Bestuur en directie NOREA
De heer drs. W.J.A. Olthof
Postbus 7984
1008 AD Amsterdam
Per email

Utrecht, 13 juni 2023

Betreft: Consultatie ‘Reporting standard Management of IT’

Geachte heer Olthof,

Met veel belangstelling heeft SRA kennisgenomen van het NOREA Reporting Initiative (hierna te noemen NRI), van maart 2023. Op 5 april jl. verzocht u ons feedback te geven op het consultatiedocument ‘Management of IT’. We stellen dit verzoek zeer op prijs.
In deze brief plaatsen we enkele algemene kanttekeningen en beantwoorden we de drie gestelde vragen.

1. Juiste balans
   De 370 SRA-kantoren, inmiddels met de nodige RE’s in hun midden, bedienen gezamenlijk zeker 55% van het Nederlandse (controleplichtige) mkb met personeel. Zij hebben daarbij in toenemende mate te maken met IT-risico’s; Vanzelfsprekend bij het uitvoeren van (wettelijke) controles, en nog veel meer in verband met grote financiële risico’s die kunnen oplopen tot situaties van discontinuïteit.

   Het is daarom evident dat het Nederlandse mkb aan de slag gaat en/of blijft met IT-risico’s. Bezien vanuit deze context is het NRI een goed initiatief. De kanttekening die wij en mkb-opdrachtgevers daarbij willen plaatsen, is dat management van IT geen ‘papieren tijger’ met onnodige administratieve lastenverzwaring moet gaan worden. Tussen stevig IT-beheer en nutteloze administratieve lasten moet de juiste balans gezocht worden.

2. Normenkader uitbestede IT-diensten
   In het mkb wordt veel gewerkt met uitbestede IT-diensten. SRA vindt het van groot belang dat er sprake is van goede ketenaansprakelijkheid, ergo dat het normenkader rekening houdt met ketenverantwoordelijkheden.

   Eén categorie MKB-bedrijven bestaat er niet. Veelal zijn IT-risico’s en impact dan ook niet af te leiden uit de grootte van een onderneming. Bij het ‘normenkader voor uitbestede IT-diensten’ kon per norm een zwaarte worden bepaald en toegelicht. Dat spreekt ons aan.
   In het voorliggende document mag een onderneming bepalen welk IT sub-topic een ‘material topic’ betreft. Wellicht is dat in de praktijk erg moeilijk te bepalen, zeker als bedrijven een lager IT-risico hebben. Dergelijke profilering mag wat ons betreft in het mkb worden toegepast. Daarmee kan wellicht ook de focus (uren/budget) worden gelegd bij die normen die cruciaal zijn voor de onderneming in kwestie.

3. We vinden het een goede stap dat ‘duurzaamheidsimpact van beheer van IT’ wordt geadresseerd.

4. We willen voorstellen dat NBA, NOREA en SRA gezamenlijk vanuit dit normenkader nader onderzoek doen naar de effecten op de accountantscontrole bij het niet voldoen aan deze standaard.

U vroeg ons te reageren op onderstaande drie vragen:

1. Zijn de openbaarmakingsvereisten en -richtlijnen voldoende duidelijk om een organisatie in staat te stellen op een consistente en zinvolle manier te rapporteren over haar beheer van IT?

   SRA mist voldoende guidance of handreikingen over hoe om te gaan met organisaties met bescheiden staf. De topics en requirements zijn terecht. Plaatsing in een mkb-perspectief is lastiger.
   Richten we ons op hoofdstuk 3 (uitbesteding), dan kan een en ander toch nog tot voldoende IT-beheer leiden, ondanks het ontbreken van beleid of richtlijnen van de mkb-onderneming zelf.
   Dus ook naar analogie van NRI zou gewerkt kunnen worden met verantwoordelijkheden in
   - scope 1: het bedrijf zelf;
   - scope 2: de direct ingekochte IT-diensten; en
   - scope 3: de ketenverantwoordelijkheid van de eerste (onder)aannemer.
   Verder zijn de requirements samen met de guidance concreet genoeg om ermee aan de slag te gaan. Ze leveren een positieve bijdrage voor het doel om bedrijven op weg te helpen in de IT-beheersing.

2. Is deze NRI-standaard voldoende bruikbaar voor alle soorten organisaties, bijvoorbeeld ondernemingen, overheidsinstellingen of andere soorten organisaties?

   De standaard is redelijk uitgebreid met veel requirements (de ‘shalls’ en ‘shoulds’). Daarom verwachten wij dat een vrijwillige ‘disclosure’ bij mkb-ondernemingen, op basis van deze NRI niet zo snel zal plaatsvinden. NRI-rapportering en audit kan beter haalbaar zijn als samengewerkt wordt met IT-beheerders en softwareleveranciers. We denken dat de standaard wel hanteerbaar zou zijn voor een assurance-opdracht, vergelijkbaar met de ISAE3000.

   Belangrijk issue voor bedrijven zal de openbaarmaking zijn. Bij ISAE hebben we de opvraagroute. Een openbare verspreiding van de rapportage inclusief details moet naar onze mening voorkomen worden. Een certificaat al dan niet met onderzoekniveau of zelfs kwantitatieve uitkomst, zou wel openbaar gemaakt kunnen worden.

3. Welke instantie zou idealiter verantwoordelijk moeten zijn voor het uitvaardigen en onderhouden van een dergelijke rapportagestandaard?

   SRA heeft geen directe voorkeur. We willen wel benadrukken dat consultatie van IT-auditors uit de mkb-praktijk ons meer dan wenselijk lijkt. Zodoende kunnen we aanbevelingen uit de mkb-praktijk inbrengen, en wellicht koppelen met audits bij IT-dienstverleners.
   We zouden graag het gebruik van NRI na twee jaar met SRA-leden willen evalueren en de resultaten daarvan terugkoppelen zodat aansluiting op de mkb-praktijk optimaal is en blijft.

Vanzelfsprekend zijn we bereid om een nadere toelichting te geven.

Met hartelijke groet,
mede namens SRA IT-Auditkring
en commissie Kwaliteit Vaktechniek

Diana Clement AA RA
bestuursvoorzitter