



CHECKLIST STAKEHOLDERANALYSE ISO 9001 EN ISO 27001

Auteur: Wiebe Zijlstra (7 February 2017)

Nu de verschillende ISO normen een gemeenschappelijke high level structure hebben, kan in feite worden volstaan met één stakeholderanalyse. Stakeholders zijn alle groepen van mensen die een belang hebben bij je organisatie en waarin je organisatie dus ook een belang heeft. Immers, zonder stakeholders heeft je organisatie geen bestaansrecht.

Stakeholders vormen daarmee dus zowel je grootste kans als ook je grootste bedreiging (naast dat je financieel ook moet rondkomen) en daarom de belangrijkste input voor je bedrijfsrisicoanalyse. (Zie ook '[Checklist risico analyse informatiebeveiliging ISO 27001 en NEN 7510](#)'.)

Behalve als input voor je bedrijfsrisicoanalyse kun je de stakeholderanalyse ook gebruiken om:

- kansen voor de organisatie te bepalen;

Je stelt daarvoor de vraag: "Op welke manier kunnen we beter aansluiten op de behoeften van onze stakeholders, om zo hun belang in onze organisatie te verhogen?"

- verspilling in kaart te brengen.

Hier geldt de vraag: 'Op welke van de activiteiten die we ontplooiën zit geen belangrijke stakeholder te wachten?'

De twee grootste valkuilen bij de stakeholderanalyse zijn, dat de klus snel even geklaard wordt, omdat het nu eenmaal moet van de ISO 9001 of ISO 27001 en daarmee vaak samenhangend, onvoldoende betrokkenheid van de directie. Het gevaar bestaat dan, dat de organisatie:

- ineens wordt overvallen door disruptieve concurrenten (zie ook : '[Disruptive innovation is onomkeerbaar](#)') ;
- de focus zo sterk wordt gericht op zaken van secundair belang, dat een hoofdzaak van belangrijke stakeholders wordt vergeten.

Een wel zeer sprekend voorbeeld van het tweede punt zijn politici die zich in de afgelopen jaren in het landsbelang zo sterk gericht hebben op onder andere het terugdringen van overheidstekorten en de bestrijding van terrorisme, dat het

eigenbelang van de burger (en dus de kiezer) vergeten is. Niet voor niets worden zittende partijen massaal weggestemd en krijgen populistten, die zich wel richten op het eigenbelang, de wind weer in de zeilen. Maar ja, ons kabinet is ook niet ISO gecertificeerd. Anders had het dit gevaar al veel eerder onderkend. :-)

Vaak wordt er gesproken over interne en externe stakeholders. Wij houden in deze checklist beide groepen aan, maar verdelen deze weer in subgroepen.

Checklist externe stakeholders

In de checklist externe stakeholders onderscheiden we de volgende subgroepen:

- groepen van klanten, cliënten, afnemers of hoe je ze ook wilt noemen;

In principe heeft ieder van je product-marktcombinaties (PMC) of dienst-marktcombinaties (DMC) een klantengroep, die soms ook weer is onder te verdelen. In de praktijk beperk je je tot de PMC's of DMC's die nu van belang zijn eventueel aangevuld met PMC's of DMC's die op middellange termijn belangrijk worden.

- ketenpartners;

Ketenpartners zijn organisaties waarvan je voor je leveringsproces afhankelijk bent en die niet gemakkelijk zijn te vervangen. Als ze wel gemakkelijk zijn te vervangen, dan gaat het meestal om leveranciers (bijvoorbeeld datacentra of producenten) of soms om afnemers (resellers). Value added resellers zijn vaak wel weer ketenpartners.

- de klant van de klant (of de klant van de ketenpartner);

Soms zijn zij van groot belang voor de eisen, die klanten of ketenpartners aan jou stellen.

- leveranciers die belangrijk zijn voor jouw leveringsproces of je productontwikkeling;

De leveranciers die minder belangrijke of onbelangrijke voor je zijn, laat je weg.

- toezichthouders;

Deze groep is sterk in opkomst. Denk bijvoorbeeld aan de Autoriteit Persoonsgegevens, de VeCoZo in de zorg of andere branche specifieke waakhonden. Vaak worden ook brancheverenigingen hieronder gerekend.

- partijen uit de omgeving;

Dit is een zeer diverse groep, die kan bestaan uit wetgevers (verandering), beïnvloeders van de publieke opinie (reputatieschade), criminelen, vakbonden, buurtbewoners enzovoort. In deze checklist gaan we op deze groep niet verder in.

Partijen uit de omgeving die er eigenlijk altijd zijn en die voor je bedrijf geen specifieke rol vervullen, worden doorgaans weggelaten uit de stakeholderanalyse. Denk hierbij aan bijvoorbeeld concurrenten, de belastingdienst, de overheid, nutsbedrijven enzovoort.

