Soll-IT
Your partner in ITauditing

De toekomst van een IT-auditor in een integrated / financial audit

Robert Johan

Tom Koning

Probleemanalyse

- Gebrek aan kennis accountant
- Niet doorvragen bij ´termen smijten´
- Moeite toegevoegde waarde te tonen
- Accepteren van een algemene opdracht
- Vertaling naar de controle uitdaging

Gebrek aan kennis accountant

- ´er is een back-up´
  - Deels virtualisatie
  - Deels mirroring
  - Meerdere servers
- ‘het netwerk is beveiligd dmv een firewall’
  - ‘Sommige medewerkers hebben VPN’
  - ‘De IT dienstverlener doet alles op afstand’

Niet doorvragen bij ´termen smijten´

- Accountant wil niet dom lijken
- Medewerker klinkt heel deskundig
- Informatie van IT deskundige nodig
- Inventarisatietool soms handig

Online vragenlijst

- Checklist met meest relevante vragen rondom IT
- Mate van automatisering – processen vaststellen
- Mate van geautomatiseerde IB maatregelen application controls
- Open vragen rondom essentiële General IT Controls
  - Hoe hebt u het geregeld
  - Wat is het belang voor uw organisatie
  - Hoe vindt u dat het geregeld is
- **BASIS VOOR CONTROLEPLAN!**

0%

Naam organisatie

Jansma Zwart

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Ingevuld door

De heer Itok

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Functie

Controller

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Plaats

Amsterdam

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Geef de branche aan waarin uw organisatie werkzaam is

Groothandel verpakkingsmaterialen

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Hoeveel vestigingen zijn er in Nederland?

3

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Geef een inschatting van het aantal medewerkers (personen) werkzaam in Nederland

150

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Geef een inschatting van het aantal medewerkers (personen) dat gebruik maakt van uw IT sy

130

Deze vraag is verplicht, u dient de vraag (volledig) te beantwoorden.

Afhankelijkheid betrouwbaarheid geautomatiseerde gegevensverwerking

Wilt u aangeven in welke mate u afhankelijk bent van de betrouwbaarheid van uw IT systemen. Een niet betrouwbare informatievoorziening heeft een niet adequaat (bij)sturing van uw organisatie als gevolg.

Onder betrouwbaarheid verstaan wij de mate waarin de informatie juist en volledig is.

Hoog geeft aan dat u volledig afhankelijk bent van de betrouwbaarheid van uw IT systemen. Alle beslissingen en transacties in de organisatie worden gebasee op informatie uit de geautomatiseerde gegevenverwerkering. Fouten in de geautomatiseerde gegevensverwerking kunnen desastreuse gevolgen voor uw organsiatie hebben.

Gemiddeld geeft aan dat u deels gebruik maakt van (papieren) informatiebronnen.

Laag geeft aan dat u helemaal niet afhankelijk bent van de betrouwbaarheid van uw IT systemen. Geen enkele informatiestroom of transactie is gebaseerd op geautomatiseerde gegevensverwerking. Hiermee geeft u aan dat u andere niet geautomatiseerde bronnen gebruikt.

	Hoog	Gemiddeld	Laag
Mate van afhankelijkheid	◉	○	○

Betrouwbaarheidsscore

Geef hieronder een *betrouwbaarheidsscore* voor uw organisatie in een van de volgende kleuren:

- GROEN: u maakt zich geen enkele zorgen over de betrouwbaarheid van de geautomatiseerde gegevensverwerking.
- ORANJE: voldoet deels en is voor verbetering vatbaar.
- ROOD: u loopt grote risico's: de betrouwbaarheid is niet gewaarborgd.

	Rood	Oranje	Groen
Betrouwbaarheidsscore	○	◉	○

Applicaties

Vul onderstaand schema in:

1. Voer de naam in de van gebruikte applicaties.
2. Geef aan welke bedrijfsprocessen worden ondersteund door desbetrefende applicatie.
3. Geef de overige specificaties per applicatie aan.

