



## **Algemene beschrijving beveiligingsmaatregelen**

BDO ICT voldoet voor de beveiliging van haar organisatie en infrastructuur aan de internationaal erkende standaard voor informatiebeveiliging: de norm ISO 27001. De norm is van toepassing op de ICT-processen: informatie, informatiesystemen, netwerken, en op het IT-personeel dat de bedrijfsprocessen ondersteunt.

Door het regelmatig uitvoeren van informatiebeveiligingscontroles en van in- en externe audits blijft het informatiebeveiligingsniveau van BDO hoog. BDO heeft alle beheersmaatregelen geselecteerd vanuit risicoanalyses en uit de baselines/beleid. Alle maatregelen uit de norm ISO 27001 zijn geïmplementeerd en de audits zijn uitgevoerd door BDO IT audit en BSI.

Het afschrift het ISO 27001 certificaat en bijbehorende verklaring van toepasselijkheid kunnen worden opgevraagd bij de afdeling Quality & Riskmanagement via eerdergenoemd e-mailadres.

De basis voor deze certificering ligt in het informatiebeveiligings- en privacybeleid van BDO. Dit beleid zorgt ervoor dat de organisatie van BDO blijft voldoen aan de norm ISO 27001. Verantwoordelijk hiervoor is de afdeling Quality & Riskmanagement. Een team van Information Security & Privacy Officers is verantwoordelijk voor het rapporteren over beveiligingsincidenten en relevante ontwikkelingen op het gebied van informatiebeveiliging en privacy aan het multidisciplinair samengestelde Forum Informatiebeveiliging binnen BDO.

Binnen het informatiebeveiligingsbeleid van BDO zijn verschillende beheersmaatregelen actief die zijn onderverdeeld in onderstaande categorieën:

- Beveiliging van de fysieke ICT-omgeving en bedrijfslocaties;
- Ontwikkeling en onderhoud van informatiesystemen;
- Veilig beheer van bedrijfsmiddelen;
- Betrouwbaarheid en integriteit van medewerkers;
- Beveiligde applicaties en toepassingen;
- Zorgvuldig leveranciersmanagement;
- Beheer en rapportage van informatiebeveiligingsincidenten.