10 ISAE 3402 myths demystified

ISACA Round Table

18:30 – 20:00, Breukelen, 6 november 2017

Spreker: drs. Norbert Kuiper CISM, CISA

Agenda

a. Welkom
b. De Theorie
c. De Praktijk
d. Vragen

Insteek

ISAE 3402 is in ontwikkeling

Veel bronnen en informatie vanuit auditor's perspectief (NOREA, accountants, e.a.)

De laatste stand van zaken via: 19 juni 2017 – ISACA Round Table – Han Boer

ISAE 3402 als aanjager voor organisatieverandering / professionaliseringsslag

Over deze sessie

In deze sessie wil ik:

- Uw kennis over ISAE3402 weer even opfrissen
- Mijn ISAE3402 ervaringen delen
- Uw ISAE3402 ervaringen horen en discussie

Mijn achtergrond:

- Het implementeren van een ISAE3402 bij een service-organisatie
- Het uitvragen van ISAE3402 eisen bij leveranciers
- Het beoordelen van diverse ISAE3402 rapportages o.a. van ISP en cloud leveranciers

Even voorstellen

drs. Norbert Kuiper CISM, CISA
Senior Consultant CyberSecurity & Business Resilience
Verdonck Klooster & Associates
06 8108 7221
norbert.kuiper@vka.nl
www.vka.nl

Verdonck Klooster & Associates

IT STRATEGIE & ARCHITECTUUR >

PROGRAMMAMANAGEMENT & COMMUNICATIE >

DATA & DIGITALISERING >

SOURCING & REGIE >

CYBERSECURITY & CONTINUÏTEIT >

PRIVACY >

INFORMATIEGESTUURD WERKEN >

INTERIM MANAGEMENT >

AGILE >

AUDIT & ASSURANCE >

Volg ons via:

Evenementen

Nieuws

10 ISAE 3402 myths demystified

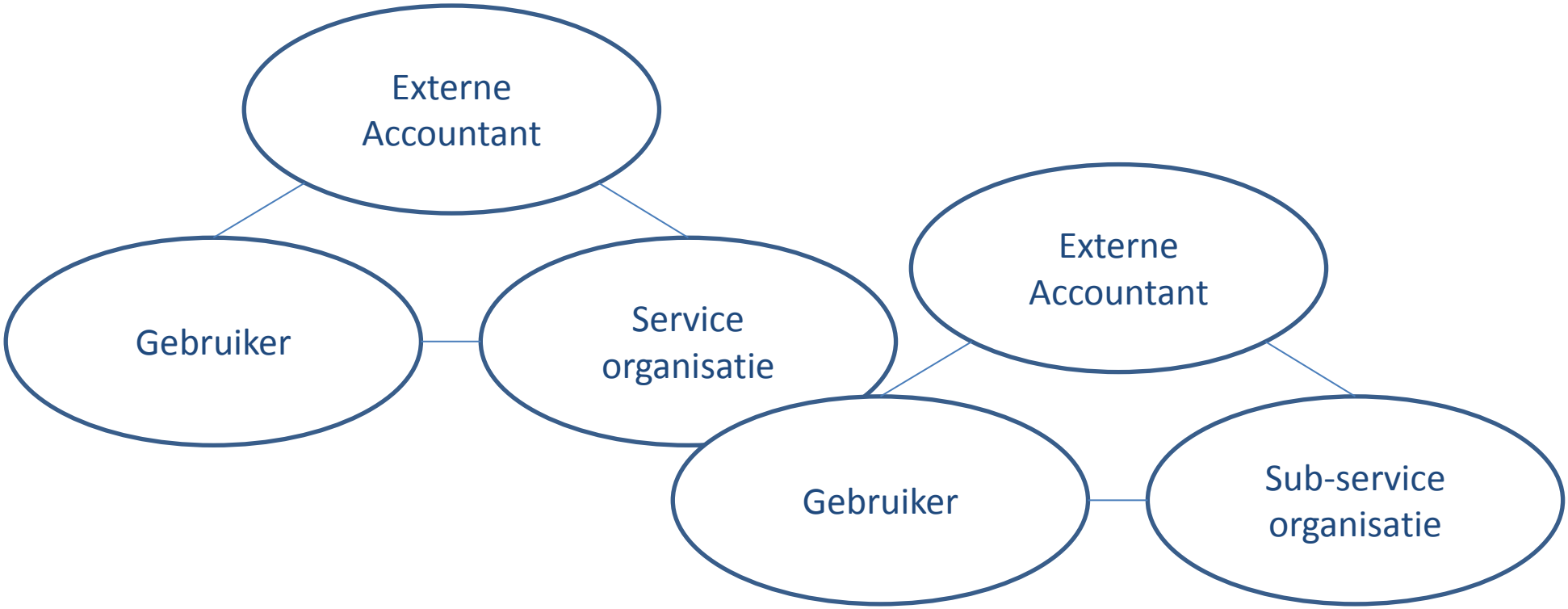
Vanuit de theorie:

1. Een ISAE 3402 is een tripartite model
2. De doelgroep van een ISAE 3402 is de gebruikersorganisatie
3. De ISAE 3402 assurance rapportage = onafhankelijk toetsing vh management systeem
4. Er is 1 soort ISAE 3402 rapportage
5. De externe auditor schrijft het ISAE 3402 rapportage

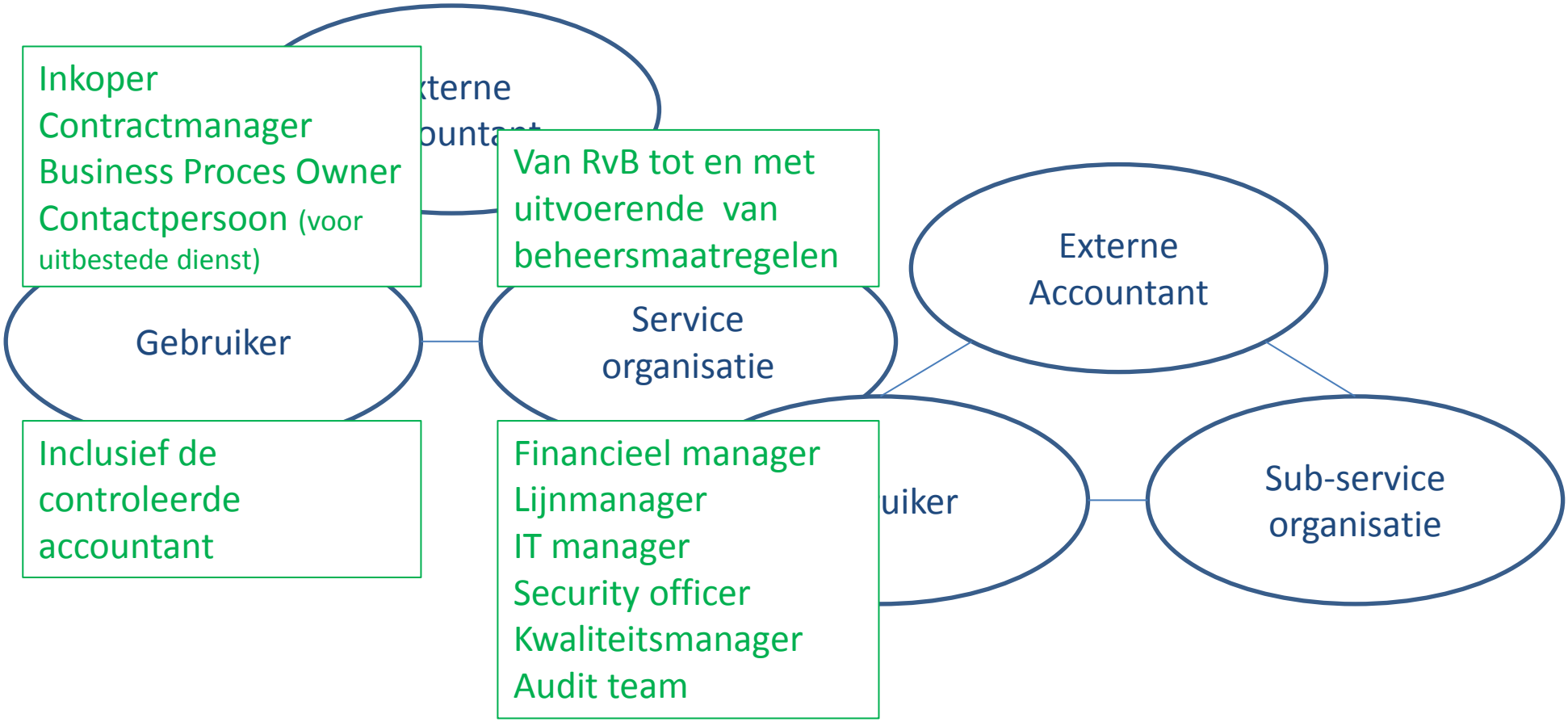
Vanuit de praktijk:

6. Een ISAE 3402 is een walk in the park
7. Een overeengekomen ISAE 3402 is vervolgens voor altijd in beton gegoten
8. Om een ISAE 3402 te behouden is de rol van de externe auditor doorslaggevend
9. Het beoordelen van een ISAE 3402 rapportage is een kwestie van 0-en en 1-en
10. Een ISAE is het enige middel om zekerheid te bieden

1. Betrokkenen bij een ISAE 3402



2. Doelgroep van een ISAE 3402



3. Doelstelling van een ISAE 3402

ISAE 3402 – assurance rapportage

a. Doel: Onafhankelijk oordeel
b. Middel: Assurance opdracht
c. Door: Externe RE-auditor
d. Scope: Vastgesteld normenkader

e. Verklaring van het management
f. Attestation van de IT-auditor

g. Mate van zekerheid
    a. Redelijke mate van zekerheid
    b. Beperkte mate van zekerheid

ISO xx001 – Management systeem

a. Doel: Onafhankelijke toetsing
b. Middel: Certificering
c. Door: Externe ISO auditor
d. Scope: Management Systeem

4. Diverse soorten ISAE 3402 rapportage

SOC 1:

- Scope: financiële verslaglegging
- Doel: volledigheid en juistheid van de financiële verslaglegging
- Type 1 (rapportage moment / opzet en bestaan) en 2 rapport (rapportageperiode / opzet en bestaan en werking over 6-12 maanden)
- Wat: systeembeschrijving, beschrijving van de transactieverwerking, beheersingsdoelstellingen/ beheersingsmaatregelen, beschrijving van de controleomgeving
- Soms *ten onrechte* ook gebruikt als instrument om een generieke verklaring af te geven

SOC 2:

- Scope: breed toepasbaar voor IT-gerelateerde processen
- Doel: vast gedefinieerde beheersdoelstellingen tav security, confidentiality, availability, processing integrity, confidentiality, of privacy
- Type 1 (rapportage moment / opzet en bestaan) en 2 rapport (rapportageperiode / opzet en bestaan en werking over 6-12 maanden)
- Wat: ISAE 3402, waarbij de beheersdoelstellingen nader zijn geconcretiseerd met ‘Principles and Criteria’
- Voorgeschreven werkwijze, voorgeschreven teksten (Amerikaanse auditorganisatie AICPA)

SOC 3:

- Zie SOC 2, maar nu ….
- Uitgebreide rapportage (2) vs beperkte rapportage (3)
- Verspreiding in beperkte kring (2) vs uitgebreide kring (3)

5. De ISAE 3402 rapportage van de service-organisatie

ISAE3402 Type 2 Rapportage

Sectie 1: Assurance-rapport van de onafhankelijke auditor en mededeling management

Sectie 2: Beschrijving service organisatie en algemene beheersomgeving

Sectie 3: Informatie verstrekt door de onafhankelijke auditor

Sectie 4: Overige informatie verstrekt door de service organisatie
- Management reactie
- Informatie omtrent overige maatregelen

Uitspraken van de onafhankelijk auditor:

'geef de beschrijving van het proces, applicaties en systemen getrouw weer zoals is opgezet en geïmplementeerd.'

'beheersdoelstellingen zijn op afdoende wijze opgezet'

'werkten de getoetste interne beheersmaatregelen, die noodzakelijk waren om een redelijke mate van zekerheid te verschaffen …… effectief.'

Verklaring van het management:

'bijgaande beschrijving is een getrouwe weergave van proces, applicaties, systeem en de daaraan gerelateerde IT beheersmaatregelen.'

'…de volgende beheersdoelstellingen niet zijn bereikt.'

