LES CONTRÔLES ET L'ASSURANCE DANS LE NUAGE, EN UTILISANT COBIT5

28 septembre 2016, Université Laval, Québec

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

David Henrard, CISM, CRISC, COBIT5 Implementation & Assessor
Conseiller en sécurité de l'information, PRP et gouvernance des TI

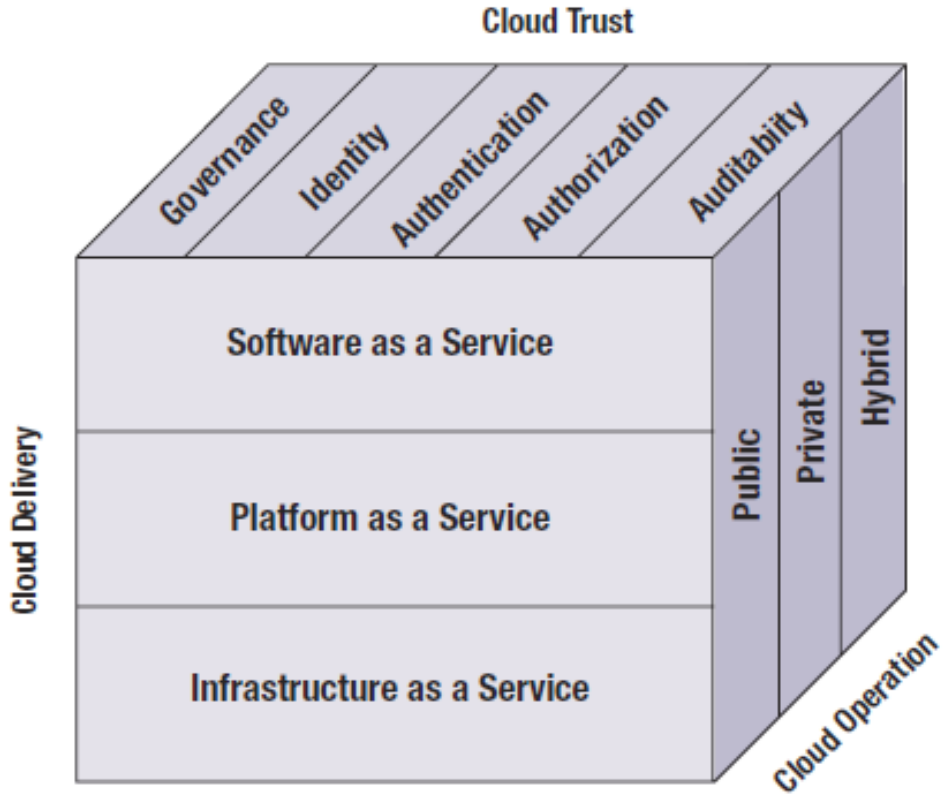
levio
AFFAIRES ET TECHNOLOGIES

Les 5 caractéristiques de l'infonuagique

Selon la définition du NIST

- Services en libre accès et à la demande (sans intervention humaine)
- Accessibles par le réseau étendu
- Ressources mises en commun
- Souplesse rapide
- Services sur mesure en fonction de l'utilisation

Figure 1—Cloud Computing Service Delivery and Deployment Model



Source: Trusted Cloud Reference Architecture © Cloud Security Alliance, *cloudsecurityalliance.org*. Used with permission.

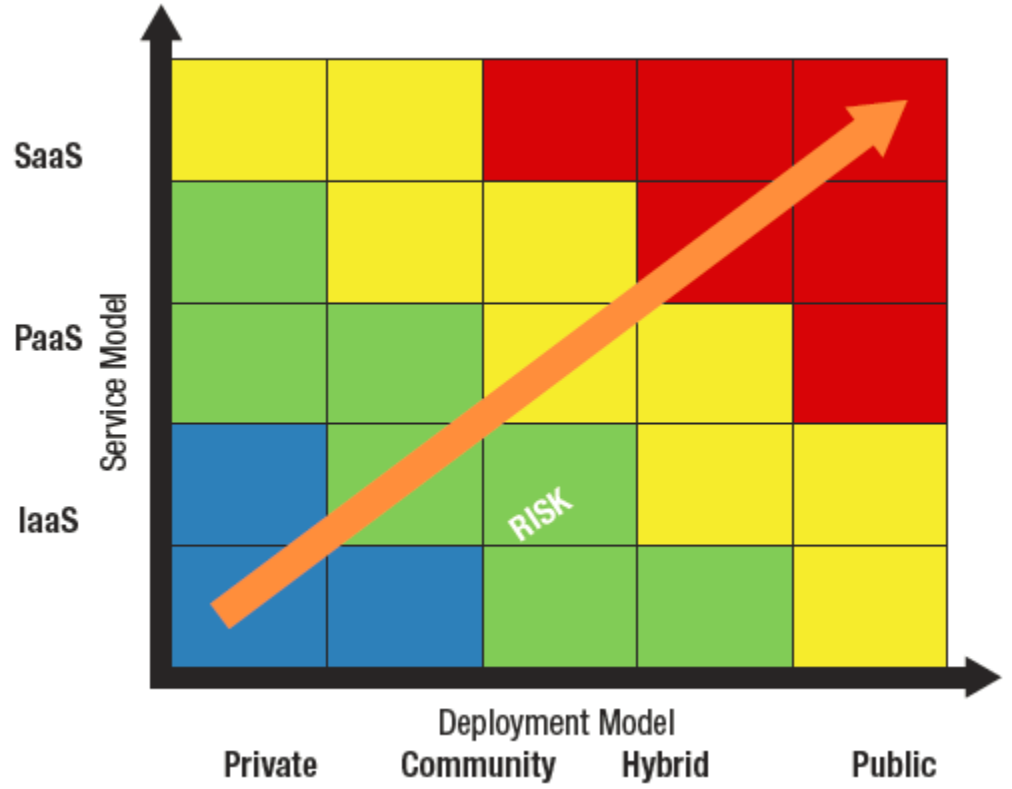
Les fondements de l’infonuagique

- Optimisation de l’utilisation des ressources
- Baisse des coûts
- Meilleure réactivité
- Cycle d’innovation plus rapide
- Réduction du temps de mise en œuvre
- Résilience (face aux interruptions)