Checklist interne stakeholders

In de checklist interne stakeholders onderscheiden we de volgende subgroepen:

- medewerkers, die weer onder te verdelen zijn in groepen en wel naar twee invalshoeken:
 - het belang dat de organisatie bij de medewerkers heeft en hoe gemakkelijk deze medewerkers beschikbaar zijn op de arbeidsmarkt.
 - de verschillen in eisen van de groep medewerkers (sales, productie, management, support).
- inhuurkrachten;

Meestal zijn dit zzp'ers die voor eigen rekening en risico werken. Werken ze via een detacheringsbureau of bijvoorbeeld een schoonmaakbedrijf of beveiligingsbedrijf, dan is dat bedrijf een leverancier. Eventueel zijn hier ook weer subgroepen in te onderscheiden (handjes, hoofdjes) met vaak verschillende eisen.

- Directie of Raad van Bestuur;

Als de directie ook een belangrijke mede-eigenaar is van het bedrijf, dan is dit een zelfstandige stakeholder. Anders valt ze onder de medewerkers in de groep management.

- aandeelhouders of financiers, die niet tevens bestuurder zijn;

Voor aandeelhouders is dividend vaak van belang en voor financiers de kredietwaardigheid. Voor een DGA (zie directie) gaat het vaak meer om behoud en groei van de waarde van het bedrijf.

- diverse groepen stakeholders met verschillende belangen, die tezamen mede het bestuur van de organisatie vormen zoals bijvoorbeeld de OR, de RvC, RvT en diverse andere raden;

Hier valt weinig in zijn algemeenheid over te zeggen. Maak deze stakeholders echter op basis van politieke correctheid niet belangrijker dan ze in werkelijkheid zijn. In deze checklist gaan we hier niet verder op in.

- achterban van de werknemers;

Soms spelen deze een belangrijke rol bijvoorbeeld bij 7*24 uur organisaties of bij expats. Als ze niet echt van belang zijn, laat ze dan weg.

Waarderen van stakeholders in de analyse

In de stakeholderanalyse moeten per stakeholder 2 zaken in kaart worden gebracht:

- Hoe belangrijk is de stakeholder voor je organisatie (bijvoorbeeld op een schaal van 1-5).
- Welke eisen en behoeften heeft de stakeholder, die voor jou relevant (kunnen) zijn, (bijvoorbeeld ook op een schaal van 1-5).

Begin met je eigen waardering van de organisatie en bedenk, dat de checklist als geheel veel te uitgebreid is. In principe kun je sowieso alle stakeholders met een waardering kleiner of gelijk aan drie weglaten.

NB: bedenk wel, dat het niet gaat om de cijfertjes maar om de kansen en risico's voor je organisatie, die in kaart gebracht moeten worden (zoals in de inleiding is besproken).

Voor de eisen en behoeften van stakeholders is het handig een checklist te gebruiken, waarbij je afsprekt of je een top 3, 5 of 7 selecteert. Als je ze allemaal probeert te waarderen of als je zonder checklist werkt, dan wordt het een zeer tijdrovende operatie, die afleidt van het in kaart brengen van risico's.

Voorbeeld checklist eisen van de stakeholder klant

Hieronder een voorbeeld checklist van mogelijke eisen en behoeften van klanten, die in de praktijk vaak gelden voor een B2B-dienstverlener. Uiteraard mag je deze checklist uitbreiden met bedrijfsspecifieke of branche specifieke eisen.

- Bewezen kwaliteit
- Beschikbaarheid
- Prijs
- Support/service
- Gebruiksvriendelijkheid
- Vertrouwelijkheid
- Betrouwbaarheid product
- Leverbetrouwbaarheid
- Uitbesteding risico's
- Continuïteit dienstverlening
- Vernieuwingen en innovaties
- Privacy
- Reputatie
- Compliance
- Ervaring
- Certificering
- Insourcing
- Materiedeskundigheid
- Inzicht
- Relevantie

Uiteraard heeft ZBC de complete sjablonen beschikbaar voor klanten tijdens de [coachingstrajecten](#) en de '[Cursus Informatiebeveiliging conform ISO 27001, 27002 of NEN 7510](#)'. Daarin wordt ook ingegaan op het gebruik en op de valkuilen bij een stakeholder analyse, zodat snel een solide basis gelegd kan worden voor een adequate bedrijfsrisicoanalyse en een tsunami aan maatregelen voorkomen kan worden.

ZBC helpt organisaties via [coaching](#) of [cursussen](#) om hun informatiebeveiliging conform ISO 27001 of NEN 7510 te verbeteren en desgewenst daarvoor gecertificeerd te worden.