



AURELIUM CHECKLIST

Efficiënte ICT

15 fouten die u beter kunt vermijden

Efficiënte ICT

15 fouten die u beter kunt vermijden

ICT vormt vaak het kloppende hart van een organisatie en moet dan ook bijdragen tot het bedrijfsresultaat. Het is echter niet altijd eenvoudig om het overzicht te bewaren, de zwakke punten binnen uw ICT-infrastructuur op te sporen en aan te pakken zodat u zeker bent dat uw ICT optimaal ingezet wordt binnen de onderneming.

Daarom stelden we deze Checklist voor Efficiënte ICT op. Hierin overlopen we samen de 15 meest voorkomende fouten die u eigenlijk perfect zou kunnen vermijden.

Zo kunt u alvast nagaan dat u hiervan niets over het hoofd gezien heeft.

01 Ondoordachte Back-up & Recovery

Het ontbreken van een goed back-upstelsysteem kan dramatische gevolgen hebben voor elk bedrijf. Heeft u hierover nagedacht?

- ☐ Hoe lang kunt u zich onvoorziene downtime permitteren?
Binnen welke tijdsspanne moet een incident hersteld zijn?
- ☐ Hoe ver kunt u teruggaan in de tijd om een recovery te doen?
Hoe ver kunt u uw business terug tracken in de tijd?
- ☐ Test u regelmatig of uw back-ups ook effectief bruikbaar zijn?
- ☐ Respecteert u de 3-2-1-regel?
- ☐ Staat uw back-up op de geback-upte server?



02 Ontbreken van een Password Policy

Werknemers die geen richtlijnen krijgen rond veilige paswoorden, kunnen een belangrijk security risico vormen voor uw bedrijf. Stel u daarom volgende vragen:

- ☐ Kent u de vereisten waaraan een 'veilig paswoord' moet voldoen?
- ☐ Worden paswoorden regelmatig veranderd?
- ☐ Gebruikt u een password history?
- ☐ Zijn uw gebruikers zich bewust van hun verantwoordelijkheid voor hun eigen gebruikerspaswoord?



03 Ontbreken of negeren van Monitoring

Een gebrekkig monitoringsysteem zal niet tijdig de nodige waarschuwingmeldingen kunnen geven, zodat u vaak niet beseft dat uw systeem dreigt uit te vallen. Zo zullen kleine problemen nodeloos, maar heel snel escaleren.

- ☐ Heeft u een monitoringsysteem?
- ☐ Consulteert u het dashboard regelmatig?
- ☐ Laten de ingestelde thresholds toe tijdig maatregelen te nemen?
- ☐ Neemt u ook meteen de nodige actie, wanneer u een alert krijgt?
- ☐ Heeft u regelmatig onderhoud ingepland staan?

04 Onvolledige Documentatie

Onvolledige of niet-geüpdatete documentatie van uw infrastructuur maakt een snelle en efficiënte probleemanalyse onmogelijk. Het is dan op cruciale momenten vaak compleet onduidelijk hoe uw ICT-infrastructuur is opgezet.

- ☐ Beschikt u over een technische beschrijving van uw infrastructuur?
- ☐ Is deze documentatie voldoende uitgebreid?
- ☐ Wordt deze documentatie regelmatig geüpdatet?

05 Onregelmatige updates

Het ontbreken van belangrijke updates kan uw systeem heel snel destabiliseren. Met enkele eenvoudige ingrepen valt dit nochtans perfect te voorkomen.

- ☐ Worden uw updates automatisch uitgevoerd?
- ☐ Werd er een WSUS-server geïnstalleerd?

06 Gebruik van verouderde software/hardware

Het (té) lang gebruiken van applicaties en toestellen lijkt misschien een goede manier om kosten te drukken. Dit heeft echter vaak een averechts effect. De processen moeten aangepast worden aan de verouderde software, de ondersteuningskosten lopen hoog op, de veiligheidsrisico's vergroten en uw systemen draaien steeds trager en beknotten de productiviteit.

- ☐ Werd er een Life Cycle Management geïmplementeerd voor uw hardware én uw software?



07 Gebrekkige Netwerk security

Een gebrekkige netwerkbeveiliging maakt uw bedrijfsnetwerk en haar data ontzettend kwetsbaar voor aanvallen.

- ☐ Wordt *unauthenticated access* tot uw netwerk toegelaten?
- ☐ Gebruikt u soms de *default paswoorden* uit de fabrieksinstellingen voor uw toestellen?
- ☐ Hebben uw gebruikers toegang tot uw hele netwerk, of enkel de secties die zij nodig hebben?
- ☐ Is uw netwerk *gelaagd* en verdeeld in segmenten?
- ☐ Heeft u alle *standaardinstellingen* aangepast volgens uw behoeften?



08 Gebrekkige Internet security

Een gebrekkige internetbeveiliging maakt uw organisatie erg kwetsbaar voor o.a. aanvallen, virussen en spam.

- ☐ Gaat uw internetbeveiliging verder dan het gebruik van een firewall en een antivirus?
- ☐ Heeft u een duidelijke policy omtrent het gebruik van ICT en internet?
- ☐ Wordt alles wat via het Internet binnenkomt ook gescand en beveiligd?
- ☐ Gebruikt u automatische Intrusion Prevention & Detection Systemen?

