

Opleiding tot CCCO[®]

Cybersecurity Compliance Officer

*Praktijkgerichte expertise in
Cybersecurity Compliance/
September 2024*



ICTRECHT

ACADEMY



We zijn als maatschappij en economie afhankelijk geworden van informatie en IT. Het is daarom belangrijk om informatie te beschermen. Niet alleen tegen hackers of kwaadwillenden, maar ook tegen menselijke fouten, technische storingen en andere soorten dreigingen. Vanuit Europa en Nederland komt steeds meer wet- en regelgeving waaraan bedrijven moeten voldoen. Een Cybersecurity Compliance Officer moet in staat zijn om deze uitdagingen aan te pakken. De praktijkopleiding tot Cybersecurity Compliance Officer biedt de noodzakelijke kennis en vaardigheden op het snijvlak van cybersecurity, wetgeving en compliance, met een focus op de praktische toepassingen.

Deze opleiding onderscheidt zich door een solide theoretisch fundament gecombineerd met een praktijkgerichte benadering waarmee je impact kan maken binnen jouw organisatie. Je leert de verschillende wetgevingen op het gebied van cyberbeveiliging, zoals de NIS2, DORA, CER en AI Act, en hoe je deze kan vertalen naar de praktijk zodat jouw organisatie compliant kan worden met deze regels. De opleiding behandelt cruciale onderwerpen zoals wet- en regelgevingen, risicomanagement, toeleveringsketen, incident- en business continuity management.

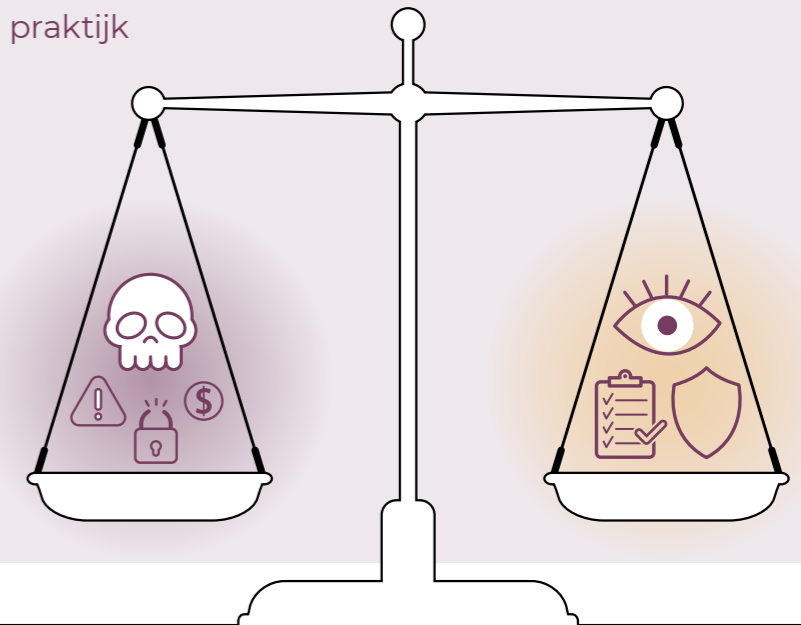
De opleiding in het kort

- Drie praktijkdagen, 11 september, 18 september en 25 september 10:00-16:00 uur
- Daarnaast online oefeningen en kennisoverdracht
- Ontvang het certificaat met recht tot voeren van titel "CCCO®"
- Prijs €2.950,- (ex btw)
- Unieke praktijkgerichte lesstof
- Alle trainingen gegeven door ervaren docenten
- Kwaliteit gewaarborgd door externe opleidingscommissie

Voor wie is de opleiding toegankelijk?

Professionals die regelmatig met cybersecurity vraagstukken te maken krijgen, zoals bestuurders, (bedrijfs-) juristen, CISO's/ISO's/SO's, risk/compliance officers, functionarissen gegevensbescherming, privacy officers, IT-managers, IT-beheerders, en notarissen. Specifieke voorkennis of vooropleiding is niet noodzakelijk.

Compliance en governance in de praktijk



Waarom Cybersecurity Compliance Officer worden?

