Cloud Computing,
een inleiding

ICT Accountancy & Financials congres 2013:

Cloud computing en eFactureren

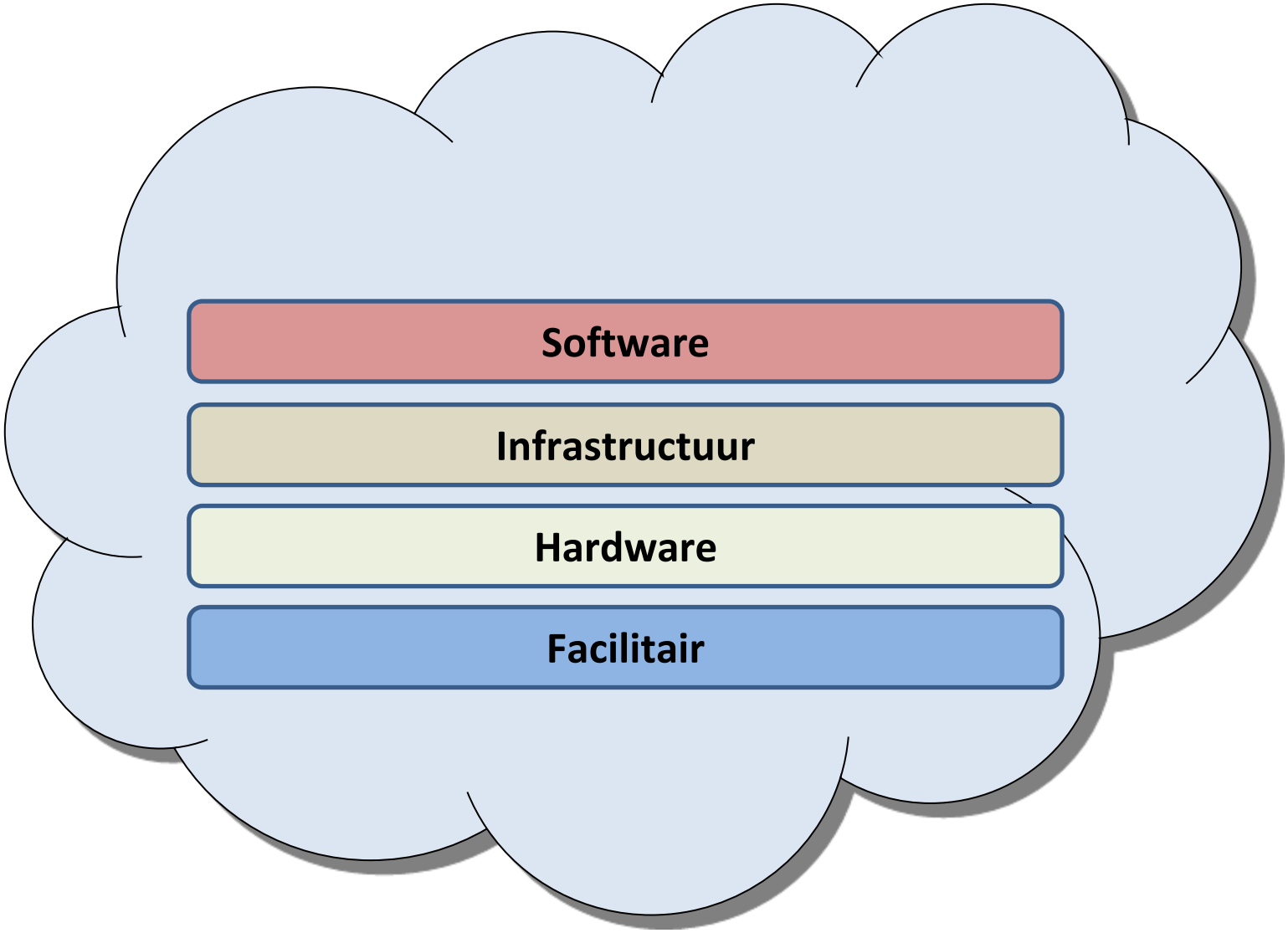
10 december 2013

Jan Pasmooij RA RE RO: jan@pasmooijce.com

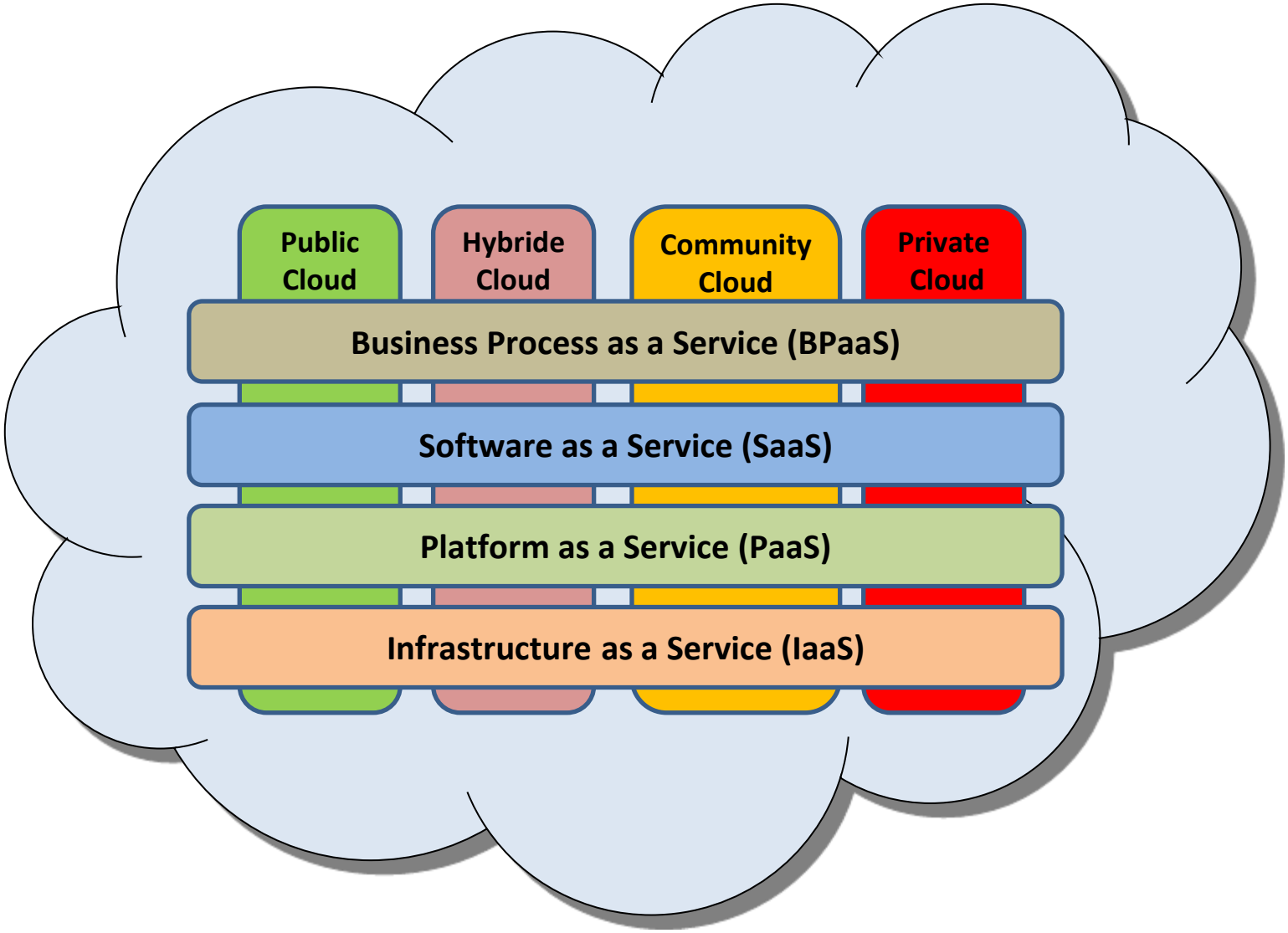
Kenmerken van Cloud Computing

- Overal toegankelijk (via Internet)
- Lagere kosten (alleen betalen voor gebruik)
- Schaalbaar
- Gemeenschappelijk en gedeeld gebruik (efficiencyvoordelen)
- Geen beheer en onderhoud (afhankelijk van de soort Clouddienst en het gebruik)
- Groot aanbod diensten

Cloud Computing



Cloud Computing (in theorie)



Cloud Computing (in de praktijk)

- Combinatie van toepassingsmodellen
- Redenen:
  - Samenwerking Cloudaanbieders
  - Flexibiliteit
- In de praktijk niet altijd duidelijk wie feitelijk de Clouddienst levert en onder welke voorwaarden

‘Nieuwe’ risico’s

- Afhankelijkheid van de aanbieder
- Afscherming van de gegevens (beveiliging en vertrouwelijkheid)
- Bedrijfszekerheid (performance en continuïteit)
- Aanpassingen en aansluiting op bestaande bedrijfsprocessen
- Verantwoordelijkheid maar ook aansprakelijkheid bij dataverlies / schade
- Gemeenschappelijk en/of gedeeld gebruik van verwerking en opslag
- Het kunnen voldoen aan wet- en regelgeving
- Het kunnen overstappen naar een andere aanbieder

Aandachtspunten

- Vermenging van data door virtualisatie / gedeeld gebruik (Multi-tenancy)
- Dataopslag (locatie / omstandigheden)
- Intern beheer en interne beheersing bij aanbieder (waaronder change management)
- Beveiliging (logisch en fysiek)
- Continuïteit / performance
- Connectiviteit
- Compliance
- Aansprakelijkheid
- Vendor lock-in

Potentiële risico's bij uitbesteden?

