Bijlage 1: Toetsingskader AO/IC

Nr.	Aspect	Aanlevering van de beschrijving van de AO/IC	Toetsingscriteria
1.	**Wet- en regelgeving** *De energieleverancier dient te voldoen aan de geldende wet- en regelgeving.*	Een beschrijving van de interne beheersmaatregelen in organisatie van de energieleverancier waarmee gewaarborgd wordt dat aan de van toepassing zijnde wet- en regelgeving kan worden voldaan.	• De door de energieleverancier opgestelde normen voldoen aan de wet- en regelgeving • Interne beheersmaatregelen dienen te waarborgen dat te allen tijde wordt voldaan aan de van toepassing zijnde (branche specifieke) wet- en regelgeving. • Medewerkers kennen de wet- en regelgeving die, afhankelijk van hun functie, relevant is en de instanties die toezicht houden.
2.	**Integer handelen** *De genoemde beheersmaatregelen kunnen teniet gedaan worden door 'niet integer (non-conform)' handelen van organisatieleden. De organisatie kan op papier juist werken, maar als voorschriften niet worden nageleefd, en (controle technische) 'checks and balances' omzeild worden, dan kan dit alsnog non-conforme output/prestaties tot gevolg hebben. Het is de primaire verantwoordelijkheid van elke bestuurder/manager/werknemer, bij een energieleverancier om integer te handelen.* *Dit aspect is deels ingevuld aan de hand van de publicatie "Accountants en Toon aan de Top" van de Nederlandse Beroepsorganisatie van Accountants (NBA). Hierbij is uitgegaan van de drie voorwaarden:* *1. Walk the talk: beleving van voorbeeldgedrag van bestuurders;* *2. Zichtbaarheid: voorbeeldgedrag bestuur is zichtbaar;* *3. Open cultuur en vertrouwen: ruimte voor het bespreekbaar maken van dilemma's en of de top open staat voor kritiek.*	Een beschrijving van ten minste de volgende onderdelen: a. Organisatiecultuur; b. Gedragscode; c. Voorkomen van schade in het vertrouwen dat cliënten hebben in de leverancier.	• Er is een gedragscode opgesteld die geldt voor alle medewerkers (inclusief directie, management en ingehuurde derden) van de energieleverancier. Deze gedragscode behandelt tenminste de volgende onderwerpen: a. Integer handelen; b. De wijze waarop het management het goede voorbeeld geeft; c. Aanspreekbaarheid van directie en management door medewerkers; d. De wijze waarop de energieleverancier omgaat met klanten; • Bij de energieleverancier is de rol van compliance officer ingesteld, niet zijnde de hoogste leidinggevende; • In de organisatie is sprake van periodiek overleg, waarbij bestuurders aandacht vragen voor de thema's integer handelen en dilemma's. Dit thema maakt onderdeel uit van gesprekken met nieuw personeel en/of inhuurkrachten.
3.	**Controle technische functiescheiding** *Al naar gelang de omvang van de energieleverancier dienen verschillende personen bevoegd te zijn te beschikken, registreren en controleren.*	Een beschrijving van de opzet van de administratieve organisatie en interne beheersing van de belangrijkste processen (inkoop, verkoop, betaling en administratie) van de energieleverancier. Wanneer processen van de energieleverancier geheel en/of gedeeltelijk zijn uitbesteed dan is dit in de beschrijving van de opzet van de administratieve organisatie en interne beheersing meegenomen.	• Er bestaat adequate controle-technische functiescheiding tussen inkoop, verkoop, betaling en administratie. • Passend naar de omvang van de energieleverancier worden secundaire functiescheidingen aangebracht: er bestaat functiescheiding binnen de processen inkoop, verkoop, betaling en administratie (hierbij zijn verschillende functionarissen verantwoordelijk voor beschikken, registreren, bewaren, uitvoeren en controleren).