Les éléments influençant les risques

- Type de modèle de services dans le nuage
- Robustesse des opérations TI de l'entreprise
- Niveau d'acceptation des risques d'affaires

Cartographie des risques liés à l'infonuagique



Évolution des services dans le nuage

- Nouveaux services:
  - SecaaS (sécurité)
  - DRaaS (reprise des activités)
  - IDaaS (Identité)
  - Data Storage and Data Analytics as a Service (Big Data)
  - InfoaaS (Information)
  - IPaaS (Plateformes intégrées)
  - FRaaS (Investigation légale)
- Courtage en services d'infonuagique
- Standardisation de l'infonuagique (portabilité, interopérabilité, certifications)
- G-Cloud

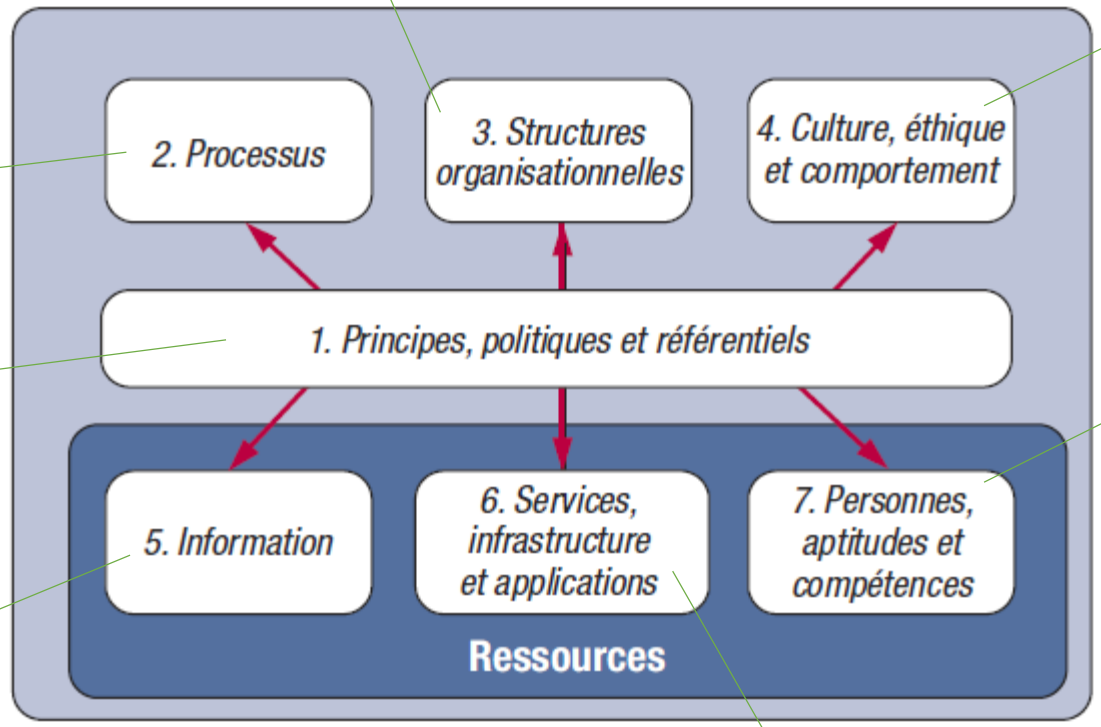
Les défis de l'infonuagique en relation avec les 7 facilitateurs de COBIT5

- Vérification des propriétaires des composantes du service

- Contrôles de sécurité adéquats

- Transparence en matière de politiques et de procédures
- Exigences de conformité

- Propriété des données
- Protection des journaux pour fins d'audits et d'enquête
- Élimination des données