'de overige beheersmaatregelen op afdoende wijze zijn opgezet en effectief werkten.'

> 'De risico's die het bereiken van de doelstellingen in gevaar kunnen brengen, werden onderkend.'
>
> 'Beheersmaatregelen een redelijke mate van zekerheid zouden verschaffen dat die risico's het behalen van de doelstellingen niet zouden verhinderen. '
>
> 'Maatregelen zijn consistent toegepast zoals opgezet, inclusief de handmatige maatregelen zijn toegepast door personen die de geschikte competentie en bevoegdheid hebben.'

10 ISAE 3402 myths demystified

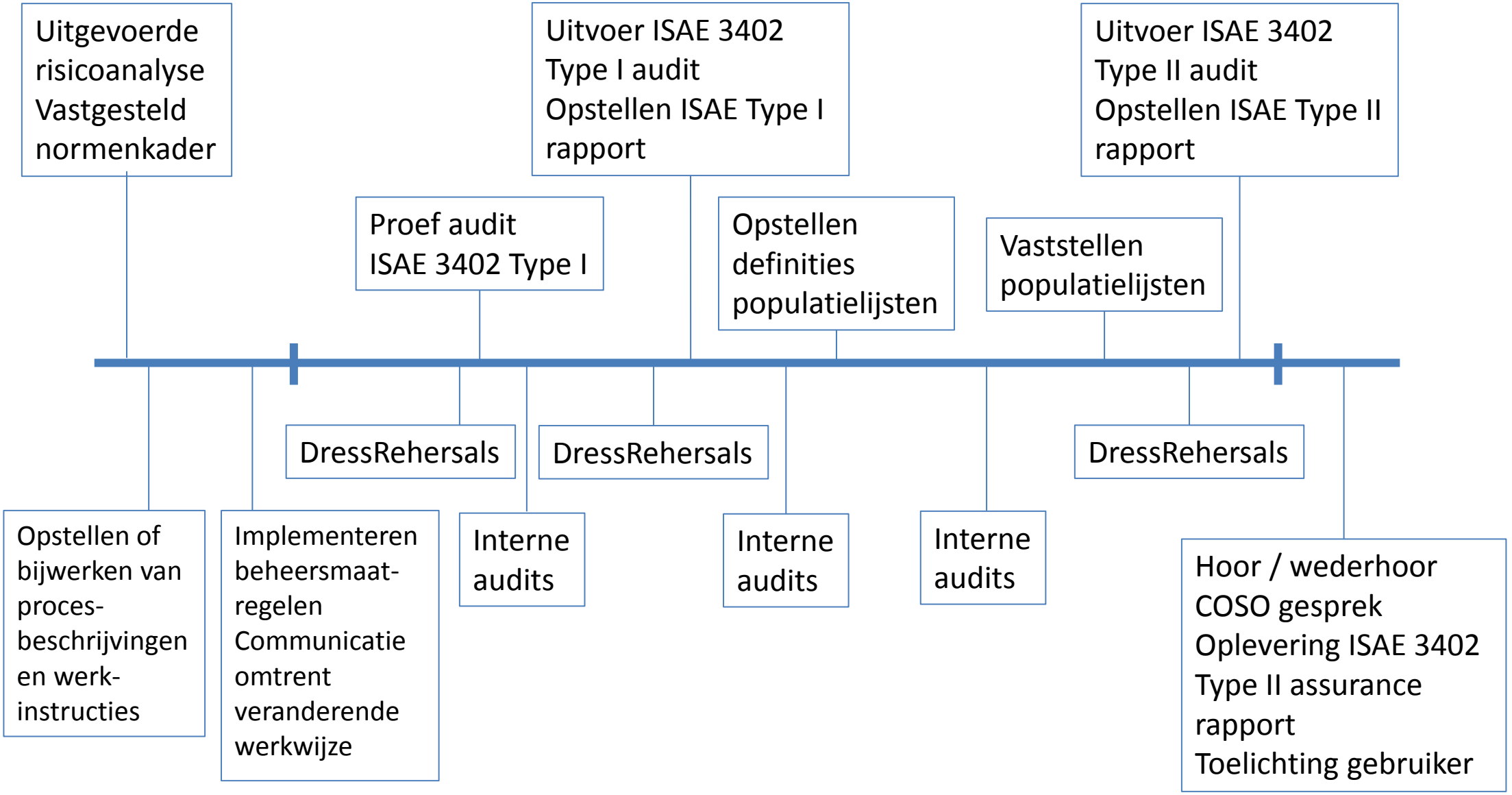
Vanuit de theorie:

1. Een ISAE 3402 is een tripartite model
2. De doelgroep van een ISAE 3402 is de gebruikersorganisatie
3. De ISAE 3402 assurance rapportage = onafhankelijk toetsing vh management systeem
4. Er is 1 soort ISAE 3402 rapportage
5. De externe auditor schrijft het ISAE 3402 rapportage

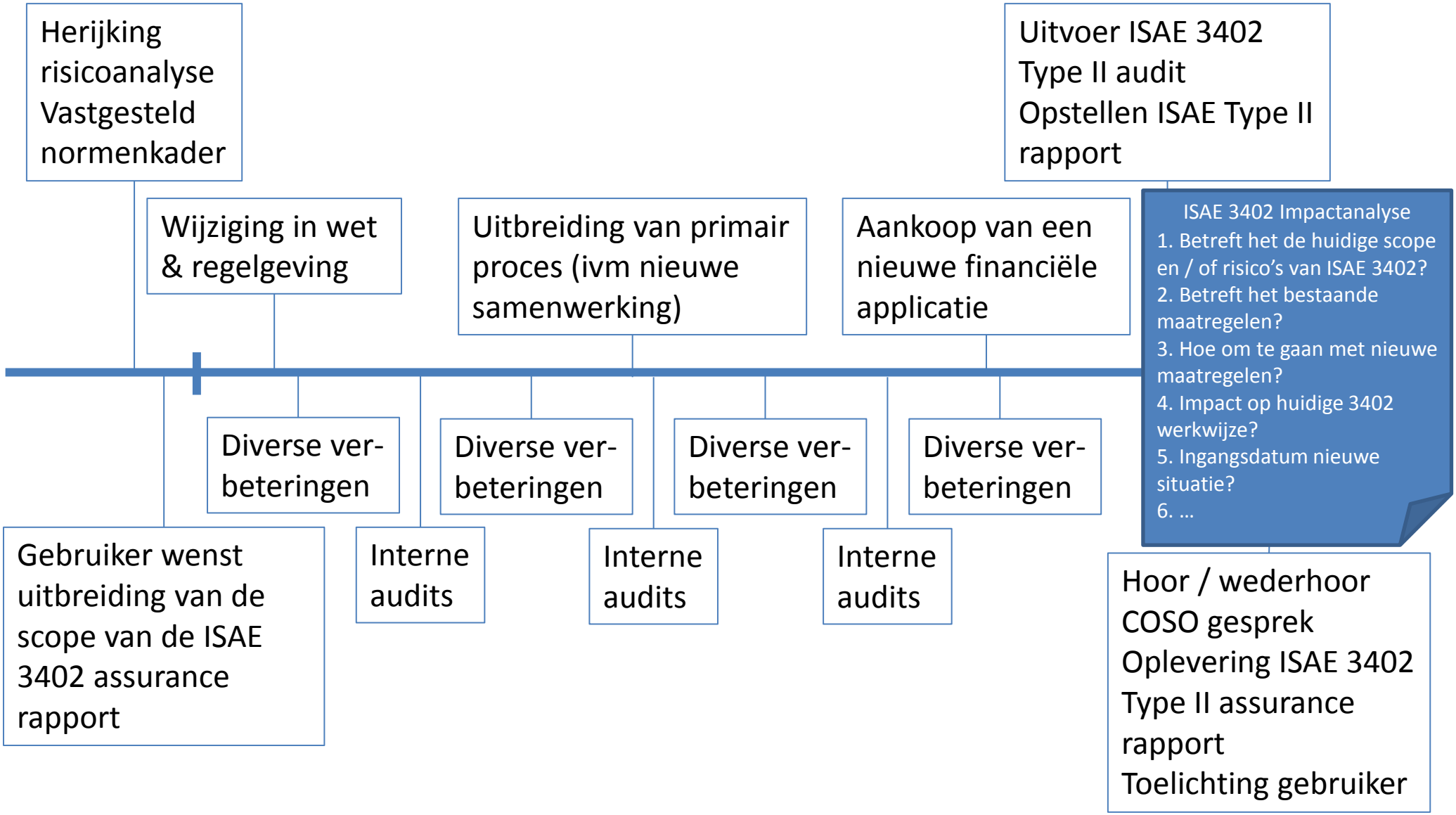
Vanuit de praktijk:

6. Een ISAE 3402 is een walk in the park
7. Een overeengekomen ISAE 3402 is vervolgens voor altijd in beton gegoten
8. Om een ISAE 3402 te behouden is de rol van de externe auditor doorslaggevend
9. Het beoordelen van een ISAE 3402 rapportage is een kwestie van 0-en en 1-en
10. Een ISAE is het enige middel om zekerheid te bieden

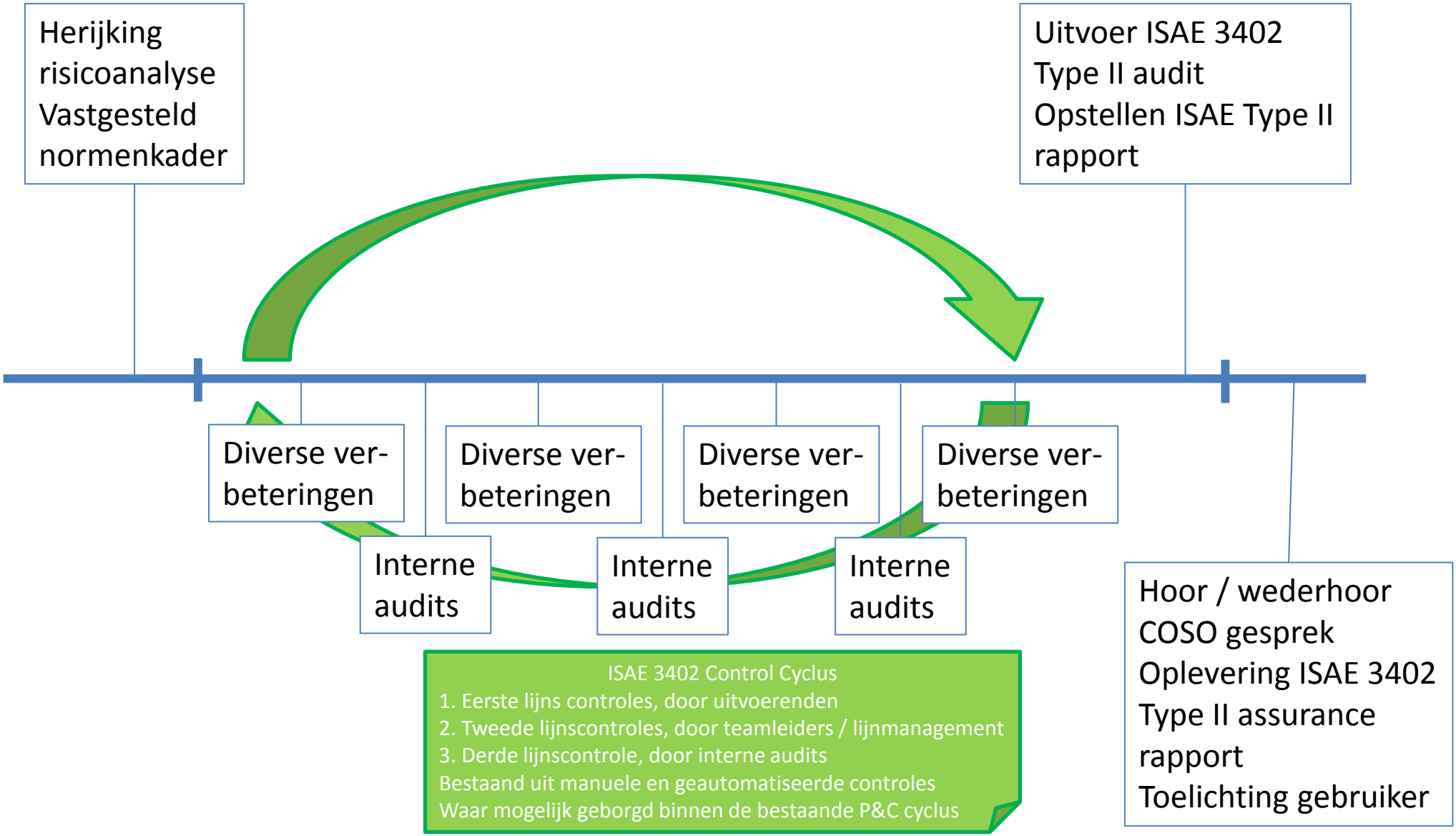
6. De tijdslijn van een ISAE 3402 Type II – jaar 1