In onze digitale samenleving speelt cybersecurity een cruciale rol. Het vermogen om gevoelige gegevens te beschermen en cyberdreigingen te voorkomen, is van onschatbare waarde. Zonder adequate beheersmaatregelen kunnen organisaties te maken krijgen met ernstige gevolgen zoals datalekken, financiële verliezen en reputatieschade. Als Cybersecurity Compliance Officer beschik je over de expertise om deze uitdagingen aan te

pakken. De titel CCCO® bewijst je kwaliteiten op dit gebied.

Na deze opleiding:

- Heb je een diepgaand begrip van de juridische en compliancy uitdagingen op het gebied van cybersecurity en informatiebeveiliging.
- Heb je begrip van wet- en regelgevingen omtrent cybersecurity en informatiebeveiliging (zoals de NIS2,

DORA, CER, AI Act en privacywetgeving) evenals hun onderlinge samenhang en hoe normen en standaarden (zoals ISO 27001) zich ertoe verhouden.

- Weet je hoe je in de praktijk compliancy met wet- en regelgeving omtrent cybersecurity en informatiebeveiliging kunt waarborgen.



Waarom kiezen voor de ICTRecht Academy?



Permanente Educatie

Voor behoud van jouw titel na twee jaar ben je verplicht permanente educatie te volgen. Dit kan onder meer door volgen van relevante trainingen bij ICTRecht of derden. ICTRecht zal jaarlijks een update-training aanbieden.



De praktijk voorop

Bij ons staat de praktijk voorop en wij maken leren leuk! Na de theorie doorgenomen te hebben, ga je o.a. aan de slag met interactieve praktijkoefeningen met de focus op het verhogen van je skills.



Opleiders uit het vak

Ons trainingsprogramma is opgesteld door specialisten uit het werkveld. Zij zullen ook de trainingen verzorgen. Alle docenten zijn ervaren cybersecurity specialisten. Zij weten als geen ander welke kennis en skills de functie vereist.



Blended leren: maximale flexibiliteit

Naast de praktijkmiddagen krijg je stof aangeboden via webinars en e-learnings. Die kun je in je eigen tijd doorlopen, precies wanneer het jou uitkomt. Je kunt ze ook gebruiken als naslagwerk om na de praktijkmiddagen nog eens door te nemen.



Volop aandacht voor vaardigheden

Wij geven je tijdens de opleiding de kernkwaliteiten die de functie vereist. Denk aan het identificeren, analyseren en oplossen van cybersecurity gerelateerde vraagstukken. Word zo een Cybersecurity Compliance Officer die opgewassen is tegen allerlei situaties die voorbij kunnen komen in de praktijk.





10% korting bij adviesbureau ICTRecht


Als deelnemer ontvang je na deelname aan een volledige opleiding 10% korting op de kosten in de eerstvolgende offerte bij adviesbureau ICTRecht, tot een maximale kortingswaarde van € 500,-. Deze korting is gedurende één jaar na de uitgiftedatum in te zetten voor advies via een knipkaart, abonnement of los adviesproduct, over alle specialismen waar ICTRecht op actief is.

Inhoud van de opleiding

De invulling van de opleiding is uniek en gericht op de professional die zowel in eigen tijd als op locatie, online en ter plaatse, aan de slag wil. Wij gebruiken hierbij drie leervormen:

 **Webinars** zijn inleidende videopresentaties met interactieve elementen die je in eigen tijd bekijkt. Een webinar duurt ongeveer 15 tot 20 minuten.

 **E-learning:** Met online theorie, oefeningen, puzzels en uitdagende simulaties verdiep je jouw kennis en vaardigheden. Deze voer je uit in eigen tijd na het volgen van de webinars.

 Op de **praktikdagen** ga je op locatie (Utrecht) aan de slag met jouwmede-deelnemers en docenten met veel praktijkervaring. Je oefent met praktijkcases en verdiepende stellingen. Iedere dag begint om 10:00 uur en eindigt om 16:00 uur, met pauzes en een geheel verzorgde lunch.

Bij de praktikdagen wordt aangenomen dat je de webinars en e-learnings hebt afgerond.

Je mag de eindtoets afleggen als je een of meer praktikdagen hebt gemist, maar de kans op een voldoende ligt natuurlijk substantieel hoger als je wel aanwezig bent.