	Naam	Versie	Naam van de leverancier	Onderliggende platform/OS	Database model applicatie	Aard applicatie	Bedrijfsproces
Applicatie 1	Dynmaics Nav	4.5	ABC	MS Windows 2008	MS SQL	Maatwerk (deels)	☑ Inkopen ☑ Voorraadbeheer ☑ Financiële administratie ☑ Verkopen ☐ Geldverkeer ☐ Produktie ☐ Lonen en salarissen
Applicatie 2	Rabobank	1.89	Rabobank	Anders	Overig	Standaard	☐ Inkopen ☐ Voorraadbeheer ☐ Financiële administratie ☐ Verkopen ☑ Geldverkeer ☐ Produktie ☐ Lonen en salarissen

Inkoop

Kunt u aangeven welk van onderstaande beheersmaatregelen van toepassing zijn binnen uw organisatie. In de eerste kolom kunt u aangeven of de beheersmaatregel binnen uw organisatie geïmplementeerd is (buiten het systeem om). In het tweede kolom kunt u aangeven of uw applicaties onderstaande beheersmaatregelen / application controls bevatten.

	Ingebed in organisatie	Ingebed in systeem	Beheersmaatregel niet geïmplementeerd
Prijzen en kortingen worden eenmalig in een stambestand vastgelegd en kunnen niet bij het aanmaken van de inkooporder worden gewijzigd	☑	☐	☐
Bestellingen worden in het systeem ingevoerd	☐	☑	☐
Bestelling dienen geflatteerd te worden voordat er besteld kan worden	☐	☐	☑
	☐	☐	☐

Authenticatie

Nadat een gebruiker is *geïdentificeerd* tot een specifieke medewerker dient een adequate *authenticatie* te waarborgen dat de medewerker degene is die hij pretendeert te zijn.
Hieronder vindt u vragen over de wijze van *authenticatie* in uw systemen. Om een adequate authenticatie te waarborgen kunnen verschillende maatregelen worden getroffen, zowel *organisatorisch* (beveiligingsbeleid, richtlijnen, training)
als *technisch* (strak wachtwoordbeheer ondersteund door hardwarematige token of certificaten).

Organisatorische maatregelen dienen bijvoorbeeld ervoor te zorgen dat medewerkers hun wachtwoorden *strikt vertrouwelijk behandelen* en dat zij aansprakelijk zijn voor eventueel misbruik hiervan.
Technische maatregelen zijn maatregelen in systemen die een strikte authenticatie dienen te ondersteunen. Denk hierbij aan het periodiek wijzigen van wachtwoorden, minimale lengte hiervan en inzet van zogenaamde tokens.

Slechte authenticatie kan leiden tot *functievermenging* en dus tot een *onbetrouwbare informatievoorziening*.

Wilt u hieronder aangeven welke maatregelen zijn getroffen om een adequate authenticatie te verzorgen. Geef ook aan hoe en door wie dit gecontroleerd wordt.
Wij willen u verzoeken om dit voor de volgende drie lagen te doen:
1. Applicaties
2. Netwerkomgeving
3. Toegang vanuit publieke netwerken zoals Internet

Authenticatie applicaties. Geef hieronder aan tot welke applicaties apart toegang wordt verschaft en hoe de authenticatie is geregeld in desbetreffende applicatie.

Stelling authenticatie
Wilt u in onderstaande het volgende aangeven:
- Het belang van authenticatie voor uw organisatie. (*Hoog* = van groot belang, Gemiddeld = deels van belang, Laag = geen enkel belang)

	Hoog	Gemiddeld	Laag
Het belang van authenticatie	◉	○	○

Mate van beheersing
Geef met een kleur aan in welke mate u vindt dat uw organisatie met de genomen maatregelen aan dit belang voldoet:

- **GROEN:** het is conform uw vereisten.
- **ORANJE:** voldoet deels en is voor verbetering vatbaar
- **ROOD:** er zijn ernstige tekortkomingen

	Rood	Oranje	Groen
Mate van beheersing	○	○	◉

Moeite toegevoegde waarde te tonen

- Adviezen geven geen aanknopingspunt
- Door gebrek aan gevonden fouten onvoldoende draagkracht
- IT auditors zonder ‘modder aan de schoenen’