Nr.	Aspect	Aanlevering van de beschrijving van de AO/IC	Toetsingscriteria
4.	**Beheersing bedrijfsprocessen (waaronder risicobeheersing)** *De energieleverancier verschaft inzicht in bedrijfsprocessen en de samenhang met hierna benoemde verbandscontrole, controles op informatie en normen. Tevens geeft de energieleverancier een beschrijving van de voornaamste risico's waarmee zij wordt geconfronteerd en heeft de energieleverancier een beschreven methodiek om deze risico's te beheersen.*	Een beschrijving van de belangrijkste bedrijfsprocessen, de aanwezige risico's binnen deze processen en de wijzewaarop deze risico's door de energieleverancier worden beheerst. Tenminste de volgende hoofd processen zijn beschreven: a. Verkoop; b. Inkoop c. Liquiditeitsbeheer; en d. Klachtenbeheer. Bij de beschrijving van de hoofdprocessen zijn tenminste de volgende sub-processen beschreven: a. Facturatie (waaronder het proces voor het opstellen van voorschotnota's en jaar- en eindafrekeningen); b. Meetgegevens processen (het verloop van het berichtenverkeer); en c. Debiteurenbeheer (waaronder de incassoprocedures en het incassobeheer).	• Het proces 'Verkoop' bevat tenminste de volgende interne beheersmaatregelen: a. Verkooptarieven worden vastgesteld door het bestuur van de energieleverancier; b. Afwijkende verkooptarieven worden goedgekeurd door de directie/het bestuur van de energieleverancier; c. Offertes, contracten en verkoopfacturen worden doorlopend genummerd; d. Er zijn duidelijke normen voor: 1) het bepalen van voorschotten; 2) de periode waarbinnen de (eind) afrekeningen aan de klanten worden verstrekt; en 3) de periode waarbinnen de uitbetaling van verschuldigde bedragen aan klanten plaatsvindt; e. Voorschotfacturen en afrekeningen worden steekproefsgewijs gecontroleerd (er bestaat functiescheiding tussen het opstellen en controleren van voorschotfacturen en afrekeningen). • Het proces 'Inkoop' bevat tenminste de volgende interne beheersmaatregelen: f. Er is een geformaliseerd risicobeheersingsproces om het prijsrisico op de vaste prijs portefeuille tot een aanvaardbaar niveau te beperken (er dient een norm te zijn voor de maximale 'risk exposure' van de energieleverancier); g. Het risicobeheersingsproces wordt periodiek gemonitord (teneinde vast te stellen of de 'risk exposure' binnen de onder punt f vastgestelde bandbreedte valt); h. Voorschot- en correctiefacturen betreffende de inkoop van energie worden zichtbaar gecontroleerd (op hoeveelheden en prijzen). • Het proces 'Liquiditeitsbeheer' bevat tenminste de volgende interne beheersmaatregelen: i. Minimaal een keer per maand worden liquiditeitsprognoses door de energieleverancier opgesteld (financieringsbehoeften worden hierdoor tijdig geïdentificeerd). • Het proces 'Klachtenbeheer' bevat tenminste de volgende interne beheersmaatregelen: j. Klachten worden volledig geregistreerd in het klachtenregister en zijn per individuele registratie opvraagbaar (ook achteraf na afhandeling van de klacht, gedurende een passende termijn); k. Er is een duidelijke norm voor de periode waarbinnen klachten moeten worden afgehandeld.

Nr.	Aspect	Aanlevering van de beschrijving van de AO/IC	Toetsingscriteria
4.			• Wanneer de energieleverancier processen geheel en/of gedeeltelijk uitbesteedt, heeft de energieleverancier tenminste de volgende interne beheersmaatregelen geïmplementeerd: l. Service level agreements (SLA) tussen ondernemer en leveranciers zijn aanwezig; m. In de SLA dient aandacht te worden besteed aan de hiervoor beschreven interne beheersmaatregelen (onder punt a t/m l) en de continuïteit van de dienstverlening door leveranciers. n. De ondernemer controleert periodiek of de bepalingen in de SLA worden nageleefd.