Juridische Context


1. Digitale Decennium: Europa's en Nederland's strategie in het Cybersecurity tijdperk;
2. Basisbeginselen van informatiebeveiliging
3. Overzicht wet- en regelgeving
 - a. NIS2 en Cyberbeveiligingswet
 - b. CER en Wet Kritieke Entiteiten
 - c. DORA
 - d. AI Act
 - e. Privacywetgeving
4. Normen, standaarden en assurance


Compliance deel I


1. Risicobeheersing – wet en proces
2. Risicobeheersing – Risicoanalyse
3. Toeleveringsketen

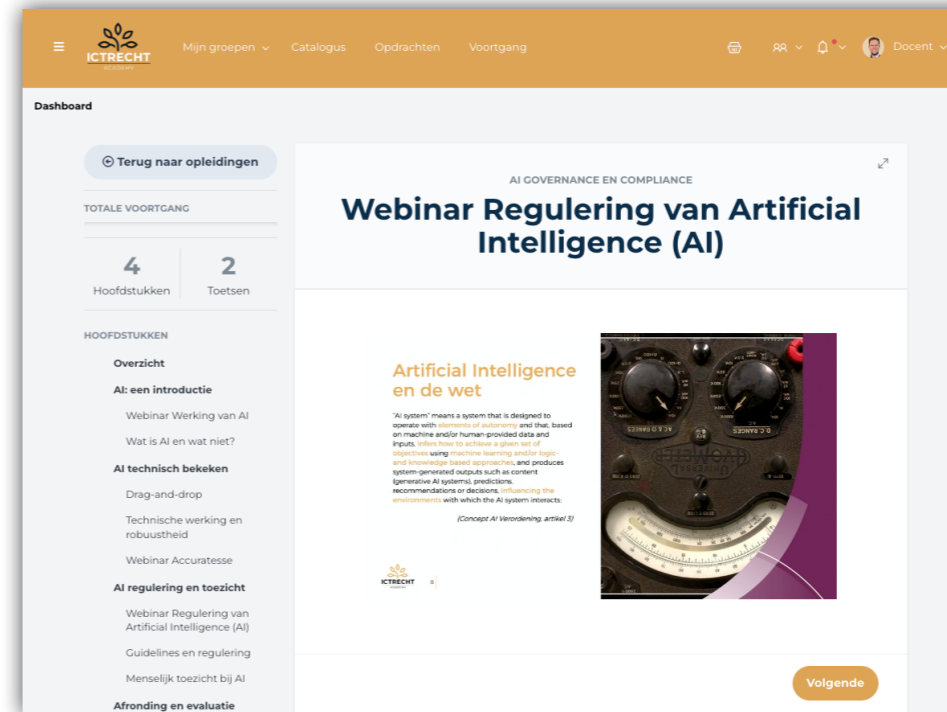
Compliance deel II

1. Incidentmanagement en business continuity – wettelijke verplichtingen
2. Incident management en business continuity - meldplichten
3. Incidentmanagement en incident response plan
4. Businessmanagement en business continuity plan

 ± 1,5 uur

 ± 45 minuten

 ± 1 uur



Dashboard

Terug naar opleidingen

TOTALE VOORTGANG

4 Hoofdstukken | 2 Toetsen

HOOFDSTUKKEN

Overzicht

AI: een introductie

Webinar Werking van AI

Wat is AI en wat niet?

AI technisch bekeken

Drag-and-drop

Technische werking en robuustheid

Webinar Accuratesse

AI regulering en toezicht

Webinar Regulering van Artificial Intelligence (AI)

Guidelines en regulering

Menselijk toezicht bij AI

Afronding en evaluatie

AI GOVERNANCE EN COMPLIANCE

Webinar Regulering van Artificial Intelligence (AI)

Artificial Intelligence en de wet

"AI system" means a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, uses how to achieve a given set of objectives using machine learning and/or logic and knowledge based approaches, and produces system-generated outputs such as content, generative AI systems, predictions, recommendations or decisions, influencing the environments with which the AI system interacts. (Concept AI Verordening artikel 3)

Volgende

Screenshot webinar

E-learnings

Juridische context

1. Oefeningen over de toepassing wet- en regelgeving
2. Werken met begrippen rondom informatiebeveiliging.
3. Case study analyse van verschillende dreigingen waar een organisatie mee te maken kan krijgen.