Een algemene opdracht

- Geen integratie
- Geen consequenties
- Lastig indien vervelende bevindingen
- Budget
- Geen toegevoegde waarde accountant / klant
- Afbreuk beroep

Een algemene opdracht

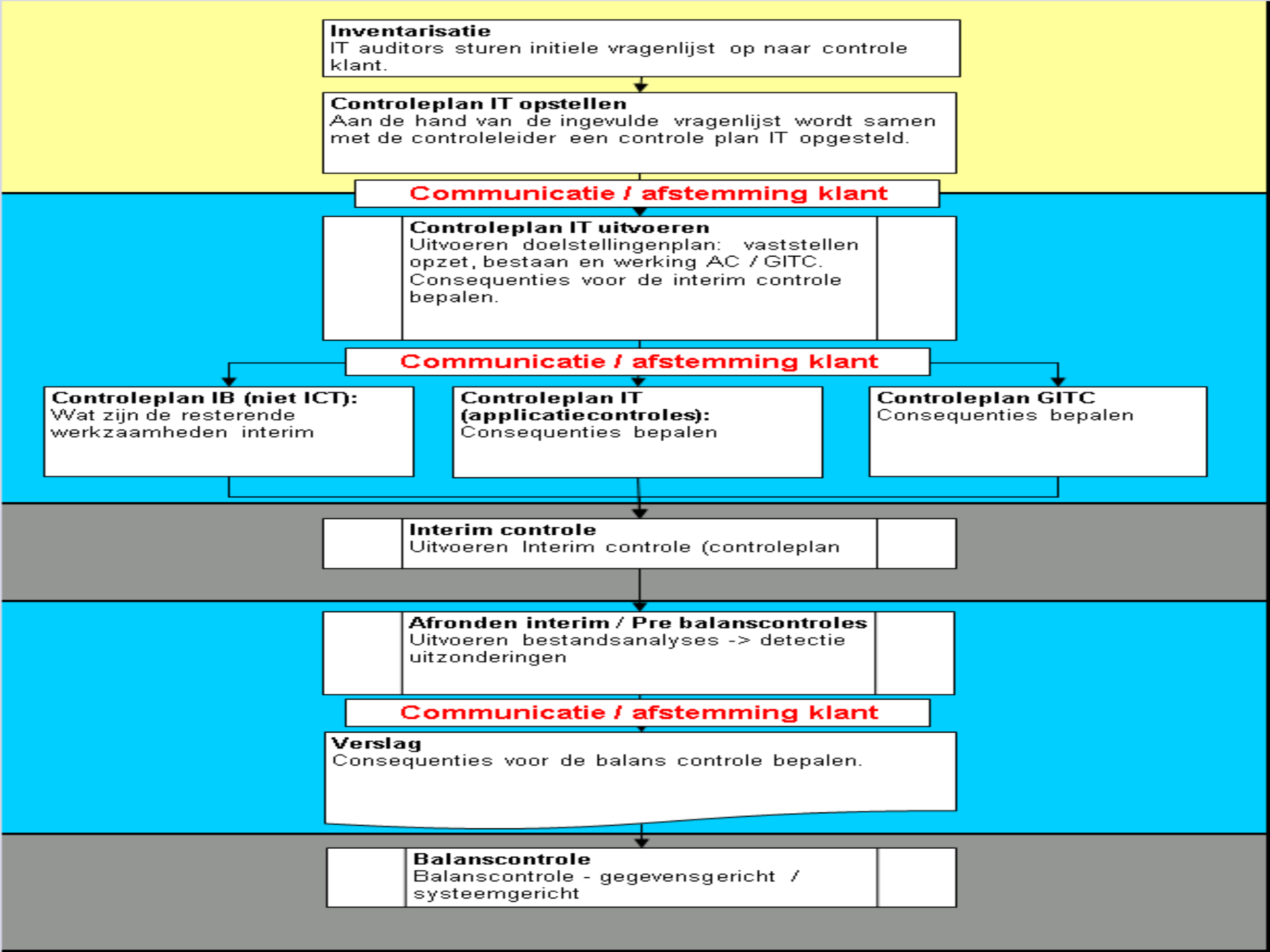
- Kies één onderwerp
- Bevraag accountant over omstandigheden
- Informeer de accountant over risico's
- Stem werkverdeling af
- Draag in jaar 2 over en kies volgende onderwerp

