

# Opleiding tot Cybersecurity Compliance Officer (CCCO®)

Praktijkgerichte expertise in  
Cybersecurity Compliance

## De opleiding in het kort

- Drie praktijkdagen van 10:00-16:00 uur
- Daarnaast online oefeningen en kennisoverdracht
- Ontvang het certificaat met recht tot voeren van titel “CCCCO®”
- Unieke praktijkgerichte lesstof
- Kwaliteit gewaarborgd door externe opleidingscommissie
- Alle trainingen gegeven door ervaren docenten

## 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

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.

Prijs  
€3.075,-

Exclusief btw

## 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

01

Heb je een diepgaand begrip van de juridische en compliance uitdagingen op het gebied van cybersecurity en informatiebeveiliging.

02

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.

03

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

04

## Waarom kiezen voor de ICTRecht Academy?



### 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 situaties in de praktijk.

05



### 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.



### Permanente educatie

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



## Webinars

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



## E-learning

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.



## Praktijkdagen

Op de praktijkdagen ga je op locatie (Utrecht) aan de slag met jouw mededeelnemers 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.

## Inhoud van de opleiding

06

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 de drie leervormen die links opgesomd worden.

Bij de praktijkdagen wordt aangenomen dat je de webinars en e-learningen hebt afgerond. De online stof wordt dus niet opnieuw behandeld bij de praktijkcases.

Je mag de eindtoets afleggen als je niet meer dan één praktijkdag hebt gemist, maar de kans op een voldoende ligt natuurlijk substantieel hoger als je aanwezig bent bij alle praktijkdagen.

07

# Webinars

## Juridische Context

01

Digitale Decennium: Europa's en Nederland's strategie in het Cybersecurity tijdperk

02

Basisbeginselen van informatiebeveiliging

03

Overzicht wet- en regelgeving  
a. NIS2 en Cyberbeveiligingswet  
b. CER en Wet Kritieke Entiteiten  
c. DORA  
d. AI Act  
e. Privacywetgeving

04

Normen, standaarden en assurance

🕒 ± 1,5 uur

## Compliance deel I

01

Risicobeheersing – wet en proces

02

Risicobeheersing – Risicoanalyse

03

Toeleveringsketen

🕒 ± 45 minuten

## Compliance deel 2

01

Incidentmanagement en business continuity – wettelijke verplichtingen

02

Incident management en business continuity - meldplichten

03

Incidentmanagement en incident response plan

04

Businessmanagement en business continuity plan


🕒 ± 1 uur

Terug naar dashboard
↗

E-LEARNING | CERTIFIED CYBERSECURITY COMPLIANCE OFFICER (CCCO)

## NIS2 & Cyberbeveiligingswet

In dit webinar praten we je bij over de NIS2 Richtlijn. De Richtlijn van de Europese Unie om de cyberweerbaarheid van de lidstaten en organisaties te vergroten. Nederland werkt momenteel aan het omzetten van de richtlijn naar nationale wet. Een conceptversie hiervan is onlangs gepubliceerd, de Cyberbeveiligingswet en alhoewel deze nog niet definitief is weten we wel in grote lijnen wat de wet behandelt.



Interactieve Video

ICTRECHT  
ACADEMY

0:00 / 27:22

ALLEEN LEZEN

TOTALE VOORTGANG

---

**4**

Hoofdstukken

**0**

Toetsen

HOOFDSTUKKEN

**Overzicht**

**Juridische context**

- Het Digitale Decennium
- Het Digitale Decennium: Europa en Nederland in het Cybersecurity tijdperk
- Informatiebeveiliging - de basis
- Juridisch overzicht
  - NIS2 & Cyberbeveiligingswet
  - CER & WWKE
  - DORA
  - AI Act
  - AVG
  - ISMS en informatiebeveiligingsstanda:

# E-learnings

## Juridische Context

01

Oefeningen over de toepassing wet- en regelgeving

02

Werken met begrippen rondom informatiebeveiliging

03

Case study analyse van verschillende dreigingen waar een organisatie mee te maken kan krijgen.