5.	**Controle op informatie, verbandscontrole** *Periodiek legt de energieleverancier in ieder geval een sluitend verband tussen ingekochte hoeveelheden energie en de daaruit voortvloeiende inkoopbedragen enerzijds en verkochte hoeveelheden energie en de daaruit voortvloeiende verkoopbedragen anderzijds. De verbandscontrole bestaat uit totalen en is herleidbaar per afnemer.*	Een beschrijving van de energiebalans en het proces van verbandscontrole, waarbij zowel voor elektriciteit als voor gas is aangegeven hoe de leverancier omgaat met allocatie en reconciliatie. *De registers zijn tevens zichtbaar verwerkt in de aangeleverde procesbeschrijvingen, zoals vermeld onder aspect vier.*	• Zie aspect vier, punt f en g voor de minimumnormen voor de energiebalans. • Maandelijks controleert de energieleverancier of de ingekochte energie overeenkomt met de verkochte n energie, zowel in volume als in bedrag (het opstellen en het controleren van dit verband wordt door verschillende functionarissen uitgevoerd). • Bij levering van duurzame energie controleert de energieleverancier maandelijks of de geleverde hoeveelheden duurzame energie per product overeenkomt met een tijdige afboeking van de hiervoor ingekochte garanties van oorsprong.
6.	**Controle op informatie, registers** *De administratie houdt een contractenregister bij waarin alle inkoopcontracten en alle verkoopcontracten zijn opgenomen. Tevens worden er registers bijgehouden van de belangrijkste processen, bijvoorbeeld onderhanden klachten en lopende incasso-trajecten.*	Een beschrijving van tenminste de volgende registers: a. Contractenregister verkoop; b. Contractenregister inkoop; c. Klachtenregister. *De registers zijn tevens zichtbaar verwerkt in de aangeleverde procesbeschrijvingen, zoals vermeld onder aspect vier.*	• De registers zijn afgeschermd, zodat ongeautoriseerde gebruikers geen toegang hebben tot de registers; • Procedures waarborgen dat de registers volledig zijn en opvraagbaar zijn per individuele registratie; • Invoercontroles waarborgen de juist- en volledigheid van ingevoerde gegevens.
7.	**Beveiliging** *De energieleverancier heeft een methodiek om de continuïteit van gegevensverwerking te waarborgen. Daaronder vallen bijvoorbeeld maatregelen om verlies van originele contracten, klachten en elektronische data te voorkomen.*	Een beschrijving van de wijze waarop de aanvrager de continuïteit van gegevensverwerking waarborgt tegen brand, diefstal, cybercrime en fraude. Met specifieke aandacht voor het voorkomen van het verlies van gegevens, het in staat zijn gegevens terug te halen en een functionele en technische scheiding in toegang tot de gegevens.	• Er is functiescheiding tussen de gebruikers- en de beheerorganisatie en de systeemontwikkeling (dit ter voorkoming van niet geautoriseerde wijzigingen in de automatisering); • Applicaties en data zijn afgeschermd door middel van logische toegangsbeveiliging. Dit is erop gericht ongeautoriseerde toegang tot applicaties en data te voorkomen (de functie-scheiding zoals beschreven in de AO/IC zijn via autorisaties vastgelegd in de applicaties). Hierbij zijn er procedures voor het beheer van gebruikersrechten (het toekennen, wijzigen en intrekken van gebruikersrechten dient gecontroleerd plaats te vinden);

Nr.	Aspect	Aanlevering van de beschrijving van de AO/IC	Toetsingscriteria
7.			• Alle mutaties worden gelogd, zodat achteraf is vast te stellen wie welke mutaties heeft aangebracht. • Back-up procedures, om te voorkomen dat elektronische data en originele contracten verloren gaan, zijn aanwezig; • Recovery procedures, om back-up systemen te starten, zijn aanwezig (en worden periodiek getest); • Externe toegang tot systemen (door externe en interne onbevoegden) is afgeschermd.