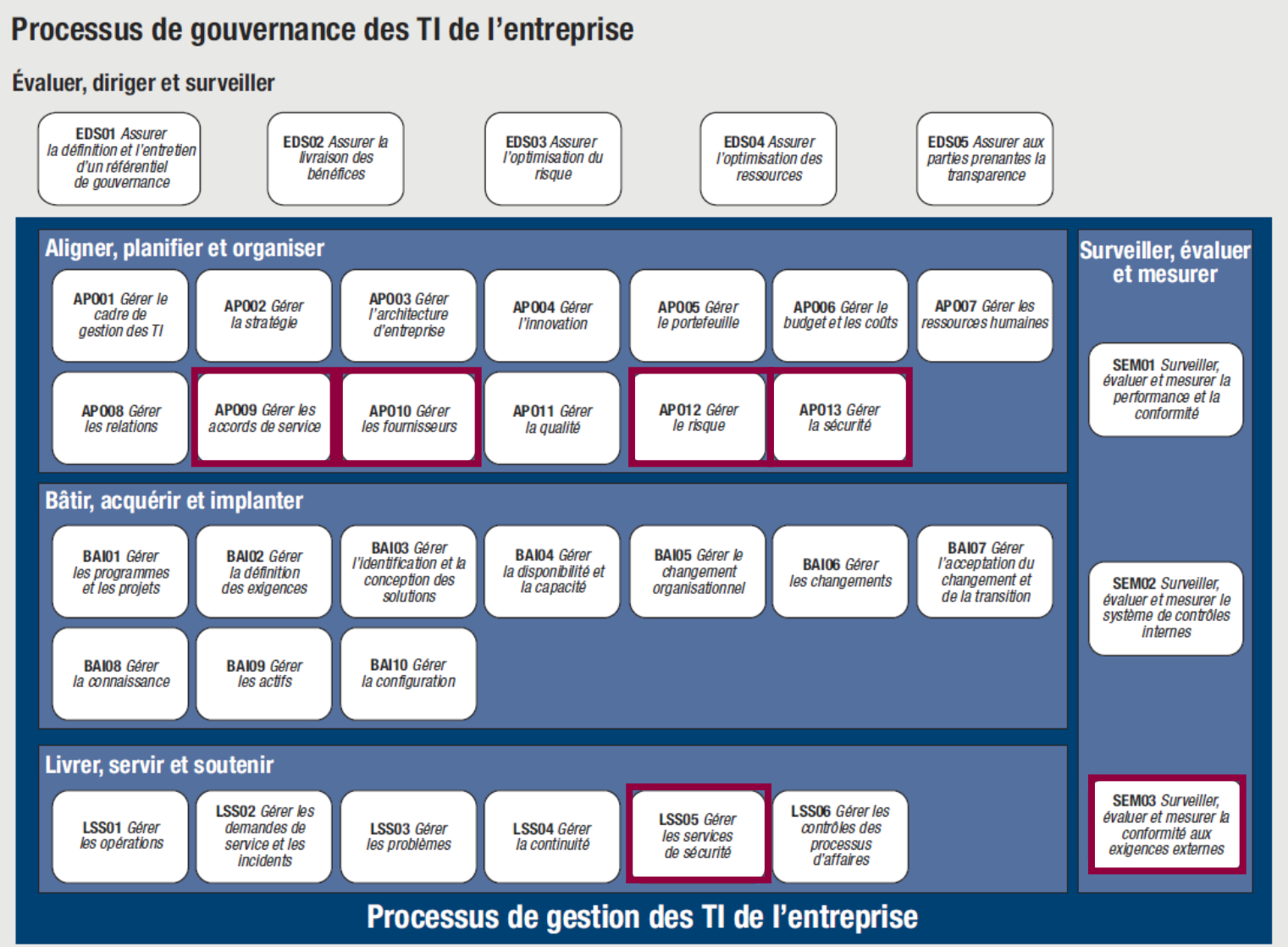


- Viabilité des fournisseurs
- Sélection des autres clients
- Culture de sécurité

- Dépendance envers des interfaces propriétaires du fournisseur

- Localisation des données
- Données amalgamées
- Gestion des accès et des identités
- Récupération après sinistre