Bevragen accountant

- Backup?
  - RPO / RTO
  - Virtualisatie
  - SAN
  - Redundantie (RAID oplossingen zoals mirroring)
  - Online
  - Imaging
  - Cloud

Vertaling naar de controle uitdaging

- Continuiteitsrisico wordt soms laag ingeschat
  - Pas diepgang van werkzaamheden daarop aan
  - Wijs op formele verplichting
- Let op verschil tussen fraude en fouten
  - Bij fouten is diepgaande analyse netwerkbeveiliging minder cruciaal
  - Zoek naar belangrijkste schattingen en daarbij behorende rapportages
  - Zorg ervoor dat je opvolging paraat hebt


Inventarisatie
IT auditors sturen initiele vragenlijst op naar controle klant.
Controleplan IT opstellen
Aan de hand van de ingevulde vragenlijst wordt samen met de controleleider een controle plan IT opgesteld.
Communicatie / afstemming klant
Controleplan IT uitvoeren
Uitvoeren doelstellingenplan: vaststellen opzet, bestaan en werking AC / GITC. Consequenties voor de interim controle bepalen.
Communicatie / afstemming klant
Controleplan IB (niet ICT):
Wat zijn de resterende werkzaamheden interim
Controleplan IT (applicatiecontroles):
Consequenties bepalen
Controleplan GITC
Consequenties bepalen
Interim controle
Uitvoeren Interim controle (controleplan
Afronden interim / Pre balanscontroles
Uitvoeren bestandsanalyses -> detectie uitzonderingen
Communicatie / afstemming klant
Verslag
Consequenties voor de balans controle bepalen.
Balanscontrole
Balanscontrole - gegevensgericht / systeemgericht

Help de accountant over de drempel!

- Elke application control moet een andere activiteit vervangen!
- Wat is het belang van de application control en wat zijn de consequenties indien niet / onvoldoende aanwezig.
- Welke General IT Controls zijn van belang?
- Stel IT risico's vast en maak vertaalslag naar audit risks.
- **ZO BEREIK JE TOEGEVOEGDE WAARDE IN DE CONTROLE MAAR OOK VOOR DE KLANT!**

Hoe dan wel -> de praktijk

- Groothandel -> risico verkoopproces:
  - Juistheid prijzen + niet factureren leveringen
- IB maatregel klant -> anomalie lijst
- Accountant stelt vast procedure rondom anomalielijst
- IT auditor stelt vast juistheid anomalielijst-> code review -> verdieping kennis data-model
- Geconstateerd -> code review akkord echter:
  - Geen aantoonbare change management…….
  - Te ruime bevoegdheden logische toegangsbeveiliging GIP (authenticatie + autorisatie)

Praktijk voorbeeld–Logische toegangsbeveiliging

- Casus AFM rapport -> schadeverzekeraar
- IT auditor -> “Autorisatie toetsen”
- Bevinding -> autorisaties zwak -> groot aantal medewerkers hebben toegang tot alle functies in het systeem.
- Risico -> doorbreking functiescheidingen: polis- en schade administratie, financiële administratie en stamgegevens.
- Conclusie accountant -> Deze General IT Controls zijn toereikend voor de controle……
- Onvoldoende beoordeeld wat de risico’s zijn voor deze tekortkomingen.
- Specifieke combinaties identificeren de sleutel

Hoe dan wel -> de praktijk

- Mediabedrijf-> risico verkoopproces:
  - Juistheid tarieven advertenties
- IB maatregel klant -> ´beoordeling totale opbrengst´
- IT auditor regelde backup ERP pakket
- Naar IDEA inlezen via SQL express
- Tarieven en omzetten bleken volstrekt onbetrouwbaar