- Grote afhankelijkheid van derde partij
- Gebrek aan eigen deskundigheid en daarmee onvoldoende aansturing / controle
- Derde partij is niet in staat bedrijfswensen in te vullen en daarmee strategische voordelen te realiseren
- Lange doorlooptijden om zaken te kunnen realiseren
- Uiteindelijk hogere kosten en minder flexibel
- Geen partner maar 'tegenstander'
- Uitbesteder heeft zijn zaken niet op orde, daardoor geen of onvoldoende aansturing
- Verwachtingen uitbesteder vooraf onvoldoende duidelijk

Wat moet je zelf regelen?

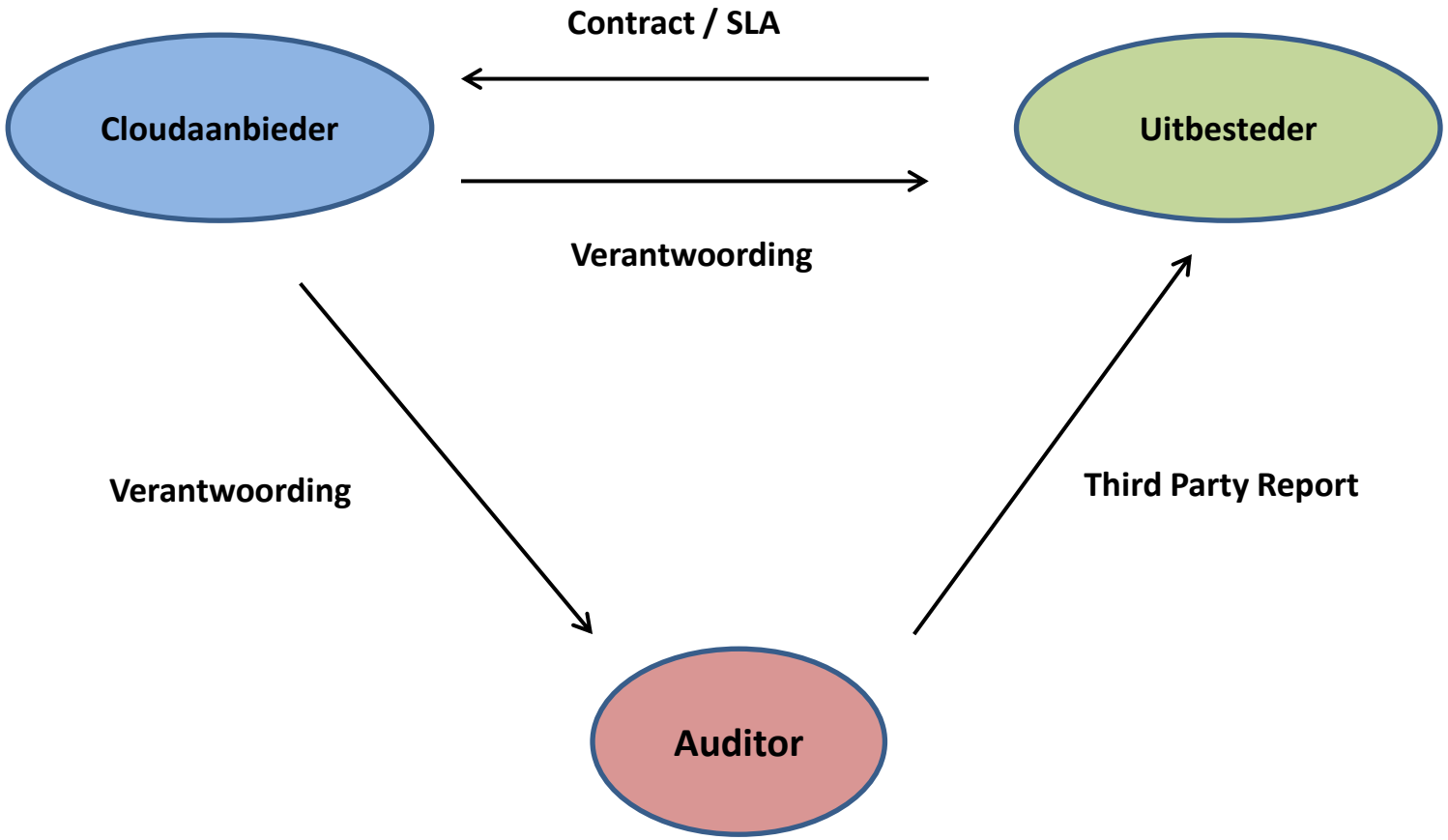
- Duidelijkheid vooraf wat wel / niet uitbesteden en voorwaarden waaronder
- Contract met SLA waarin operationele afspraken in de vorm van meetbare KPI's.
- Flexibiliteit zodat ingespeeld kan worden op ontwikkelingen
- Voldoende eigen deskundigheid in huis om te kunnen aansturen / controleren
- Eerst eigen organisatie / processen op orde, dan pas uitbesteden