Compliance deel I


1. Oefeningen over risicoanalyses.
2. Opdrachten omtrent het in kaart brengen van de toeleveringsketen.

Compliance deel II

1. Herkennen van de wettelijke verplichtingen en meldplichten m.b.t. incidentmanagement en business continuity.
2. Oefeningen m.b.t. incidentmanagement en incident response
3. Oefeningen m.b.t. business continuity en incident response

In het interactief boek hieronder gaan we nader in op de basis van regulering van AI zoals in Europa uitgewerkt. Klik op de pijltjes om het boek volledig scherm te openen.

≡ Tekst slepen: tussenoefening 12 / 20 < > ✕

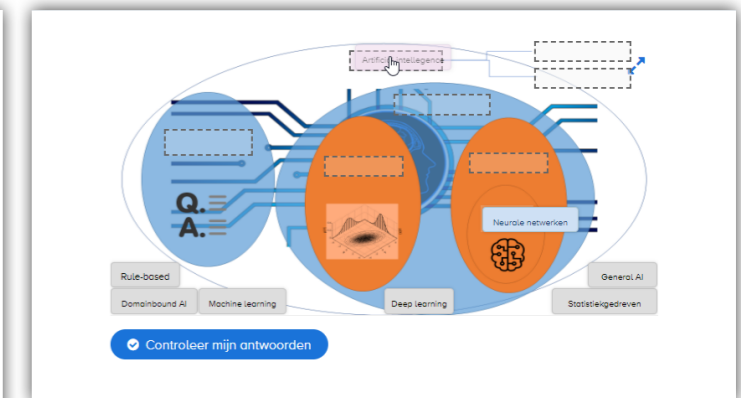


De vele termen duizelen u wellicht. Zet met de volgende oefening een en ander op een rij:

Wanneer een AI vaak onjuiste uitkomsten geeft waardoor gebruikers er het vertrouwen in verliezen, heeft deze een probleem op het gebied van .

Een AI die zonder menselijke tussenkomst leert converseren met ouderen in een verzorgingstehuis, moet met name vanuit perspectief van zorgvuldig opgezet worden.

Een bedrijf dat met een AI significant vaker vrouwen uitsluit van promotie, heeft een probleem met het aspect van AI.



Screenshot E-learning

🕒 1 uur

🕒 1 uur

🕒 1 uur

Screenshot webinar

Praktijkdagen

Dag 1

- Juridische context
- Begrijpen basisbeginselen informatiebeveiliging
- Gebruik van normen en standaarden

 5 uur

Dag 2

- Risicomanagement – risicoanalyses
- Toeleveringsketen in kaart brengen

 5 uur

Dag 3

- Incidentmanagement en businesscontinuity plan maken
- Crisissimulatie

 5 uur

Bij de praktijkdagen wordt aangenomen dat je de webinars en e-learnings hebt afgerond. De online stof wordt dus niet opnieuw behandeld bij de praktijkcases. Je mag de eindtoets afleggen als je een of meer praktijkdagen hebt gemist, maar de kans op een voldoende ligt natuurlijk substantieel hoger als je wel aanwezig bent.



Sfeerimpressie praktijkdag

Docenten

De praktijkdagen worden gegeven door een of meerdere academisch opgeleide juristen met ruime ervaring in het desbetreffende onderwerp. De hoofddocenten staan hieronder getoond. Je kunt ook andere specialisten van adviesbureau ICTRecht en externe trainers treffen als docent van een training.