Les processus de COBIT5 en lien avec l'infonuagique

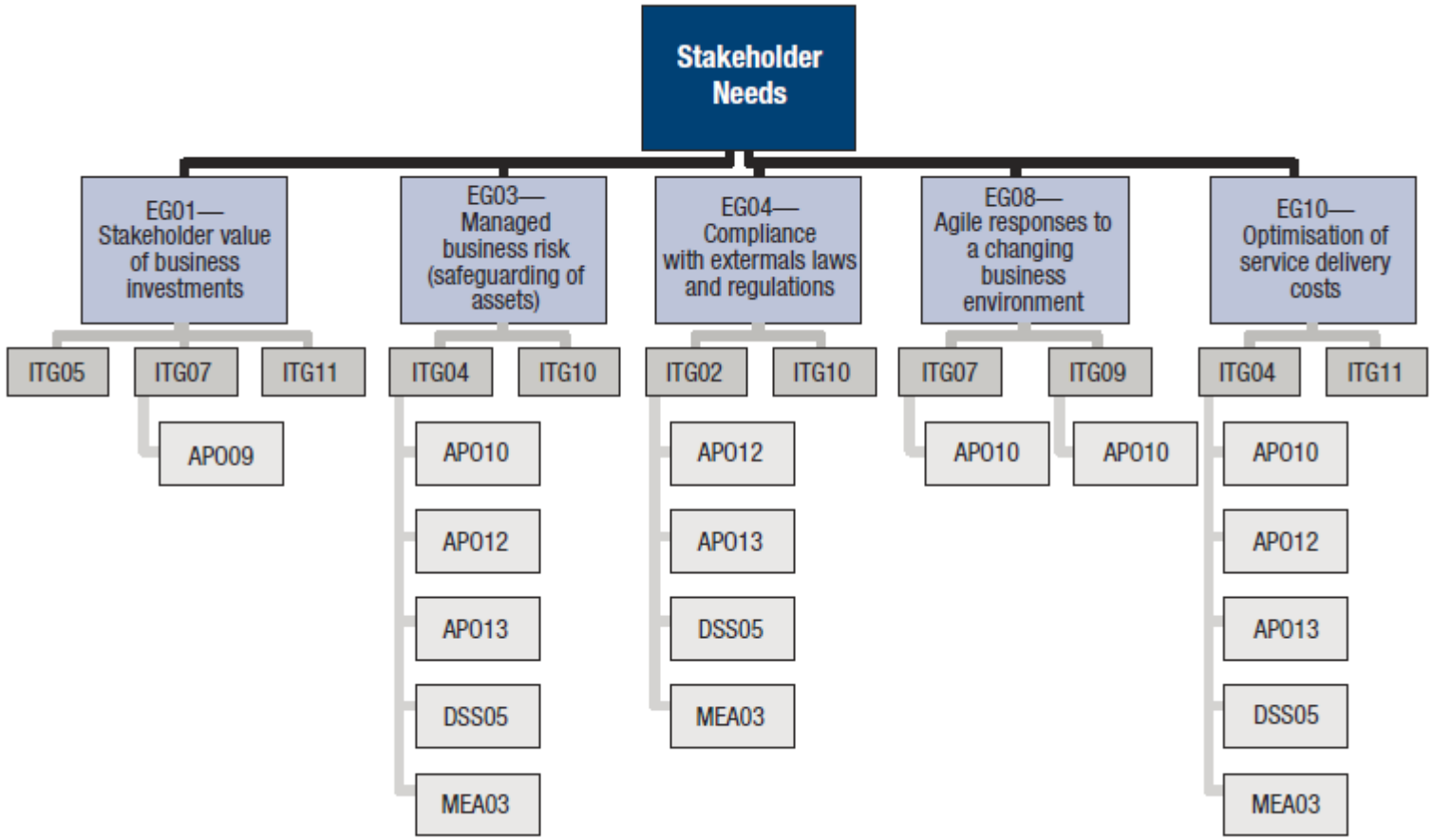


ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

L’établissement du besoin des parties prenantes envers le nuage

1. Identifier les besoins des parties prenantes désirés au regard des capacités actuelles des TI
2. Définir les opportunités envisageables
3. Quantifier les gains envisagés
4. Identifier les processus
5. Identifier la législation applicable
6. Valider ces informations avec les parties prenantes
7. Comparer les objectifs pour le nuage vs. les TI traditionnelles
8. Développer un cas d’affaires

Cascade d'objectifs pour l'infonuagique



Étapes vers la prise de décision

- Étape 1: Préparation de l'environnement interne
  - 7 facilitateurs, calcul du ROI (bénéfices-coûts), défis organisationnels
- Étape 2: Sélection du modèle de service d'infonuagique
- Étape 3: Sélection du modèle de déploiement
- Étape 4: Sélection du fournisseur