09 Fysieke beveiliging verwaarlozen

Een server wordt vaak zomaar weggemoffeld 'ergens' onderaan in een kast of gewoon naast de frigo in de keuken. Uw gevoelige bedrijfsdata wordt op deze manier heel kwetsbaar voor de inwerking van stof en veranderende temperaturen, maar ook voor de grijpgrage handen van malafide individuen.

- ☐ *Staan uw servers in een afgesloten, stofvrije ruimte?*
- ☐ *Is er voldoende ventilatie en/of airco voorzien?*
- ☐ *Staan de servers in afgesloten racks?*
- ☐ *Wordt de toegang tot de serverruimte voldoende gecontroleerd?*

10 Fout opgezet Wifi-netwerk

Wifi wordt vaak gezien als dé oplossing voor connectiviteit. Een slecht afgestelde Wifi werkt niet alleen contraproductief, maar brengt ook ernstige veiligheidsrisico's met zich mee.

- ☐ *Werd uw wifi-netwerk 'gerightsized'?*
- ☐ *Werkt u met tijdelijke paswoorden voor uw gasten of gebruiken ze allemaal één zelfde paswoord?*
- ☐ *Hebben gasten enkel toegang tot het Internet of meteen ook tot uw volledige netwerk?*



11 Verkeerd ingeschat ICT-budget

ICT vormt bij de meerderheid van de bedrijven het kloppende hart van de organisatie. Het onderschatten of verkeerd inschatten van het nodige ICT-budget kan dus nefaste gevolgen hebben voor de bedrijfscontinuïteit.

- ☐ *Doet u aan capacity planning?*
- ☐ *Heeft u een Asset Management systeem?*
- ☐ *Wie is verantwoordelijk voor het Licensing Management?*
- ☐ *Evalueert u uw budgetplanning regelmatig op basis van deze 3 elementen?*

12 Ondoordachte Capacity Planning

Ondoordachte Capacity Planning stelt u vaak voor onaangename verrassingen, zoals onverwachte, zware kosten of zelfs een onderbreking van de bedrijfsprocessen.

- ☐ *Ontwerpt u uw systemen zuiver voor de behoeften van het moment zelf?*
- ☐ *Houdt u hierbij rekening met de maximale workload die uw systeem moet kunnen trekken?*
- ☐ *Houdt u rekening met de bedrijfsgroei die u voorziet in de nabije toekomst?*
- ☐ *Kan de scalability van clouddiensten een oplossing bieden?*

13 Ontbrekend Asset Management

Zonder correct Asset Management kunt u uw ICT-budget niet accuraat inschatten en loopt u grotere risico's doordat uw toestellen niet systematisch en tijdig vervangen worden.

- ☐ *Houdt u bij wie welke devices in gebruik heeft en waar de toestellen staan?*
- ☐ *Houdt u bij wanneer toestellen afgeschreven zijn en vervangen moeten worden?*
- ☐ *Heeft u hiervoor automatische alerts ingesteld?*

14 Gebrekkig Licentiebeheer

Gebrekkig licentiebeheer kan vervelende en verregaande juridische, technische en financiële gevolgen hebben. Het is belangrijk te weten dat uw softwarelicenties te allen tijde overeenkomen met uw bedrijfsbehoeften. Zo bent u zeker dat u niet te veel geld spendeert aan licenties en dat u geen zware boetes riskeert voor het onrechtmatige gebruik van (clandestiene) software.

- ☐ Houdt u het aantal software-installaties en aangekochte licenties bij?
- ☐ Bewaart u alle CD's en licentiecodes en noteert u wie welke software in gebruik heeft?
- ☐ Voert u jaarlijks een inventaris en vergelijkende analyse uit?

Meer info? Download de **checklist voor efficiënt Software License Management**.

15 Geen Policy over ICT-gebruik

Zonder vaste policy is het voor uw werknemers vaak onduidelijk wat kan, mag en moet. Ze zijn zich niet bewust van hun eigen verantwoordelijkheden en voelen zich niet aansprakelijk voor eventueel misbruik.

- ☐ Heeft u de verwachtingen en verplichtingen omtrent ICT-gebruik duidelijk geformuleerd?
- ☐ Heeft u ook expliciet vermeld welke gevolgen misbruik kan hebben?
- ☐ Is deze policy door elke werknemer gekend en erkend?



Uw ICT-infrastructuur optimaliseren met een ICT Audit

Benieuwd of uw ICT-infrastructuur geoptimaliseerd is? Of uw ICT-vesteringen en uw bedrijfsdoelstellingen wel op dezelfde lijn liggen? En welke elementen u juist nodig heeft om uw doelen te bereiken? We gaan het grondig na tijdens de Aurelium ICT Audit.

Vraag hem snel aan!

Haalt u een maximale ROI uit uw ICT?

De Aurelium ICT Audit stemt doelstellingen en investeringen optimaal op elkaar af. Contacteer ons vrijblijvend!

Vraag uw Aurelium ICT Audit aan!