🕒 1 uur

## Compliance deel I

01

Oefeningen over risicoanalyses

02

Opdrachten omtrent het in kaart brengen van de toeleveringsketen

🕒 1 uur

## Compliance deel 2

01

Herkennen van de wettelijke verplichtingen en meldplichten m.b.t. incidentmanagement en business continuity.

02

Oefeningen m.b.t. incidentmanagement en incident response

03

Oefeningen m.b.t. business continuity en incident response

🕒 1 uur

E-LEARNING | CERTIFIED CYBERSECURITY COMPLIANCE OFFICER (CCCO)

# Business Continuity Management - Business Continuity Plan

In het volgende webinar nemen we je mee in wat business continuity management is, het belang van een business continuity plan (BCP) en wat de hoofdcomponenten van een BCP zijn.



Lees ook de informatie van het Digital Trust Center (onderdeel van het Ministerie van Economische Zaken en Klimaat) m.b.t. [het maken van een bedrijfscontinuïteitsplan](#).

# Praktijkdagen

## Dag 01

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

🕒 5 uur

## Dag 03

- Incidentmanagement en businesscontinuity plan maken
- Crisissimulatie

🕒 5 uur

## Dag 02

- Risicomanagement – risicoanalyses
- Toeleveringsketen in kaart brengen

🕒 5 uur

## Eindtoets

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 niet meer dan één praktijkdag hebt gemist, maar de kans op een voldoende ligt natuurlijk substantieel hoger als je aanwezig bent bij alle praktijkdagen.



# Docenten



**Kors  
Monster**

Portfolio Manager

**Expertise**

Compliance



**Melanie  
van Leeuwen**

Compliance Consultant

**Expertise**

Compliance

## Docenten

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

# De ICTRecht Academy

- ✓ Originiele en creatieve invulling
- ✓ Kleinschalig
- ✓ Al meer dan 500 juristen getraind
- ✓ Sinds 2015
- ✓ Fijne onderlinge sfeer
- ✓ Praktijkgericht



**Kors**  
Monster

Portfolio Manager



**Melanie**  
van Leeuwen

Compliance Consultant

De opleiding is vormgegeven door Portfolio Manager Kors Monster en Compliance Consultant Melanie van Leeuwen.



**Mariam**  
El Madani

Opleidingscoördinator



**Nikki**  
Hofs

Opleidingscoördinator

Onze opleidings-coördinatoren Mariam El Madani en Nikki Hofs zijn je aanspreekpunten voor praktische zaken.



**Esmée**  
Baljet-Kuyt

Programma Manager  
Academy

Twijfel je nog of de opleiding voor jou geschikt is? Dan kijkt Programma Manager Academy Esmée Baljet-Kuyt graag met je mee.

## Tijdelijk 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.

**01 Startdata**  
Toegang tot onlinestof

**02 Eerste praktijkdag**

**03 Tweede praktijkdag**

**04 Derde praktijkdag**

**05 Eindtoets**

## Vorbereiding en studiebelasting

<b>Webinars</b>	3 uur 15 min
<b>E-learnings</b>	3 uur*
<b>Praktijkmiddagen</b>	15 uur
<b>Eindtoets</b>	2 uur*

\* Het betreft hier een schatting. Een en ander hangt natuurlijk af van je achtergrond en kennis- en vaardigheidsniveau.

## 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 12.45 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, terug te vinden is. 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](mailto: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 en e-learnings

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 mededeelnemers 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 training of wettelijk verplicht is. Het volledige privacyreglement krijg je van ons bij je inschrijving. Neem graag contact met ons op als je daar nog vragen over hebt.

## Kosten en voorwaarden

De kosten voor de opleiding bedragen €3.075,- excl. btw inclusief tweemaal deelname aan de eindtoets.

We vragen je de kosten in één keer te voldoen.

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](mailto:academy@ictrecht.nl)  
of telefoonnummer: [020-663 19 41](tel:020-6631941).

**Instagram**    [@ICTRecht](https://www.instagram.com/ICTRecht)

**Linkedin**     [@ICTRecht](https://www.linkedin.com/company/ICTRecht)