7. De tijdslijn van een ISAE 3402 Type II – jaar 2, …



8. De rol van de interne auditor is doorslaggevend



9. Het beoordelen van een ISAE 3402 Type II rapportage

Maturity level 0-1:

i. Geen basis
ii. Spraak verwarring
iii. Onduidelijkheid omtrent maatregelen
iv. Wij versus jullie

Maturity level 2-3:

i. ISO 27001 of soortgelijke certificering
ii. Rollen en verantwoordelijkheden zijn belegd
iii. Is kwaliteitsdenken (PDCA) geborgd
iv. Samen kijken naar verbeteringen

Maturity level 4-5:

i. ISAE 3402 verklaring
ii. Welke maatregelen voert de service organisatie voor mij uit en is dit effectief
iii. Zijn mijn risico's hiermee voldoende afgedekt
iv. Samenwerken tav risicomanagement

10. Alternatieven voor ISAE 3402

Assurance via ISAE 3402

ISAE3402 Type 2 Rapportage

1. Sturend proces 1
2. Financieel proces 1
3. Financieel proces 2
4. Primair proces 1
5. Primair proces 2
6. Primair proces 3
7. Primair proces 4
8. Primair proces 5
9. IT Proces 1
10. IT proces 2
11. IT proces 3
12. IT Proces 4
13. IT Proces 5

Zekerheid op alternatieve wijze

Operationele rapportages

1. Sturend proces 1
2. Financieel proces 1
3. Financieel proces 2

ISO 9001

4. Primair proces 1
5. Primair proces 2
6. Primair proces 3
7. Primair proces 4
8. Primair proces 5

IT General Controls

9. IT Proces 1
10. IT proces 2
11. IT proces 3
12. IT Proces 4
13. IT Proces 5

Legenda:

- Assurance via ISAE 3402
- Zekerheid obv diverse operationele rapportages
- Zekerheid obv certificering
- Zekerheid obv toetsing ITGC als onderdeel van jaarrekeningcontrole

10 ISAE 3402 myths demystified

Vanuit de theorie:

1. Een ISAE 3402 is een tripartite model
2. De doelgroep van een ISAE 3402 is de gebruikersorganisatie
3. De ISAE 3402 assurance rapportage = onafhankelijk toetsing vh management systeem
4. Er is 1 soort ISAE 3402 rapportage
5. De externe auditor schrijft het ISAE 3402 rapportage

Vanuit de praktijk:

6. Een ISAE 3402 is een walk in the park
7. Een overeengekomen ISAE 3402 is vervolgens voor altijd in beton gegoten
8. Om een ISAE 3402 te behouden is de rol van de externe auditor doorslaggevend
9. Het beoordelen van een ISAE 3402 rapportage is een kwestie van 0-en en 1-en
10. Een ISAE is het enige middel om zekerheid te bieden

Dank voor uw aandacht!

Vragen?

drs. Norbert Kuiper CISM, CISA
Senior Consultant CyberSecurity & Resilience
Verdonck Klooster & Associates
06 8108 7221
norbert.kuiper@vka.nl
www.vka.nl

Interessante links:

Theorie:

https://www.compact.nl/articles/nieuwe-ontwikkelingen-it-gerelateerde-service-organisation-control-rapportages/

http://www.spo.nl/Uploads/2013/10/6.1.1-Praktijkgids-4-ISAE-3402--KPMG-2012-.pdf

https://chapters.theiia.org/Denver/ChapterDocuments/SOC%20Presentation%20Denver%20IIA.pdf - UPDATE

Overige links:

https://www.isae3402.nl/

https://www.auditconnect.nl/nl/it-audits/isae-3402/type1-en-type2/