het verkrijgen van inzicht en bij de bewustwording van de risico's die u loopt met het toepassen van sociale netwerken. Voor deze toepassing brengen wij voor u in beeld welke maatregelen u hiervoor additioneel kunt treffen en tegen welke voorwaarden.

Feit blijft dat we een groeiende berichtgeving zien over organisaties die getroffen worden door hacker- en virusaanvallen. Het gebruik van sociale netwerken en eigen devices waarmee een netwerkverbinding is opgezet is in een aantal gevallen de oorzaak geweest.

Wilt u ons bezoeken op de Infosecurity beurs? Dan kunt u zich via onze site www.complions.nl aanmelden voor gratis toegang. U kunt ons vinden in Hal 1, ons standnummer is 01A092.

Trends

Privacy- en informatiebeveiliging, IT risicomanagement en compliance zijn voor veel organisaties belangrijke thema's. Sommige organisaties besteden hier aandacht aan door de processen Security- en Risicomanagement in te richten. Taken en verantwoordelijkheden worden dan vaak toegewezen aan een Information Security Officer of Risk Manager. Andere organisaties hebben deze processen niet ingericht, omdat zij niet beschikken over voldoende of gekwalificeerd personeel of over niet voldoende middelen om deze processen goed te borgen. Hierdoor ontstaat er een groeiende behoefte om deze processen te outsourcen en door een expert te laten uitvoeren.

Daarom is er tijdens de Infosecurity beurs 2012 speciale aandacht voor onze outsourcingsdienst en abonnementen: **Security Officer as a Service (SOS)**, **Security Manager as a Service (SMS)** en **IT Auditing as a Service (IAS).**
Met onze nieuwe outsourcingsdienst **Information Security & Risicomanagement Outsourcing (ISRO)** kunt u uw gehele informatiebeveiliging, IT risicomanagement en -compliance processen inclusief **ISMScontrol**-tooling aan ons uitbesteden op basis van een ISMS zoals is voorgeschreven in de ISO 27001 en NEN 7510 norm. Ook op de beurs vertellen wij u hier graag meer over.

U kunt hier alvast informatie aanvragen over onze nieuwe outsourcingsdienst **ISRO**. U kunt ons ook bezoeken op de Infosecurity beurs. Via onze site www.complions.nl kunt u gratis toegang aanvragen.

ISO 27001 schept verplichtingen

Van onbewust risico lopen naar bewust risico nemen
In de afgelopen maanden hebben in Nederland diverse incidenten plaatsgevonden waarbij vertrouwelijke dossiers van organisaties openbaar zijn geworden door hackers of als gevolg van menselijke fouten.
Een aantal van deze organisaties is ISO 27001 gecertificeerd. Tot nu toe betrof het geen van onze klanten, maar die mogelijkheid is wel aanwezig.

Belangrijk is dat ISO 27001 geen garantie biedt over de mate van implementatie van bepaalde beveiligingsmaatregelen. Het zegt iets over het proces, waarbij je op basis van een risicoafweging tot een maatregelenselectie komt. Dit proces moet continu getoetst en indien nodig verbeterd worden. Daarbij kan het voorkomen dat een onderkent risico genomen wordt omdat dit nu eenmaal de keuze van de organisatie zelf is of dat er onvoldoende middelen voorhanden zijn om de maatregel te kunnen implementeren.

In dit laatste aspect zit vaak het probleem. Men gaat er veelal vanuit dat er impliciet een bepaald beveiligingsniveau geboden wordt door een organisatie met een ISO 27001 certificaat, ondanks dat dit geen onderdeel is van een contract of

SLA.

Het is dus lastig uit te leggen voor een datacenter met een ISO 27001 certificaat dat er down time is opgetreden, ook al valt deze ruim binnen de marge van de SLA. Dit kan één keer gebeuren, maar indien dit vaker gebeurt, zegt dit toch vaak iets over het risicomanagementproces en de effectiviteit van maatregelen.

Risicoanalyses en audits zijn over het algemeen een momentopname. Zodra een organisatie of een (informatie)systeem door bijvoorbeeld een update verandert, kan er door deze verandering een nieuw risico ontstaan en kan een eerdere effectieve maatregel niet meer toereikend zijn. Het is dus zaak deze risicobeoordelingen en afwegingen frequent uit te voeren vooral als er zich veranderingen voordoen zowel intern als bij een ketenpartner.

