

FUNCTIEPROFIEL

Chief Information Security Officer (CISO)





Taken, verantwoordelijkheden en competenties

Risico's vaststellen, de juiste maatregelen nemen, bewustzijn creëren bij medewerkers, samenwerking met leveranciers en een plek op de directieagenda; alles telt mee. Wat verstaan we precies onder het deskundig omgaan met informatiebeveiliging? Welk functieprofiel past bij de rol informatiebeveiliging om dit organisatiebreed te waarborgen.

Veilig omgaan met informatie vereist dagelijkse aandacht. Het vraagt om een professional met de juiste expertise, ervaring en persoonlijkheid om binnen uw organisatie de nodige aandacht voor dit onderwerp te waarborgen.

Om u te helpen bij het vinden van een kundige en vaardige CISO hebben we een functieprofiel opgesteld. Een handig kompas om binnen of buiten uw organisatie de perfecte kandidaat te vinden. De omvang en complexiteit van de organisatie bepaalt de samenstelling van de rol of de zwaarte van de rol ten opzichte van de organisatie. Wij kunnen u uiteraard helpen dit goed in te schatten.

Er zijn verschillende benamingen voor deze rol: Chief Information Security Officer, Information Security Officer of Security Officer.



Competenties

De ideale CISO beschikt tenminste over:

- Minimaal 3-5 jaar **relevante ervaring** op het gebied van informatiebeveiliging en privacy.
- Uitgebreide **kennis** en **ervaring** in het implementeren en beheren van een Informatiebeveiliging Managementsysteem (ISMS).
- Sterke **affiniteit** met zowel organisatorische als technische aspecten van informatiebeveiliging.
- **Grondige basiskennis** van privacywetgeving en gegevensbescherming in de praktijk.
- **Uitmuntende communicatie- en overtuigingsvaardigheden** op bestuurlijk niveau.
- **Vastberadenheid** om als coördinator, implementator en beheerder van het ISMS ook minder populaire boodschappen te brengen.
- In staat om in de praktijk **voorbeeldgedrag** op het gebied van informatiebeveiliging te vertonen.
- Bij voorkeur **trainingen** gevolgd zoals (C)ISO, CISSP, CISA, CISM, RE en examens.
- **Ruime ervaring** met praktijkcases in informatiebeveiliging.





Plek in de organisatie

Als strategische functie bevindt de CISO zich veelal direct onder de Raad van Bestuur of Directie, waardoor zijn/haar rol niet beperkt blijft tot specifieke afdelingen zoals ICT, Facilitair, HR of Inkoop.

Informatiebeveiliging is een organisatiebreed vraagstuk en daarom gaat de verantwoordelijkheid van de CISO ook altijd over alle afdelingen heen. Bescherming tegen (digitale) dreigingen en cyberaanvallen is een gezamenlijke inspanning voor de gehele organisatie.



Verantwoordelijkheden en werkzaamheden van een CISO

Een CISO waarborgt integrale coördinatie en onderhoud van het Informatiebeveiliging Managementsysteem (ISMS). Hij onderhoudt contact met de portefeuillehouder informatiebeveiliging, adviseert over technische en organisatorische maatregelen en bespreekt incidenten. Expertise en toewijding zorgen voor een veilige digitale omgeving, waarin de organisatie optimaal beschermd is.

Een CISO is verantwoordelijk voor:

- Het integraal coördineren en onderhouden van het Informatiebeveiliging Managementsysteem (ISMS) van uw organisatie.
- Het periodiek contact onderhouden met de portefeuillehouder informatiebeveiliging binnen de Raad van Bestuur/Directie over ontwikkelingen, risico's, beheersmaatregelen en verbeteractiviteiten op het gebied van informatiebeveiliging.
- Het informeren, communiceren en adviseren over informatiebeveiliging gerelateerde onderwerpen, met de wet- en regelgeving, normen, standaarden, contractuele eisen en risicoanalyseresultaten als leidraad.
- Adviseren over technische en organisatorische maatregelen met betrekking tot informatiebeveiliging.
- Het bespreken van incidenten, klachten en zorgen van managers en medewerkers over informatiebeveiliging binnen uw organisatie.
- Het formeel beoordelen en goedkeuren van verzoeken om buiten de vastgestelde informatiebeveiligingsprocedures en protocollen te werken of om toegangsrechten buiten de vastgestelde autorisatiematrixen te verlenen.
- Het organiseren en begeleiden van interne en externe audits voor informatiebeveiliging.



Bevoegdheden

Als CISO heeft men de bevoegdheid om:

- Managers en medewerkers aanwijzingen te geven over het volgen van vastgestelde informatiebeveiligingsprocedures, werkinstructies en andere beheersmaatregelen.
- In gesprek te gaan met medewerkers over informatiebeveiliging gerelateerde aspecten zonder formele toestemming van leidinggevenden.
- Zwaarwegende adviezen te geven met betrekking tot (complexe) verzoeken over bijvoorbeeld afwijkingen van toegangsrechten en mandaten, afsluiting van (delen van) het netwerk en netwerkdiensten of tijdelijke of permanente beheersmaatregelen om de informatiebeveiliging te waarborgen.



Tips bij de invulling van de rol

Waar kunt u het beste op letten bij het inhuren van een CISO? Gezien de verantwoordelijkheden en bevoegdheden van de CISO zijn drie zaken van groot belang:

- Om als CISO effectief te functioneren en de verantwoordelijkheden en bevoegdheden optimaal te benutten, is het belangrijk dat hij goed geïnformeerd blijft over de huidige stand van zaken, ontwikkelingen en belangrijke gebeurtenissen binnen én buiten de organisatie.
- Externe ontwikkelingen op het gebied van informatiebeveiliging nauwlettend te volgen en te vertalen naar consequenties voor de organisatie.
- Een goede formele en informele communicatiestructuur op te bouwen, onder andere door regelmatig overleg met sleutelfunctionarissen. Medewerkers bewust maken dat zij zich met specifieke informatiebeveiligingsvragen of -incidenten kunnen melden bij de CISO, inclusief een toegankelijk 'loket' met een eigen telefoonnummer.





Inhuren van een CISO

Risico's vaststellen, maatregelen nemen, bewustzijn creëren bij medewerkers en dit op de directieagenda krijgen; dit vraagt deskundigheid in informatiebeveiliging. Zoekt u ook de juiste persoon? Onze strategische CISO waarborgt integrale coördinatie en onderhoud van ISMS, hij of zij adviseert en bespreekt incidenten.

Onze CISO heeft minimaal 5 jaar ervaring met informatiebeveiliging en privacyvraagstukken, implementeert en beheert uw ISMS, heeft veel affiniteit met organisatorische en technische aspecten. Hij kent de privacywetgeving, is overtuigend op bestuurlijk niveau en toont vastberadenheid. Kies daarom met een CISO van BMGRIP voor een veilige toekomst voor uw organisatie! U kunt rekenen op een CISO die uw informatiebeveiliging organisatiebreed waarborgt. Samen zorgen we voor een optimale bescherming en een naadloze integratie van veiligheidsmaatregelen.

Neem contact met ons op en ontdek hoe onze expertise uw bedrijf kan helpen versterken. Samen bouwen we aan een sterke, veilige en succesvolle toekomst!





Computerweg 22 | 3542 DR Utrecht
030 - 200 8243
info@bmgrip.nl | www.bmgrip.nl