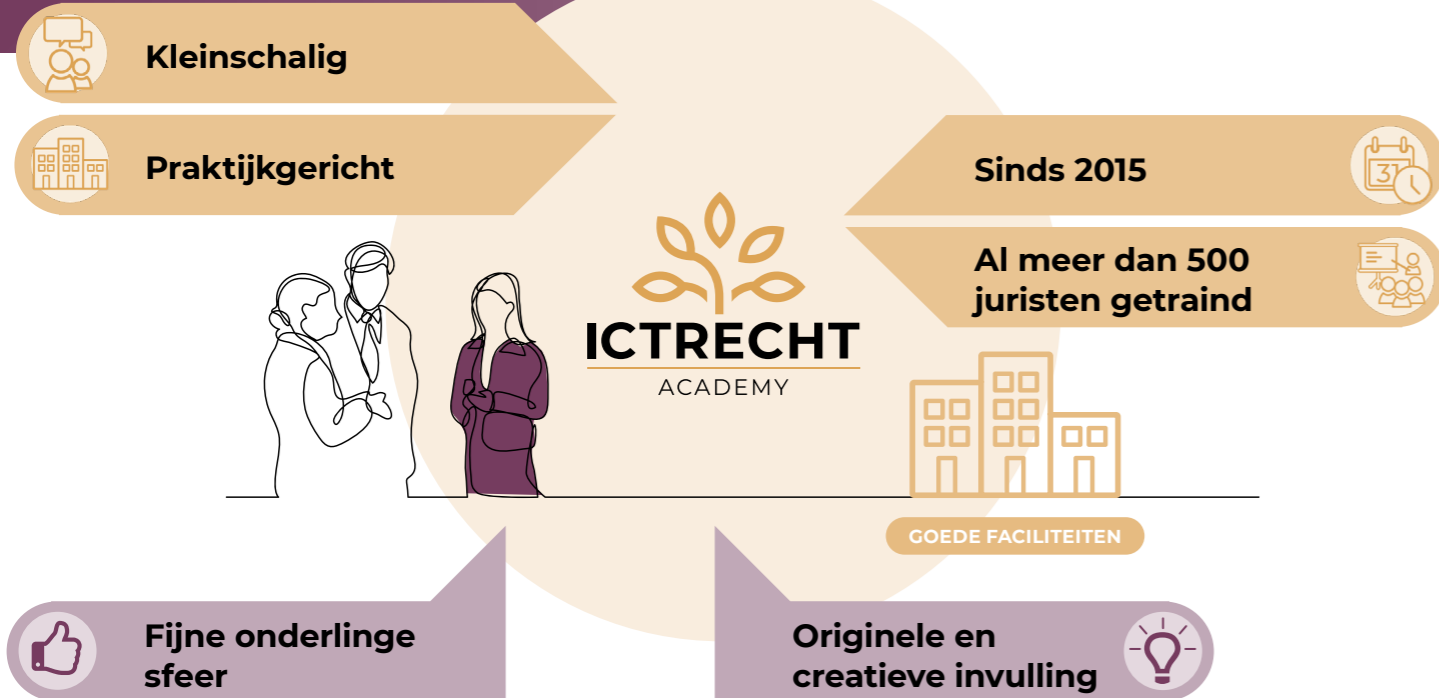
Melanie van Leeuwen
NIS2, Informatiebeveiliging,
Zorg & ICT



Kors Monster
Director ICTRecht Security - CIPP/E



De ICTRecht Academy



Organisatie



ICT-jurist en blogger **Arnoud Engelfriet**, Chief Knowledge Officer en Opleidingsdirecteur bij ICTRecht, is initiatiefnemer van de ICTRecht Academy. Arnoud verzorgt zelf vele trainingen en geeft sturing aan de overige docenten bij het samenstellen van de inhoud van de trainingen.



Onze opleidingscoördinatoren **Mariam El Madani** en **Nikki Hofs** zijn je aanspreekpunt voor praktische zaken.



Twijfel je nog of de opleiding voor jou geschikt is? Dan kijkt Manager **Dimmen Smolders** van ICTRecht Academy graag met je mee.



Mail ICTRecht Academy via academy@ictrecht.nl of bel: 020 663 19 41.

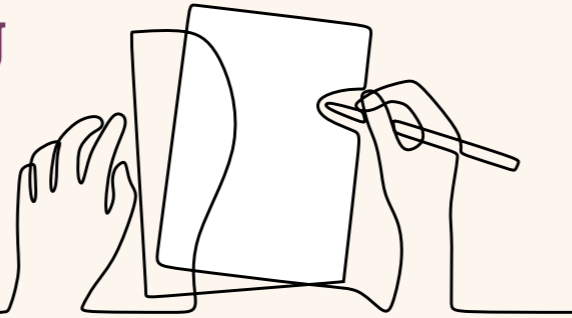


Tijdlijn opleiding

Iedere praktijkdag begint met een inloop van 9:30 tot 10:00 uur, het onderwijs start om 10:00 uur met een lunchpauze van 12:30 tot 13:30 uur en wordt afgesloten om 16:00 uur.







Voorwaarden en invulling



Vorbereiding en studiebelasting

De studiebelasting in uren is als volgt:

| | | |
|--|---------------|---------------------|
|  | Webinars | 3 uur en 15 minuten |
|  | E-learnings | 3 uur* |
|  | Praktijkdagen | 15 uur |
|  | Eindtoets | 2 uur |

*het betreft hier een schatting. Een en ander hangt natuurlijk af van je achtergrond en kennis- en vaardighedenniveau.