Figure 22—Example Cloud Scenario Model Decision Tree

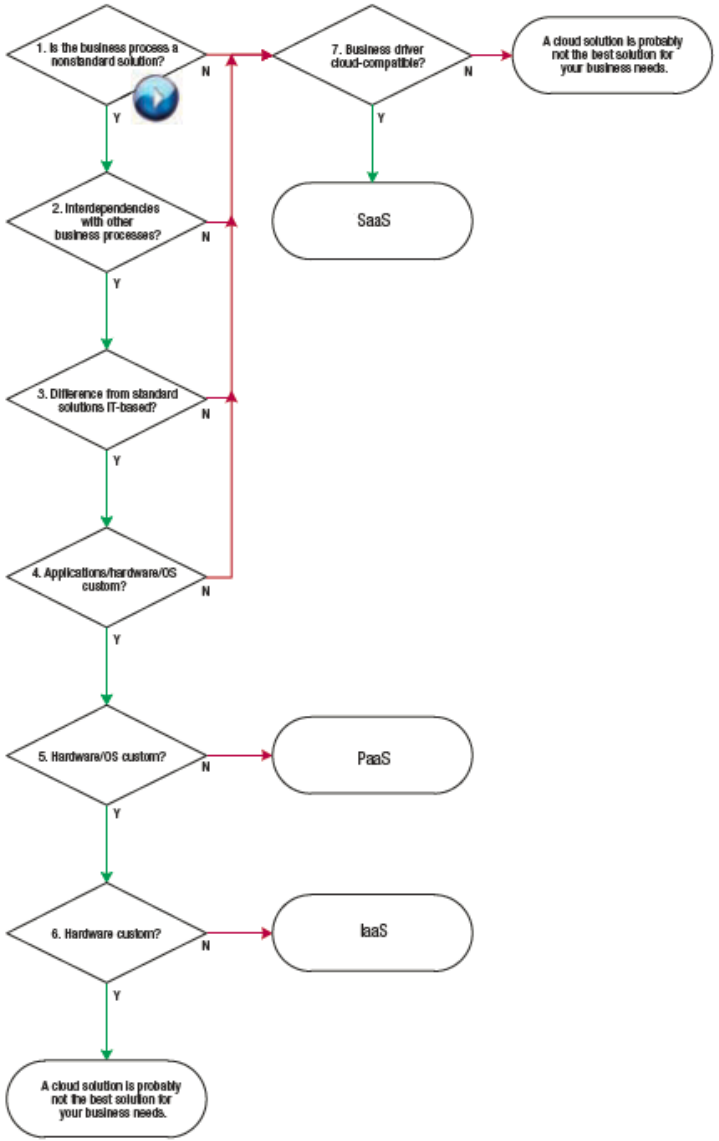
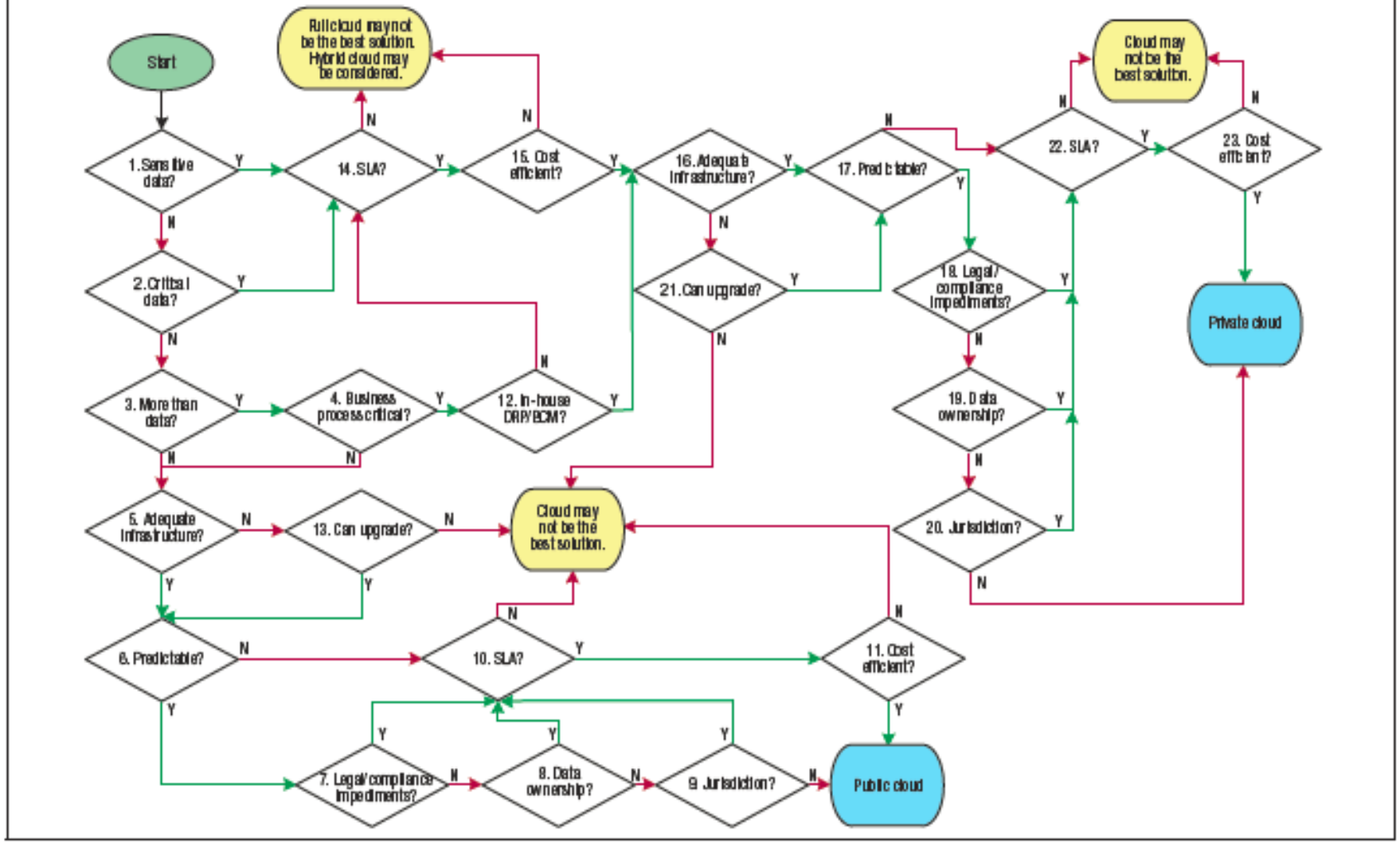


