Dutch Harbor
The Procurement Engineers

ICT audit @ Dutch Harbor

Oktober 2019

Kosten Kliniek
Raadgevers en Ingenieurs
More Care, Less Cure, No Repair

Het ICT-gebouw en de behoefte aan een audit

Aanleiding

Het is inmiddels moeilijk geworden om een goed overzicht te hebben op de status van het ICT landschap binnen de organisatie. Het zicht betreft de infrastructuur, netwerk, hardware, applicaties, communicatie, opslag, diensten, etc.. Wat is de huidige situatie, wat zou de situatie kunnen zijn - gegeven de beschikbaarheid van nieuwe inzichten en marktomstandigheden-, is er een acceptabel verschil of dient er een inhaalslag gemaakt te worden. Wat zijn de actuele werkelijke integrale kosten en wat zijn de te verwachten kostenontwikkelingen. Tevens welke risico's worden er op verschillende onderwerpen gelopen ten aanzien van betrouwbaarheid van functioneren, beheersbaarheid, bedrijfscontinuïteit en privacy-zaken. Lastige vragen voor een onderwerp dat bijna al een direct onderdeel van de directe kernactiviteiten is geworden. Tijd voor een audit?

De audit

Kijk naar het ICT-gebouw als een architect. Het gebouw, de functie, de omgeving en de gebruikers. Geef duiding aan de verschillende onderdelen. Past alles nog bij de behoefte van de organisatie. Observeer vanuit de landschapsverkenning naar SWOT analyses, risico assessment en dan veranderen. In de juiste volgorde, veilig en in de tijd die het nodig heeft. Het vertrouwen in robuustheid moet weer terug.

Het onderzoek, de audit, dient zeker drie onderdelen te bevatten hardware, software en beheersing:

1. Functioneren van de hardware; datanetwerk, werkstations, telefonie, wifi, narrowcasting, etc.
2. Functioneren van de software; de verschillende applicaties en het beheer ervan, prestaties op het netwerk, contractbeheer en licenties, is het huidige applicatiepakket efficiënt, en aanpalende relevante vragen.
3. Functioneren van de ICT (externe) beheersorganisatie, wat gaat er goed, wat kan er beter, kunnen de vragen en wensen vanuit de organisatie adequaat afgehandeld worden, etc..

Aanpak voor de audit

1. Landschapsverkenning. Eerst focus aanbrengen en kijken. Wat is de situatie, wie zijn de stakeholders, wat zijn de belangen. Wat zeggen de gebruikers, managers, directie, ICT-manager en andere belanghebbenden. Wat staat er in het jaarverslag over ICT en wat zijn de cijfers. Wat is de ICT-strategie, wat zijn de doelstellingen.
2. SWOT. Om een adequate audit uit te voeren wordt gekeken wat de sterke eigenschappen en kansen zijn die gebruikt kunnen worden. Tevens sterke eigenschappen sterker maken, zwakke eigenschappen aanpakken. De krachten van buiten ook scheiden in kansen om uit te nutten en bedreigingen om te pareren. Per onderdeel te voorzien van een actieplan.
3. Audit. De audit dient te worden onderverdeeld in specifieke hoofdonderwerpen naar aard en gebruik. Samen met de landschapsverkenning, de stakeholder assessment en de SWOT analyse kan een risico assessment gedaan worden. De uitkomst geeft dan de kern van de audit aan. *What if …*
4. Resultaat. Het resultaat is een opsomming van zaken. Waarnemingen vanuit het landschap, bevindingen van stakeholders, assessment van het ICT-gebouw, de omgeving en de diverse functionaliteiten. Verschillende vormen van SWOT analyses op de eigen organisatie en de omgeving. Welke risico's er zijn gesignaleerd en in welke mate zijn die afgedekt. Wat is de huidige situatie, en wat is de gewenste situatie, en hoe daar te komen. Tevens een uitstapje naar de uitvoering en de borging van de gewenste resultaten.

andre.filet@dutch-harbor.nl
www.dutch-harbor.nl

Landschapsverkenning, stakeholders, risico's, organisatie en kosten

Landschapsverkenning – wat zie je vanaf afstand
Wat is in scope, wat is in focus en wat is adresseerbaar. Zijn er dubbelingen. Zijn er gaps & overlaps van functionaliteit bij verschillende pakketten, wat is nut en noodzaak op onderdelen. Zijn er de juiste koppelingen tussen pakketten. Hoe oud zijn de zaken, wat is het huidige aanbod.

Stakeholders assessment – wat vinden de mensen zelf
Een actieve stakeholderdialoog is een belangrijk middel om kansen te benutten en om risico's in de uitvoering van de ICT audit te mitigeren. Hierbij is te zien dat stakeholders verwachtingen hebben van de organisatie om aan hun eigen rol support te kunnen geven.

Mogelijke vragen die beantwoord kunnen worden gaan over o.a. de volgende zaken:

- Wat is de rol en het gewicht van de stakeholder in het geheel.
- Wat is de visie op de support functie van ICT; wat zou die moeten doen.
- Wat is de beleving van de huidige situatie; in detail en toegespitst.
- Wat dient er te veranderen om aan de verwachtingen te voldoen.
- Waar ziet de organisatie als de extremen in termen van jeuk en lol, tops & tips.

Risicomanagement en risicobeheersing
Organisaties willen in het ICT landschap doorgaans nieuwe kansen benutten en risico's zo veel mogelijk voorkomen. Om de belangen zorgvuldig te behartigen betracht men meestal een bepaalde mate van terughoudendheid bij het nemen van risico's. Het tijdig onderkennen en op een juiste wijze inspelen op risico's is daarom cruciaal. Het is van belang dat in alle lagen van de organisatie het risicobewustzijn aanwezig is. De deskundigheid, houding en het controlebewustzijn van de medewerkers spelen hierbij een belangrijke rol.

Het managen van het risico's en de bereidheid om een bepaald risico te aanvaarden dient voor ICT in ieder geval toegespitst te worden op de volgende topics:

- Veiligheid (systeemtechnisch)
- Continuïteit (korte en lange termijn)
- Competenties (kennis van zaken, intern/extern)
- Relaties (partnerkeuzes)
- Flexibiliteit (uitbreidbaarheid)
- On/off premises (cloud)
- Leveranciers afhankelijkheid (make/buy/ally)
- Compliance (privacy, administratieve integriteit, verantwoording)
- Core of non-core

Organisatie. TBV's. Wie doet wat en waarom. Wat zijn de competenties die men nodig heeft en die er zijn. Wat zijn de gaps, wat is het risico dat daarbij hoort en hoe is dit te compenseren. In welke mate wordt de continuïteit van het bedrijfsproces door de beschikbare of ontbrekende competenties bedreigd en indien zo, welke dienen er te worden aangevuld om de continuïteit te managen en te waarborgen.

Kosten. Contract management, waar betaal je voor en wat krijg je expliciet, impliciet en niet. Compleetheid en aanpassingen op inhoud en scope. extern beheer, eigen staf Aard van het onderhoud, preventief of correctief. Reparatie of vervanging. Wie kan de aanvraag beoordelen.