Hoe zicht op kwaliteit dienstverlening Cloudaanbieder?

- Eigen onderzoek (vaak niet mogelijk of doelmatig)
- Beschikbaarheid van vormen certificering of Third Party Reports, waarin inzicht wordt gegeven in kwaliteit dienstverlening

- Vormen kunnen zijn:
  - ISO 27001/2
  - Third Party Report op basis van ISAE 3000 of 3402
  - Keurmerk ‘Zeker Online”

Verhoudingen tussen de partijen



Belangrijke vragen bij gebruik TPR

- Object van onderzoek?
  - Veelal overeengekomen diensten / interne beheersing
- Afbakening?
  - Scope (Opzet / Bestaan / Werking)
  - Invalshoek (kwaliteitscriteria)
- Normenkader?
  - Algemeen normenkader (maatschappelijk aanvaard)
  - Normenkader aanbieder
- Aard van het oordeel?
- Kwalificaties uitvoerend auditor?
- Welke audit standaarden gehanteerd?
- Welke werkzaamheden uitgevoerd?

Knelpunten bij gebruik TPR

- Onjuiste afbakening object van onderzoek (Out of scope)
- Geen match met beheerdoelstellingen gebruiker
- Gehanteerde normen?
- Oordeel gebaseerd op onvoldoende bewijs
- Onvoldoende inzicht uitgevoerde werkzaamheden
- Onderzoek niet gebaseerd op audit standaarden
- Rol en positie van de auditor?
- Betreft alleen opzet en bestaan, maar geen werking
- Onderzoeksperiode (werking) te beperkt
- Bij oordeelsvorming onvoldoende rekening gehouden met belang tekortkoming(en) voor gebruiker(s)
- Verspreiding buiten doelgroep
- Onjuiste interpretatie inhoud en waarde
- Wordt gezien als certificaat of garantiebewijs of In-control statement

Kenmerken ISAE 3000

- Assurance-rapport voor brede doelgroep
- Kan gericht zijn op: Opzet / Bestaan of Opzet / Bestaan en Werking (periode)
- Richtlijn ISAE 3000 stelt eisen aan:
  - De betrokken partijen
  - De auditor
  - De opdrachtverstrekking / -acceptatie
  - Het object van onderzoek
  - De te hanteren normen (o.a.: objectief, maatschappelijk draagvlak, dekkend)
  - Het bewijs
  - Keuze tussen “redelijke mate” of “beperkte mate” van zekerheid

Kenmerken ISAE 3402

- Primair communicatiemiddel tussen accountants (voorheen SAS 70)
- Assurance-rapport voor besloten verkeer: (accountant) gebruiker dienstverlening
- Kan gericht zijn op: Opzet / Bestaan (Type I) of Opzet / Bestaan en Werking (Type II)
- Object en te hanteren normen (niveau van beheersing) worden door de dienstverlener (Cloudaanbieder) bepaald
- Alleen oordeel met “redelijke mate” van zekerheid mogelijk

Kenmerken ISO 27001/2

- Focus vooral op Informatiebeveiliging
- Algemene set van normen, invulling afhankelijk van de organisatie
- Eisen aan onderzoek en bewijs beperkt

Complicerende factor

Bring Your Own Device (BOYD)

- Potentiele bedreiging voor:
  - Integriteit en/of verlies van bedrijfsdata
  - Vertrouwelijkheid
  - Compliance
  - Ondersteuning vanuit de organisatie

- Mogelijke oplossing
  - Bedrijfsbeleid m.b.t. gebruik van BYOD
  - Afgescheiden en beveiligde omgeving op YOD (MDM)