Figure 24—Example Cloud Deployment Model Decision Tree



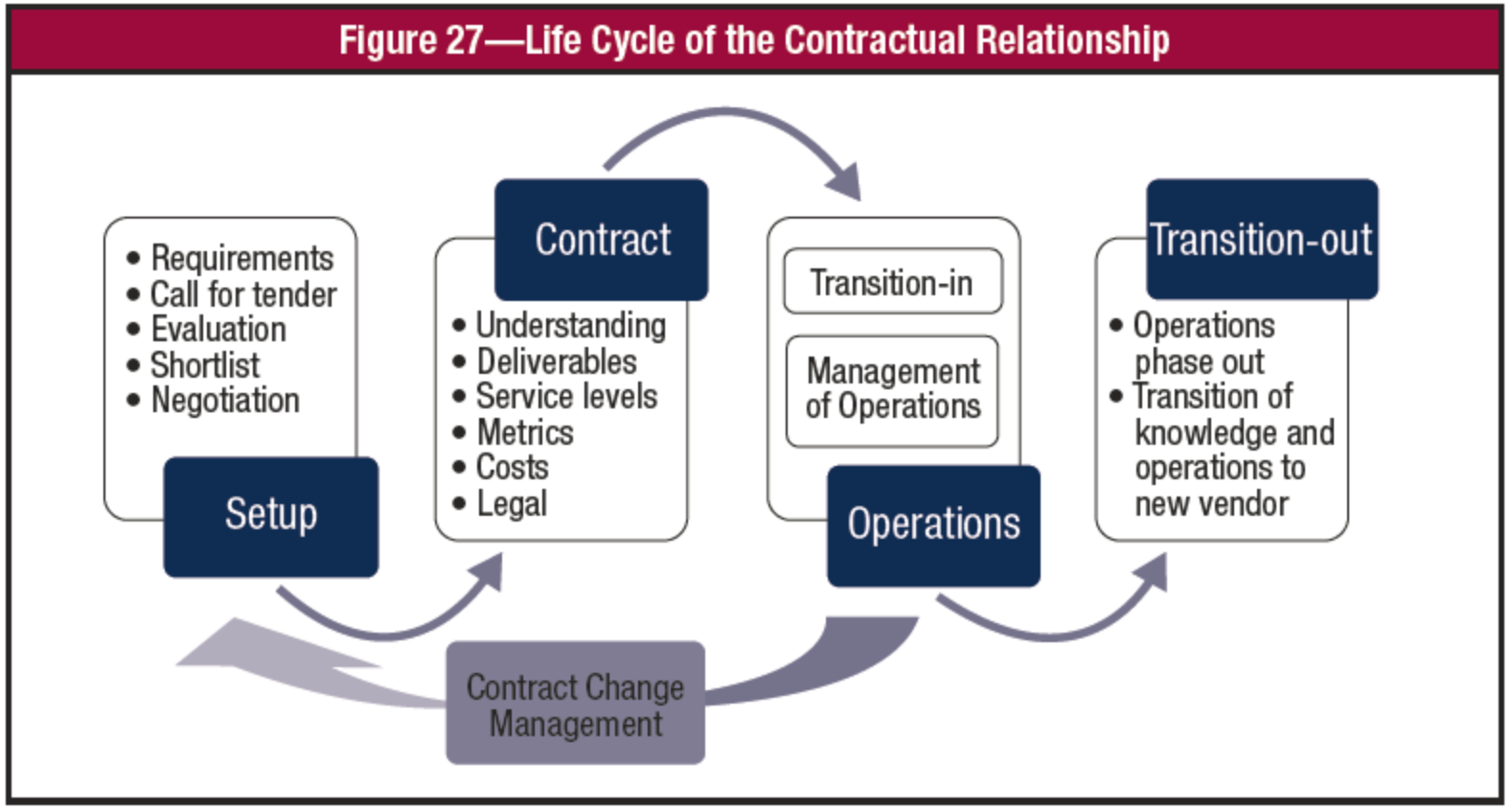
Critères de sélection du fournisseur

- Expertise du fournisseur
- Capacité du fournisseur
- Gestion des risques par le fournisseur
- Taille du fournisseur
- Lois applicables

Répartition des responsabilités

Figure 26—Vendor Management RACI Chart				
Stakeholders	Contractual Relationship Life Cycle			
	Setup	Contract	Operations	Transition-out
C-level executives	A	A	A	A
Business process owners	R	R	I	R
Procurement	R	R	I	R
Legal	R	R	C	C
Chief risk officer	C	C	R	R
Compliance and audit	C	C	C	C
IT	R	R	R	R
Security	R	C	R	C
HR	C	C	C	C

Cycle de vie de la relation contractuelle



Éléments à considérer dans les contrats

- Frais
- Rôles et responsabilités
- Documentation
- Flux de travail
- Procédure de récupération
- Pénalités
- Confidentialité de l’information
- Propriété intellectuelle
- Procédure de sortie

Sécurité dans le nuage

- Énoncé de risques
  - Risques techniques
  - Risques de conformité/légaux
  - Risques liés à la gouvernance de la sécurité de l’information

L’assurance dans l’infonuagique

Définitions:

- « Quelque chose qui inspire ou qui tend à inspirer la confiance » - *The Merriam-Webster dictionary*
- « Examen objectif de preuves en vue d’obtenir une évaluation des processus de gestion du risque, de contrôle ou de gouvernance d’une organisation » - *ISACA*

Une multitude de référentiels

COBIT 5

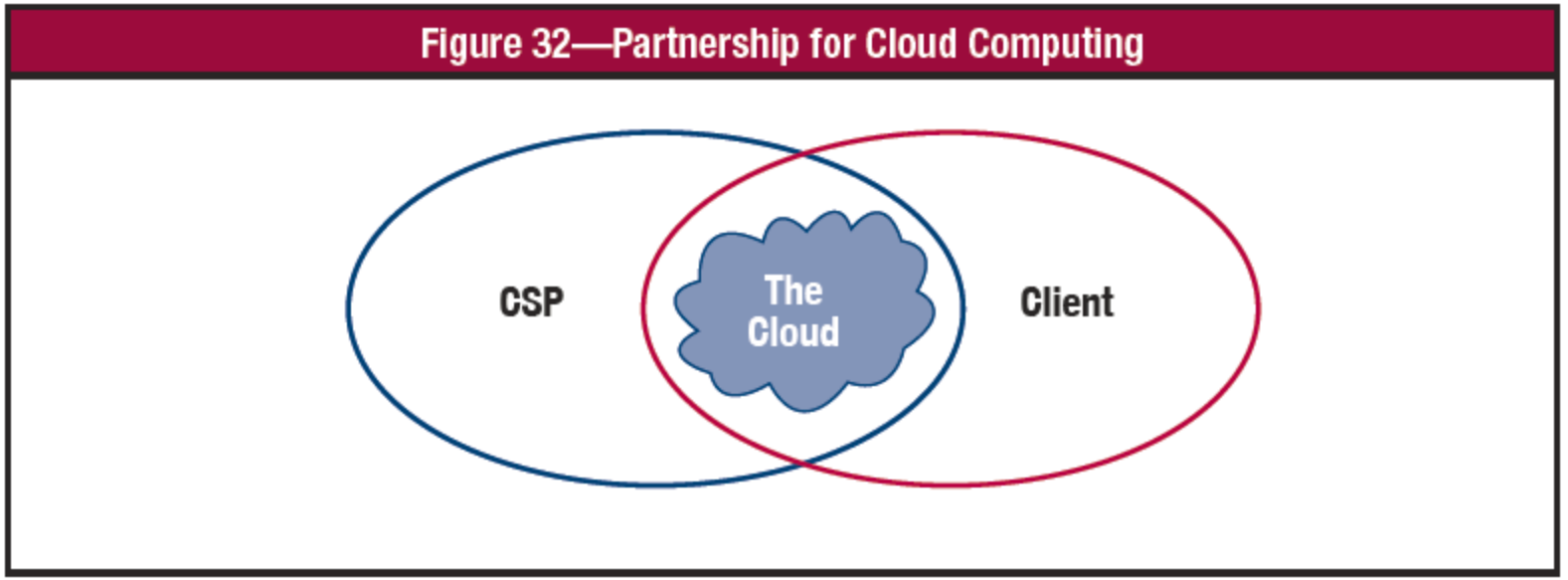
enisa
European Network and Information Security Agency