Goede wijzigingsprocedures met impactanalyses en triggers voor het eventueel uitvoeren van risicoanalyses, zijn essentieel voor het risicomanagementproces. Organisaties met een ISO 27001 certificaat worden geacht dit op orde hebben. Zonder goede wijzigingsprocedures is feitelijk nooit hard te maken of de maatregelen in overeenstemming zijn met de risicoafwegingen en daarmee nog effectief zijn. ISO 27001 schept dus verplichtingen. Klanten gaan ervan uit dat deze procedures effectief zijn en men verwacht impliciet een bepaald beveiligingsniveau, een niveau dat zelfs contract/SLA overstijgend is.

Velen van u zullen zich op dit moment drukker maken om een controle audit, maar wanneer u zich bij het risicomanagementproces ook richt op de wijzigingen, is de kans erg groot dat het wel goed komt met de controle audit en u uw certificaat behoudt en het beveiligingsniveau verhoogt.

Ing. Marcel Lavalette CISA EMITA
Directeur
Lead auditor ISO 27001

ISMScontrol nieuws

Wij verwelkomen de volgende klanten als nieuwe gebruikers van onze tooling ISMScontrol:

- **Denit hosting solutions,** datacenter/hosting
- **IT Creation,** IT automatiseerder
- **LCL Belgium nv,** datacenter
- **RoutIT,** Application Infrastructure Service Provider
- **St. Antonius Ziekenhuis,** locaties Utrecht en Nieuwegein

Voor meer informatie over deze onderwerpen, kunt u onze website bezoeken of contact met ons opnemen.

Vacatures

Wij hebben momenteel onderstaande vacatures openstaan.

- **Junior Consultant Informatiebeveiliging**

Meer informatie over deze vacature vindt u hier.

Trainingen

Klassikale trainingen

Wij verzorgen ook maatwerk en Incompany trainingen. Voor meer informatie over trainingen op maat kunt u hier informatie aanvragen.

1-daagse Security Management training

Deze training is bedoeld voor iedereen die verantwoordelijk is voor het opzetten of beheren van een ISMS (ISO 27001/NEN 7510) of meer inzicht wil krijgen in: informatiebeveiliging, IT governance, risicomanagement en compliance. De cursus is voor Security Officers/Managers, Kwaliteitsmanagers, Informatiebeveiligings- en/of kwaliteitsmedewerkers.

Kosten
€ 595,- per persoon (excl. BTW).

ISMScontrol Expert training voor Security Officers en/of Kwaliteitsmanagers (2 dagen)

Deze training is bedoeld voor iedereen die verantwoordelijk is voor, of betrokken wordt bij, de invoering, beheer en het verbeteren van een systeem voor informatiebeveiliging en risicomanagement met behulp van ISMScontrol.

Kosten
€ 895,- per persoon (excl. BTW).

ISMScontrol trainingen voor Proceseigenaren (1 dag)

Deze training is bedoeld voor iedereen die betrokken is bij de uitvoering van taken met behulp van ISMScontrol in de functie van Proceseigenaar.

Kosten
€ 495,- per persoon (excl. BTW).

ISMScontrol trainingen voor Audit Managers (1 dag)

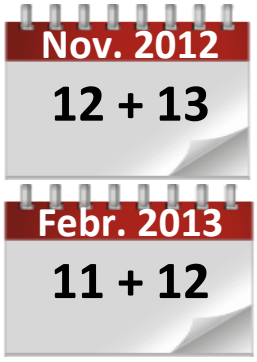
Deze training is bedoeld voor iedereen die betrokken is bij de uitvoering van taken met behulp van ISMScontrol in de rol/functie van Audit Manager.

Kosten
€ 495,- per persoon (excl. BTW).

Agenda

1-daagse Security Management training

Wilt u zich inschrijven, dan kunt u zich hier opgeven.



ISMScontrol Expert training voor Security Officers en/of Kwaliteitsmanagers (2 dagen)

Wilt u zich inschrijven, dan kunt u zich hier opgeven.

ISMScontrol trainingen voor Proceseigenaren (1 dag)

Wilt u zich inschrijven, dan kunt u zich hier opgeven.

ISMScontrol trainingen voor Audit Managers (1 dag)

Wilt u zich inschrijven, dan kunt u zich hier opgeven.

Kijk voor meer informatie op onze website www.CompLions.nl.
Aan-/afmelden nieuwsbrief of vragen/opmerkingen?
Neem contact op met CompLions via 0570 – 63 47 17 of via info@CompLions.nl

CompLions B.V.
Keulenstraat 8E, 7418 ET Deventer
Postbus 2147, 7420 AC Deventer

T 0570 - 63 47 17
F 0570 – 63 41 58
W www.CompLions.nl
E info@CompLions.nl

ING 67.82.53.137
KvK Oost Nederland 08183263