Trainingsduur en locatie

De webinars en e-learnings worden online aangeboden en kunnen in eigen tijd worden verwerkt. De praktijkdagen worden op een centrale locatie in Utrecht verzorgd. Inloop is om 9:30 uur, het onderwijs start om 10:00 uur met een lunchpauze van 12:30 tot 13:30 uur en wordt afgesloten om 16:00 uur.

Online leeromgeving

Tijdens de opleiding maken we gebruik van een online leeromgeving waarin alle informatie en documenten die voor de opleiding relevant zijn is terug te vinden. In de online leeromgeving is er ook een plek waar je met mededeelnemers kunt communiceren over de lesstof.

Mocht tijdens de opleiding de online leeromgeving onverhoopt niet bereikbaar zijn, dan kun je altijd contact met ons opnemen via Academy@ictrecht.nl. Telefonisch zijn wij tijdens kantooruren te bereiken via 020-663 1941. Als er belangrijke zaken zijn die niet via de online leeromgeving kunnen worden gecommuniceerd, nemen we zo snel mogelijk contact met jou op.

Studiemateriaal

Online studiemateriaal, met o.a. juridische teksten en relevante artikelen en de casussen met uitwerking (achteraf verstrekt). Toegang tot de studiematerialen blijft, zolang je gecertificeerd blijft.

Eindtoets

De opleiding wordt afgesloten met een digitale eindtoets. Deze wordt 2 weken na de laatste praktijk dag als online meerkeuzetoets aangeboden. De eindtoets is open boek; je mag alle materialen en bronnen gebruiken die je wilt. Alleen overleg of samenwerken met mede-deelnemers is verboden en leidt tot intrekking van het certificaat.

Privacy en persoonsgegevens

Wij stellen de privacy van onze deelnemers voorop en gebruiken de gegevens van deelnemers alleen voor het verzorgen van de trainingen.

Informatie wordt niet aan derden verstrekt, tenzij dat nodig is voor de opleiding of wettelijk verplicht is.

Het volledige privacyreglement krijg je van ons bij je inschrijving. Neemt graag contact met ons op als je nog vragen hebt.

Kosten en voorwaarden

De kosten voor de opleiding bedragen € 2.950,- excl. btw inclusief het boek. We vragen je de kosten in één keer te voldoen.

Indien meerdere personen van hetzelfde kantoor of dezelfde organisatie deelnemen, geldt een kortingstarief van 10% voor iedere deelnemer. Deze korting is niet stapelbaar.

Alle data staan vast. Alleen in uitzonderlijke gevallen worden individuele trainingen verplaatst. Je kunt je inschrijving kosteloos annuleren tot vier weken voor de eerste praktijkdag.

Overige voorwaarden vind je in de [algemene voorwaarden ICTRecht Academy](#).

Certificering en permanente educatie

Omdat cybersecurity en de regels daar omheen zo snel veranderen, kent de opleiding een aspect van permanente educatie. Je certificering is twee jaar geldig vanaf de dag van uitreiking van het certificaat. Je mag dan ook de titel CCCO® voeren.

Vanaf het tweede jaar ben je vanuit de stichting CCLTE verplicht je vakkennis op peil te houden door middel van na- en bijscholing van je vakkennis op het gebied van Cybersecurity wet- en regelgeving. Dit betekent dat je bijvoorbeeld trainingen op dit gebied volgt of congressen bijwoont. Ook het publiceren van artikelen of het zelf geven van trainingen over Cybersecurity valt hieronder.

De stichting CCLTE kan nadere regels stellen aan de permanente educatie. Hierover word je tijdig geïnformeerd. Hierbij geldt dat nieuwe regels voor bestaande certificeringen geen onevenredige impact hebben.

Er zitten geen administratiekosten aan het in stand houden van je certificering.





Schrijf je
hier in
voor deze
opleiding

Meer weten over de
opleiding of vragen?

Neem dan contact op met ons
via e-mail academy@ictrecht.nl
of telefoonnummer: **020 663 19 41**.

Volg ons op:

 @ICTRechtAcademy

 ICTRecht Academy