CSA STAR CERTIFICATION

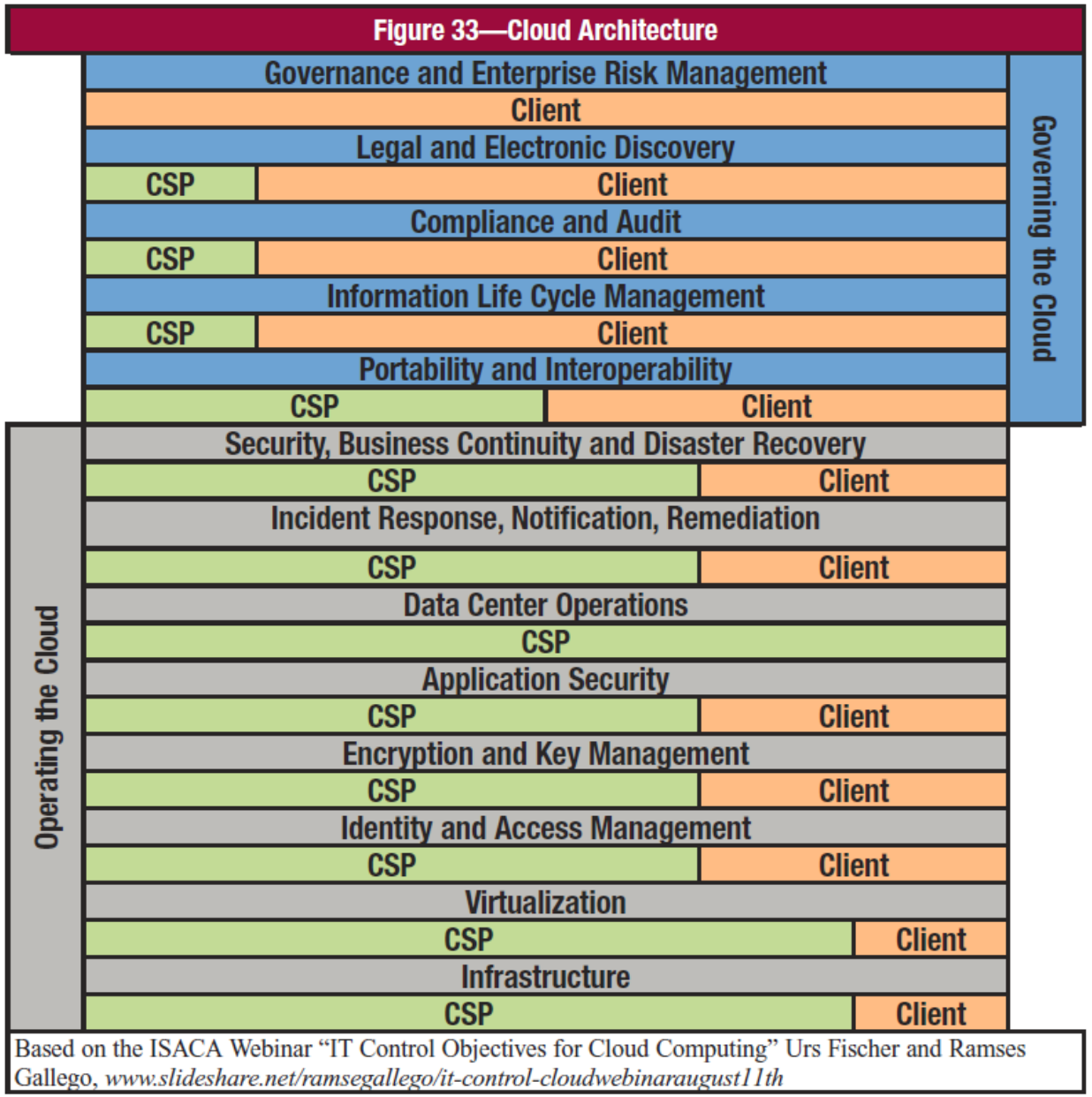
JERICHO FORUM
SELF ASSESSMENT SCHEME

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Partenariat Client/fournisseur

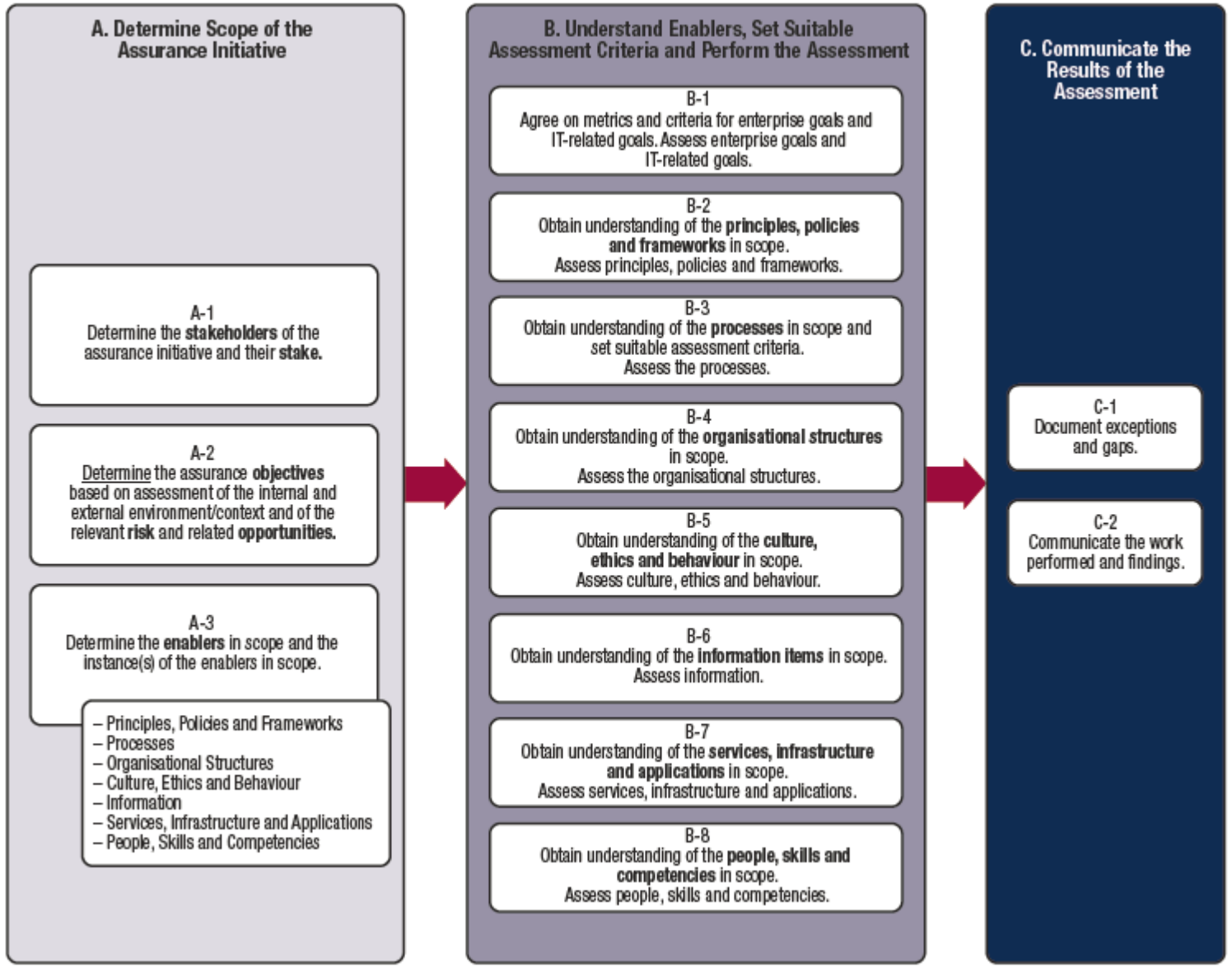


Répartition des responsabilités



Annexe A

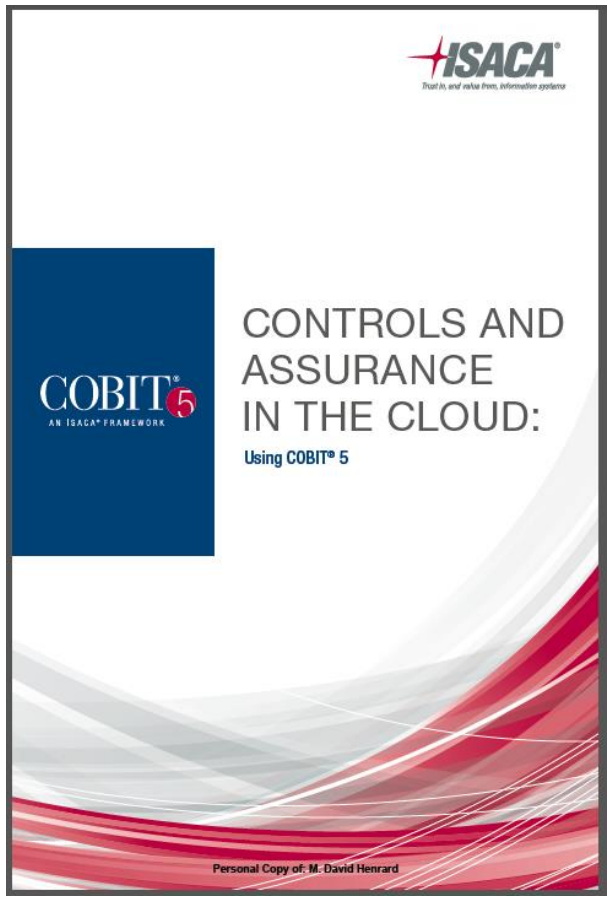
Démarche générale d'assurance basée sur COBIT5



Annexe B

ISACA
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

Références



Documents disponibles sur le site d'ISACA: http://www.isaca.org/cobit/pages/default.aspx

Merci !

AFFAIRES ET TECHNOLOGIES

David Henrard, CISM, CRISC, COBIT5 Implementation & Assessor
Conseiller en sécurité de l'information, PRP et gouvernance des TI
1995, rue Frank Carrel, bureau 219
Québec (Québec), G1N 4H9
Tél. 418 914-3623